U.S.COMMODITY FUTURES TRADING COMMISSION

CFTC TECHNOLOGY ADVISORY COMMITTEE (TAC)

Wednesday, March 27, 2019

10:04 a.m.

Commodity Futures Trading Commission - CFTC

Three Lafayette Centre

1155 21st Street, N.W.

Washington, D.C. 20581

BEFORE:

Brian D. Quintenz, CFTC Commissioner

Richard Gorelick, TAC Chairman

Daniel Gorfine, Designated Federal Official

ALSO PRESENT:

Rostin Behnam, CFTC Commissioner

Dawn DeBerry Stump, CFTC Commissioner

Dan M. Berkovitz, CFTC Commissioner

AGENDA

AGENDA (Cont'd)

P R O C E E D I N G S

MR. GORFINE: Good morning. As the TAC designated Federal officer, it is my pleasure to call this meeting to order. We are very much looking forward to today's discussions, which build on the foundation the TAC established last year and the work of our four subcommittees.

Speaking of our subcommittees, I would like to thank at the outset our outstanding ADFOs, who manage our subcommittees. And that includes Jorge Herrada, Scott Sloan, and John Coughlan. Pursuant to FACA requirements, we are also excited to welcome our new chairman of the TAC, Richard Gorelick.

TAC sponsor Commissioner Quintenz will now give his opening remarks.

COMMISSIONER QUINTENZ: Thank you, Dan. And good morning, everybody. Welcome to this third meeting of the Technology Advisory Committee.

Before we begin, let me just thank again all of our committee members for your robust participation and traveling here to be with us, taking time away from your jobs to participate and give us the benefit of

your expertise as well as to all of our subcommittee members, who are not on the full committee but who have participated in the discussions that have led to the discussion that we are going to have today. We very much appreciate all of your time and expertise.

In particular, I would like to take a moment to recognize our new chair of the Technology Advisory Committee, Richard Gorelick, for his willingness to lead and giving so generously of his time to advance our work here. Richard has a long and distinguished history as a market participant in the derivatives space. He has been an astute and consistent source of feedback for us here at the CFTC over a long period of time and has been a longstanding member of the Technology Advisory Committee, has participated on two of this committee's subcommittees. He has testified in front of Congress. Richard, thank you for continuing to provide us the benefit of your expertise and now for your leadership.

We have a packed agenda today. So forgive me for having a little bit of a longer opening statement than normal, just to try to highlight some of the

things that we will be discussing. First, starting right off the bat, for our Automated and Modern Trading Markets Subcommittee, CFTC's own Elitza Voeva-Kolev, and our new chief market intelligence officer, Mel Gunewardena, will present a new and fascinating report prepared by the CFTC's Market Intelligence Branch, entitled, "Impact of Automated Orders in the Futures Markets."

The staff report analyzes manual and automated trading's impact on the commodity futures markets. Specifically, the report examines transaction data in 30 different futures contracts for the period between January 2013 through December 2018 and analyzes the correlation, if any, of increased automated trading with volatility. The report contains several significant conclusions, including that the increase in automated order activity in all commodity futures markets has not correlated to increases in end-of-day price volatility.

The report will become in my opinion a substantial anchor and a reference point in the journey to achieve an objective, data-driven understanding of

the impact that automated and algorithmic trading play in our markets. I am extremely proud that this robust agency work product will be unveiled right here before our own TAC committee, with the public publication soon to follow.

The report is an excellent example of our staff using the data that the Commission collects in order to examine and better understand how market structure, trading activity, and market fundamentals are evolving in our core markets. I note that this report complements an earlier MIB report issued this past June examining sharp price movements in the commodity futures markets.

Further staff reports and data analysis, along with the expertise represented right here on this committee, are critical to accurately and specifically identifying the impacts and true risks associated with automated and algorithmic trading as well as how the development, adoption, and deployment of market-incentivized solutions are mitigating those risks. I look forward to more thoughts on that topic in the future from this subcommittee.

Secondly, our Virtual Currencies Subcommittee will first hear presentation from Peter Van Valkenburgh, director of research at Coin Center, on various consensus mechanisms used for virtual currencies. Currently, both Bitcoin and Ether rely on a proof of work consensus mechanism to validate their respective ledgers. However, the Ethereum Foundation has announced its plans to shift to a proof of stake consensus mechanism at some point in the future, in part, to reduce energy consumption. The transition from proof of work to proof of stake consensus mechanisms raises important questions for both market participants and regulators, including how the use of either mechanism affects the likelihood that a bad actor could manipulate or falsify the ledger. These issues are also among the many topics on which the Commission recently sought comment in a request for information about the evolution of the cryptocurrency market and potential new virtual currency-based futures and derivatives products.

Following Mr. Van Valkenburgh's presentation, we will hear from Kathryn Trkla and Charlie Mills from

the American Bar Association's Jurisdiction Working Group of the Innovative and Digital Products and Processes Subcommittee. It is a name only lawyers could love apparently. That group has recently published a comprehensive overview of the current Federal and state regulation of virtual currencies and digital assets, along with identifying key policy areas for additional consideration. I am excited to hear from these distinguished panelists on their work.

Next, our Cybersecurity Subcommittee will hear from Josh Magri, senior vice president and counsel for regulation and developing technology at the Bank Policy Institute. Mr. Magri will provide an overview of the Financial Services Sector Coordinating Council's cybersecurity profile. The profile presents a possible common, standardized approach that regulators could use when examining cybersecurity at firms.

We will also hear about how the transition to cloud-based infrastructure may pose unique cybersecurity concerns for firms as firms work to adjust their current controls to a shared-responsibilities environment.

The Cybersecurity Subcommittee has also begun to review existing regulatory guidance on third party vendor risk management, with the goal of presenting possible recommendations to the full TAC about ways in which the CFTC could strengthen its existing guidance in this area. We will hear from subcommittee members about their progress to date on this important initiative.

Finally, our Distributed Ledger Technology and Market Infrastructure Subcommittee will present on the current state of DLT, including challenges towards more widespread adoption and potential use cases. The panel will explore if there are specific areas where the CFTC regulations may be inhibiting the adoption of DLT or additional areas where further guidance from the agency could support further development.

And, lastly, we will hear from ISDA representatives about the recent release of the common domain model 2.0 for interest rate and credit derivatives. The further actualization of DLT in the derivatives space depends on the ability of market participants to digitize all aspects of their financial

transactions. Once the terms of a swap can be reduced to a completely digital, industry-accepted standard, then automated trade reporting; centralized recordkeeping; and, ultimately, smart contracts become possible. ISDA's CDM 2.0 aims to create a standard digital representation for products and lifecycle events in the interest rate and credit derivatives markets, with the hope of expanding to other asset classes later this year. CDM 2.0 is now fully accessible to all market participants, which is an important step towards building broader consensus and supporting its further application in new projects.

Just quickly, before I conclude, I would like to very much thank Dan Gorfine, our designated Federal officer and the director of LabCFTC, for his tireless work in organizing all of the conversations and effort to have today's meeting. I also would like to recognize Jorge Herrada, John Coughlan, and Scott Sloan for being the designated Federal officers for our subcommittees and for their tireless work.

I am now going to turn it over to the chairman and my fellow commissioners for their

comments, but, as many of you may have noticed, our fearless leader, Chairman Giancarlo, is not with us this morning. He is recovering from a cold and didn't want to turn our public meeting into a quarantined one. So, instead, we have Mike Gill, the agency's chief of staff, to give the chairman's remarks.

Mike, be warned the chairman assured me he would be watching very closely and judging your delivery. So please proceed.

MR. GILL: Well, I actually just got a report from our data technology group that everything was working with the webcast and such because he is actually watching this on the webcast. So, ODT, be on guard.

Thank you, Commissioner Quintenz. As you mentioned, the chairman is, unfortunately, under the weather and cannot be with us in person today, but he did want me to come and make a few remarks, specifically applauding the TAC on its structure, focus, and timeliness in exploring a range of emerging technologies and issues that are impacting our markets today.

The subcommittee's structure and the dedicated work of its members are helping to drive deep-dive consideration of issues across automated trading, virtual currencies, DLT, and cybersecurity.

I look forward to hearing from a broad range of special guest speakers, who will be sharing timely insights and feedback with the Commission. It is through this type of engagement that we as a Commission stay at the forefront of emerging issues and topics.

To that end, I want to preemptively thank our staff from DMO and specifically its MIB branch for sharing their findings on the impact of automated orders on markets. When the chairman conceived the Market Information Branch, it is exactly this type of summary in these reports that he had in mind. And so the chairman is especially pleased that MIB is here and presenting its reports.

I would also like to commend the TAC DFO. Daniel is going to get a large head after everyone thanks him for all of his work. But he and his team have done a tremendous job with this Technology Committee, and they should be recognized.

It looks like we are in for a day of rich dialogue and discussion. And I look forward to sitting in the chairman's seat and learning all I can today. So thank you very much.

COMMISSIONER QUINTENZ: Thanks, Mike.

Commissioner Behnam?

COMMISSIONER BEHNAM: Thanks, Commissioner Quintenz. Welcome to all of you back to the CFTC. Thanks, Commissioner Quintenz, for your leadership on this issue. And thanks to Mr. Gorelick. And, of course, as Richard and I discussed earlier, I am going to call him chairman from now on. So congrats to him on his new job.

I look forward to today's discussion. I do have to peel out a little bit early after lunch. So I will excuse myself now but certainly look forward to the dialogue and the findings that the committee members have.

Thank you.

COMMISSIONER QUINTENZ: Thank you.

Commissioner Stump?

COMMISSIONER STUMP: I am going to repeat

everything that everyone said. Thank you to Commissioner Quintenz for having the meeting.

This is my second TAC meeting. So I feel like I have my feet under me a bit better than I did at the last one. I am really excited. Particularly this first presentation is exciting to me. I am so happy that you all have engaged in this work. I know you all know that the commodity markets are continuing to adapt to the new automated trading environment that they operate in. In particular, near and dear to me are the agricultural markets. And so I think this work is going to be hugely helpful to those particular industries in understanding how the markets have evolved. So thanks to everyone who worked on all of the reports that are being presented today, particularly the first one.

And a huge thanks -- I doubt that Daniel is going to have an inflated ego, as Mike suggested, but you really do deserve a lot of credit for putting together a tremendous group of folks and work product. So thank you very much.

And, Richard, we are really excited that you

are chairing the TAC.

Thank you.

COMMISSIONER QUINTENZ: Thanks, Commissioner Stump.

Commissioner Berkovitz?

COMMISSIONER BERKOVITZ: Thank you, Commissioner Quintenz.

Good morning, everyone, and welcome to the CFTC. It is great to see so many people that I have been working with over the years in this forum.

I want to thank Commissioner Quintenz for hosting this meeting and welcome Richard as the chair. I am very much looking forward to our meeting today on technology. Use of ever-advancing technology has always been a key feature of the derivative markets. And the presentations today address a number of issues of significance for our market participants.

The first panel on automated order trading is very timely. As we know, automated trading is a major part of our markets and part of the -- most of the financial markets rely on automated trading. I am glad to see the Commission is continuing to examine this

issue.

I am very much looking forward to the second panel, the American Bar Association. I am very familiar with the work of that organization. Over the years, it has provided many thoughtful analyses and recommendations to the Commission on a variety of issues that have actually found their way into our regulatory structure. And so I am very much looking forward to the presentations today from those panelists.

When I was before the Senate Agriculture Committee last year during my nomination hearing, I was asked about data use and management. At that time, I informed the committee that this is an area that I believe the CFTC should be focused on going forward. The afternoon panels will touch on data protection and management. And so I am very much looking forward to that panel.

Distributed ledger technology. I recently had the privilege of being on a panel discussion with one of the distinguished members of this committee: Brad Levy, over there. We were on a panel. And not

only was I to participate on the panel, but I got to see another panel at this conference talking about potential use of distributed ledger technology in the energy industry. There were a number of exhibits at that conference on this topic. And I am very much looking forward to the presentations on how DLT can impact and improve our markets and our regulatory oversight of those markets.

So I am very much looking forward to all of the presentations today and again welcome all of the members of the committee. Thank you.

COMMISSIONER QUINTENZ: Thank you, Commissioner Berkovitz. I thank my fellow commissioners and the chairman and Mike for your thoughtful comments.

And, with that, I am very pleased to turn it over to our new TAC chair, Richard Gorelick.

CHAIRMAN GORELICK: Thank you, Commissioner Quintenz, Mr. Chairman by proxy, and all of the CFTC commissioners.

I am honored to have been a member of this Technology Advisory Committee since it was

reconstituted in 2010 and now to be named chair of the TAC. I look forward to building on the long body of work of this committee.

It has been an important venue to foster public dialogue on the role of technology and automation in today's modern electronic markets. We are witnessing a fascinating time where technologies are continuing to have a profound impact on how we trade and even what we trade. As chairman, I look forward to working with my TAC member colleagues to provide the Commission with feedback and recommendations that assist the agency in its oversight of our markets and to continue to support a regulatory environment that understands and utilizes technology to promote fair competition, encourage innovation, enhance transparency, manage systemic risk, lower costs for investors and hedgers, and give the CFTC the tools that it needs to be an effective modern regulator.

I would now like to discuss the approach for today's meeting. As previously noted, we will have presentations by our four subcommittees on Automated and Modern Trading Markets, Virtual Currencies,

Cybersecurity, and DLT and Market Infrastructure. We will also have a few special guest presentations, including from the CFTC's Division of Market Oversight.

Before we get started, please ensure that your microphone is on when you speak and that you are speaking clearly into the mike so that the webcast and the teleconference audiences can hear you. If you would like to be recognized during the discussions, please place your name card like this so that it sits vertically on the table or raise your hand. For TAC members participating by phone, please keep your phone on mute until you are ready to speak and identify yourself beforehand. Please also refrain from using electronic devices during the meeting.

We have one more item to share before we get started with our first panel. And for that, I will turn back to Daniel.

MR. GORFINE: Great. Thank you, Richard.

Shockingly, I don't have this memorized yet. So I am going to read it to you. During this meeting, there may be references to specific products, entities, or services. Please note that the views and opinions

expressed in this meeting regarding these products, entities, and services do not necessarily reflect those of the United States Government or the CFTC. Additionally, any reference to such products, entities, or services is not an endorsement or recommendation by the United States Government or the CFTC but are simply examples of technological solutions in the financial services and commodity markets. Therefore, the CFTC welcomes comments from the public about alternative technological solutions to address the matters discussed during this TAC meeting.

Instructions for submitting additional comments and the deadline for submitting such comments are provided on the CFTC website under the TAC meeting webpage. Please note that any comments made in connection with this TAC meeting will be made available to the public.

Thanks.

CHAIRMAN GORELICK: With that, let’s turn to our first panel discussion, which will include presentations from the Automated and Modern Trading Market Subcommittee and a special presentation from DMO

on the impact of automated orders on markets. You will hear first from Mel Gunewardena and Elitza Voeva-Kolev of the CFTC. Mel, who is also the new CFTC chief market intelligence officer, we will begin with you.

MR. GUNEWARDENA: Thank you, Richard.

I am going to hand this over to Elitza, who has really done a lot of the work with this report. It is the beginning, not the end of the work in automation that we do, but I think you will find that this work across almost 2.3 billion transactions that occurred between 2013 and 2018 provides great insight into the level of automation and the effects of that in our industry.

With that, I am going to hand it over to Elitza to go through the report. And we will be both open to taking questions, comments, and even suggestions as we kind of continue our work in this regard. Elitza?

MS. VOEVA-KOLEV: Thank you.

So I will be reviewing an analysis of entering orders manually and automatically in futures markets. This research is a broad overview of trading

activity. And the views expressed here are staff's views and not necessarily the views of the CFTC, the chairman, or the commissioners.

So over the past few years, staff from the Division of Market Oversight has interviewed numerous market participants who trade across different commodities. And what we discovered from these interviews is that nowadays participants, aided by technology, are able to place large numbers of transactions for significant volumes. And because it is important to understand how this technology-driven trading is affecting our markets, we followed up with this analysis and used internal CFTC transactional data. And what we did is, basically, we compared manually to automatically placed orders and examined what effects, if any, these two mechanisms had on futures markets.

What we found was that the percentage of automatically placed orders has increased for all commodity futures markets. Automated orders are smaller in size than manual orders. And the resting times are shorter than the resting times of orders

placed manually. Automated orders are almost exclusively limit orders. And although the level of automation increased steadily each year, historical volatility of end-of-day prices did not exhibit the same trend.

We used a basic historical volatility measure that involved settlement prices, instead of intraday implied volatility. And I will go into more detail later in the presentation. And now some definitions are in order.

So automated and manual order entry refers to how an order is placed on the order entry message. This is a self-identified flag, which is reported by traders themselves. And it is required only by the CME. So our analysis was limited to CME contracts. So for the CME, annual manual order entry means that somebody physically entered an order through a touchscreen or using a keyboard.

Automated orders, or ATS, how we call them, on the other hand, were generated or routed without any human intervention. And this can be a very simple program telling the computer to buy at a certain price

or it can be a really advanced algorithm.

This is the place to say that automated trading is not the same as high-frequency trading, or HFT. HFT is just a subset of automated trading because, as I said, the field does not inform on the level of sophistication. And, nowadays, most trading platforms offer some degree of automation.

We analyzed over 2.3 billion transactions from 2013 to 2018. We couldn't go further back in time because the very end of 2012 is when we started getting the field automated and manual populated in our data. We analyzed 30 contracts in 8 commodity groups. And all data was sourced internally from trade capture reports.

And this next slide, page 4, this is a list of the futures contracts that we assigned to the eight commodity groups, which are currencies, equities, financials, energies, metals, grains, oilseeds, and livestock. I am not going to list all of the futures markets, but you should know that we only included the most actively traded contract in each commodity group.

And we are going to begin by examining how

the degree of automation in futures has changed over the years. This graph on page 5 shows the share of automated orders present in futures markets. On top, you can see all of the DMO-defined commodity groups. The x-axis shows you each year. And, then, the y-axis shows you the percentage of automated orders in each commodity group.

And, as you can see, across all groups, the share of automated orders increased from 2013 to 2018. On average, the percentage of the automatically entered orders in currencies, equities, and financials, which are the first three panels on the graph, increased by 7 percent. We see a more dramatic increase of about 19 percent for the physical commodity groups of energy, metals, grains, oilseeds, and livestock.

As you can see, the level of automation for the first three panels, or the financial products, was already very high, but automation is filtering to the rest of the markets. And it was nearing 70 percent at the end of last year. And after conducting interviews with market participants, we determined that a possible explanation for the high level of automation in the

financial products is the very high transactional volumes in these markets and also the low basis risk between the futures contracts and the underlying cash market. In contrast, physical commodities usually have higher basis risk associated with contract or delivery specifications of the cash market.

We also looked into options, even though this is not reflected in this graph. On average, we found that across all groups during 2018, automated orders were 23 percent more common for futures than for options. And this observation is expected since options are very customizable, which makes it more difficult for options orders to be automated. As technology improves, we could see increased automation in options trading, too.

And, next, we are going to look at resting times of limit orders and limit orders because, as you will see in a couple of slides, limit orders are the most prevalent order type. And this graph shows you how long orders were exposed to the market before being consummated. Resting time is basically the time between when an order was entered on the order entry

message and when it was filled. In a sense, resting time is a measure of the speed of trading.

The red lines show you the automated orders. And the blue lines show you the manual orders. The graphs with the white background, the exchange uses a first in/first out, or FIFO, algorithm to match buy and sell orders; whereas, the group shaded in yellow, the matching algorithm prioritizes based on order size.

As you can see, manual orders tend to be exposed to the market for a little longer. And from interviewing market participants, we have determined that a possible explanation for that occurrence is that market limit orders tend to be placed away from the market. And that is why they take a little longer to fill. And overall from this graph, we can see that the commodity groups with the higher level of automation also have shorter resting times.

And then the next slide, on page 7, we investigated whether there was a difference in transaction size between manual and automated orders. And this graph shows on average how many contracts were consummated per transaction. Again, the automated

orders are in red, and the manual are in blue. As you can see across all markets, the average number of contracts consummated per transaction was a little smaller for automated orders. On average, in most markets, there were about two contracts per transaction with the exception of the equities and the financial groups.

The e-mini S&P, NASDAQ, the 10-year Treasury notes, Eurodollar, and the Federal funds all trade large orders. We examined the participants in our trade report database and found that in those markets, they are big institutional traders who place large orders.

We also investigated the order composition of manual and automated orders. Automated orders on this graph are shown at the top panel, and manual orders are shown at the bottom panel. The different order types that markets typically allow are limit, shown in gray; market, in purple; and stop, in orange. Limit orders allow the buyer to define a maximum purchase price for buying and minimum sell price for selling an instrument. Market orders get executed right away at

the current market price. And stop orders do not immediately go on the book. They must be triggered at the price level submitted with the order.

As you can see on the graph, automated orders are almost exclusively limit orders. Manual traders use stop orders four percent and market orders 11 percent of the time. The reason for this is that automated traders can replicate the functionality of stop and market orders by relying on their speed in reading the market and placing limit orders instead.

Even if an order has stop loss components to it in the computer behind the scenes, how it comes to the market and how we see it in our data is a limit order. What this means for us is that when we try to understand market events, we cannot rely on stop orders to help explain what happened. And since 2013, the CME updated their velocity logic of halting trading to include both stop and limit orders. And on our end, we are seeing fewer market events in which stop orders were implicated.

Next, we examined how overall prices have changed over the study period. We analyzed price

movements in two ways, the first one by counting the number of up-and-down price ticks or the number of times prices moved every day. This measurement is at the top panel of this graph. We also calculated the variance of one-day natural log price returns from the end-of-day settlement prices and then normalized them to an annual volatility measure. This is shown at the bottom panel of the graph.

Even though these two measurements seemed similar, they addressed different aspects of trading. The transaction-to-transaction price moves capture price fluctuations driven by factors intrinsic to the market, such as market structure and trading activity. The historical statistical volatility is considered to be driven by market fundamentals because it involves changes in prices over long periods of time, in this case over years.

As we see, price moves and day-to-day historical volatility move in tandem. In other words, intraday trading accurately reflects the fundamental driven volatility.

We also performed a basic statistical

analysis on the two price measurements I just discussed. This scatter plot shows the correlation between historical end-of-day price volatility and average number of price moves.

The numbers within the individual blocks represent the correlation coefficients. Most of these coefficients are above 0.5, meaning that there is a moderate-to-high positive linear relationship between the two price measurements. If the two measurements did not move jointly, that would have raised concerns about trading mechanisms and overall market structure.

So the presentation that is on the screen is actually missing one page, but everybody should have it in their presentation in front of them. The title of the slide is “Correlation Between Historical Volatility and Share of Automation.”

So we performed the similar correlation analysis that I just showed you on the relationship between historical volatility and share of automation. The correlation coefficients between the historical volatility and how automation has increased in the commodity groups, those coefficients are either around

0.1, which implies that there is no relationship between the two, or around -0.5, which implies a negative linear relationship. That simply means that as one variable increases in value, the other variable decreases.

As we discussed at the beginning of this presentation, the level of automated trading in futures markets has increased steadily from 2013 to 2018. This correlation analysis shows that historical end-of-day price volatility has not equally been increasing year over year. This does not imply that automated trading has not affected short-term market events.

And next is the last graph of the presentation. This graph simply displays trading volume and historical day-to-day volatility together. As expected, as historical volatility goes up, so does the trading volume. For example, in the equities, the well-known decrease in volatility from 2015 to 2016 and its subsequent increase in 2017 are, similarly, reflected in the changes in volume for those years.

So, again, this was a broad overview of trading in the futures markets and the increased level

of automation. And based on our analysis and interviews with market participants, we have concluded that the number of automated orders in futures markets has increased. Automated orders are smaller, faster, and mostly limit orders. And historical end-of-day volatility does not appear to follow the same increase as that of automated orders.

And we would welcome all feedback and suggestions for follow-up studies or any comments. So please feel free to reach out to me or Rahul if you would like to.

CHAIRMAN GORELICK: Okay. Thank you very much for that presentation.

Before we move on to the second presentation from this subcommittee, I wanted to open up for questions here. Is there anyone on the committee here that wanted to ask some questions about this presentation? Adam?

MR. NUNES: Thank you.

My question is, did you look at whether or not the increase in automated orders is because firms who are always sending a very large portion or just

sending more orders or that, you know, firms that previously were sending manual orders converted and started sending a bigger portion of automated orders?

MS. VOEVA-KOLEV: So it is actually a mixture. Some of it is because there is just more volume traded. And some of the manual orders are converting to automated.

CHAIRMAN GORELICK: Elitza, I had a question for you on the presentation. Did you look at distinguishing the limit orders between marketable limit orders that were immediately cross the bid-ask spread and nonmarketable that tended to be resting orders?

MS. VOEVA-KOLEV: No. We did not do that distinction.

CHAIRMAN GORELICK: Okay. I suspect that that might be an interesting follow-on to this study. And it may provide some interesting information about resting times, for example.

MS. VOEVA-KOLEV: Thank you.

MR. WORKIE: I just had a question about the last conclusion, where you talked about the increase in

automation and then compared it to a lack of increase in volatility. Were you expecting there to be an increase in volatility over that period of time? I was just trying to understand, what was the correlation you expected to see? And how did that differ from what you actually saw?

MS. VOEVA-KOLEV: I don't think that we expected to see the correlation differ because, again, this is not the volatility. It is not intraday volatility. This is just a very broad view of volatility from settlement price to settlement price. So we were happy to see that the information from the fundamentals kind of trickled to what happened in the market every day, but I don't think we expected to see a very different outcome.

CHAIRMAN GORELICK: John?

MR. LOTHIAN: Did you look at automated trading by participant type, whether commercial or professional trader or retail trader or any of those categories?

MS. VOEVA-KOLEV: No, we did not. We did not differentiate between any of the participants.

Everybody was included.

MR. LOTHIAN: Okay.

CHAIRMAN GORELICK: Brad?

MR. LEVY: Thanks.

You talk about currencies, equities, and financials being similar in level of automation because of the low basis and connection to the cash underlier but then financials seemed to be a bit different as well because of the nature of that market as larger trades, institutional. Was there any more work done there or expected to be done there on that difference between the financial side versus equities and currencies and understanding how that larger order size impacts in even certain environments that are higher-volatility? And what might the differences be?

MS. VOEVA-KOLEV: We have not studied that, but that is a very interesting idea. And we would probably follow up. Thank you.

MR. LEVY: Thank you.

CHAIRMAN GORELICK: Paul?

MR. CHOU: In terms of resting time and limit orders, did you look at, you know, the various tick

sizes that different markets might have, you know, in the sense that larger tick sizes, people might just hold it a lot longer, just, you know, where small tick size is, the resting time would likely be shorter, just one comment?

MS. VOEVA-KOLEV: We did not look at that but thank you.

CHAIRMAN GORELICK: Aubree?

MS. GREENSPUN: So I am just looking to further refine my understanding of the data set. So when we talk about orders, I am assuming that also included quotes.

MS. VOEVA-KOLEV: I am sorry. Can you please say that again?

MS. GREENSPUN: When you talk about orders, I am assuming that also includes market-maker quotes. Do we not? Are you not differentiating those in your data set?

MR. NUNES: That is not really a thing on CME on the futures side.

MS. GREENSPUN: Okay. So you don’t?

MR. NUNES: So it is order-based.

MS. GREENSPUN: Okay. And, then, lastly, as far as the data set, when we talk about orders, are they all outright orders, looking at seeking liquidity in the lit market or does that include the block orders as well?

MS. VOEVA-KOLEV: It is outright implied and also spread implied.

CHAIRMAN GORELICK: Okay. As we go forward, I would like to ask everyone to introduce themselves when they first speak and also to speak a little bit louder. I am getting some feedback that some of the sound is a little quiet. So Larry?

MR. TABB: In terms of timeliness, your granularity is pretty -- you know, at the low levels, it is kind of hard to really understand. Do you have better time granularity than seconds?

MS. VOEVA-KOLEV: No. I mean, the data does, but it was very hard to put it in the graph and, you know, show it on a yearly basis.

CHAIRMAN GORELICK: Bryan?

MR. DURKIN: I don’t have a question. I have more of a comment and a compliment to the Commission

staff. I think this report is very important to have concluded what we around this committee for a number of years have emphasized, which is this is a natural evolution of these markets. The efficiency of these markets, the analogy that you did to validate that you were not seeing any impacts to volatility or creation of volatility by the increased usage of automation I think is a very important point to have been able to conclude in this report because that has been a topic of I think misinformation that has circulated out there from time to time. So it is a great credit to you and your team for being able to do a factual representation of what has been occurring in the evolution of these markets.

I also think that it just ties into the great work of this group. And I know Richard will hear this again, but, you know, we started down this path probably 11 years ago as a unit of market participants in developing systematology and capabilities that we have had in place in anticipation of this continued evolution of these markets. When we started this whole process with this review, it was really in response to

the IOSCO recommendations in terms of having certain protocols in place, to which this Commission has led the charge in that regard in the context of the best practices and the capabilities that we have in place that I think have also been analogous to the great performance of these markets as they continue to evolve and continue to be more automated.

CHAIRMAN GORELICK: Thank you, Bryan. I will echo that comment.

I think this is a great use by the CFTC of empirical data. And I really am happy to see the CFTC acting in this role of an expert regulator to really get into the data and understand what we can learn from the market. So thank you very much for the presentation.

MS. VOEVA-KOLEV: Thank you.

CHAIRMAN GORELICK: So before we move on, is there anyone on the phone who would like to weigh in on this one?

MR. HEHMEYER: So, Richard, quick question. This report is now public?

CHAIRMAN GORELICK: Yes, it should be. Thank

you.

MR. GUNEWARDENA: It will be made public shortly.

MR. HEHMEYER: Okay. Thank you.

CHAIRMAN GORELICK: Okay. With that, we will move on to the discussion from the Automated and Modern Trading Market Subcommittee. I will turn it over to Adam, Alex, and Bryan.

MR. DURKIN: The subcommittee has continued to spend a great deal of time looking at, as we were requested to do so, the evolution of these markets. The IOSCO proposed, you know, recommendations that were recently issued, taking a good look at the various protocols that we have had in place over the years. And speaking, you know, on behalf of my fellow colleagues, you know, we feel very strongly that the model that we have had in place that the Commission has continued to support is the development of a principles-based approach to having the appropriate risk management protocols in place.

The focus of the IOSCO report has been, you know, very specifically tied to having protocols in

place to deal with velocity in the markets. And I think it is fair to say that, you know, we as a marketplace at the CME group and constituents around this table take a very holistic approach to this. And that is one element of ensuring the integrity of a marketplace and having protocols in place that deal with the practices on the front end as orders are entered into the system, the responsibilities in terms of those market participants entering those orders, having the appropriate risk protocols in place on the front end on the part of the exchanges in terms of having their automated systematology in place to preserve that market integrity as those orders reach the platform and providing the marketplace with a robust set of controls, whether it be on pre-trade or post-trade basis, for the marketplace to be able to respond to and take appropriate corrective action should there be, you know, a situation of concern and then continuing to evolve those capabilities as these markets continue to evolve. So I think we all feel very strongly that, you know, the process and the approach that we have taken collectively is the right

approach in terms of being standard bearers in evolution and making sure that these controls and these capabilities continue to evolve with these markets.

MR. NUNES: So I think the only thing I would add, we did discuss that with respect to SEFs. And, you know, Bryan alluded to principles-based approach. You know, we did discuss that the market structure on SEFs is significantly different from the DCMs that we see, you know, with such a high degree of automation and that, you know, the pre-trade controls are likely to be different. But if we take a principle-based approach, they can be applied in the appropriate manner based on the market structure of the SEF.

MR. STEIN: So I would just add the small point that the established liquid markets in the SEFs work very well and as we evaluate options to bring better oversight and integration of the less-liquid one-off trades, that we don’t undermine the liquidity and the well-functioning nature of the current market.

CHAIRMAN GORELICK: Okay. Thank you for that discussion.

I just want to kick it off to the

subcommittee and to the committee here to confirm sort of Bryan's statement here. Does the subcommittee feel that the major U.S. futures exchanges generally adhere to these IOSCO principles that we have been talking about?

MR. DURKIN: Well, speaking for the exchanges, yes, we absolutely do.

(Laughter.)

MR. DURKIN: In fact, you know, I would say we have led those efforts. And, you know, clearly that is something I think for the U.S. markets to be extremely proud of and for the CFTC to be extremely proud of because the things that were outlined in that report are mechanisms and, you know, guidelines and programs that we all collectively have developed over the years and have adhered to and have led those efforts. So yes.

CHAIRMAN GORELICK: Good. Thank you, Bryan.

From the rest of the group here, were there any thoughts on this discussion that we have heard today?

(No response.)

CHAIRMAN GORELICK: Okay. So to just briefly summarize, I think what I am hearing from the subcommittee, that the U.S.-based exchanges are today complying with the IOSCO principles, that the SEFs present some -- because of the different trading mechanisms, they present some unique questions around these mechanisms as well.

Are there exceptions or areas on the SEFs that require special handling, things that would be distinct from the IOSCO principles, as we see them applied on the exchanges?

(No response.)

CHAIRMAN GORELICK: Okay. Maybe that is a topic we need to continue to consider in the subcommittee going forward.

So, with that, I would open it up to questions from anyone on the phone or, otherwise, I think we are prepared to move on.

(No response.)

CHAIRMAN GORELICK: So I thank you very much to the subcommittee.

I think we will arrange for a quick shift

here. And in a few minutes, we will pick up with the Virtual Currencies Subcommittee presentations. Thank you.

MR. GORFINE: Okay. While we are actually switching panels and presentations, we will take a five-minute coffee break and then reconvene here in about five minutes.

(Recess taken.)

CHAIRMAN GORELICK: I think we are going to get started here. We have got two very detailed and extensive presentations here this next segment that I would love to give the appropriate amount of time to. So I would now like to turn to our next panel, in which we will hear from our Virtual Currencies Subcommittee members Mr. Gary DeWaal and Mr. Peter Van Valkenburgh and guest speakers Mr. Charles Mills and Ms. Kathryn Trkla, who will discuss the recent American Bar Association publication that provides a comprehensive survey of the regulation of virtual currencies and other digital assets. We will then open up the conversation to the TAC membership to explore next steps for the subcommittees and its work.

With that, I will turn this over to Mr. DeWaal.

MR. DeWAAL: Thank you, Richard. And I might note that until at least a couple of days ago, Richard was co-chair of this subcommittee, departed off on a trip to Cuba. The next thing I knew, I was running this thing alone. So thank you very much, Richard, for that opportunity.

Thank you, commissioners, for having us. Thank the rest of the TAC members. And, of course, thank the audience for all being involved in these important conversations.

And, again, without being repetitive -- of course, it is repetitive -- this is fast. It is great. But the CFTC has a Technology Advisory Committee. It is so consistent with the chairman’s objective of being a Twenty-First Century regulator, emphasizing technology. And, you know, I personally appreciate being a part of this process.

The subcommittee has been spending time trying to understand and trying to make recommendations related to potentially where the Commission may be

going in approving other derivative contracts. Currently, there are approvals on derivates based on Bitcoin, but there is certainly interest in seeing approvals of other derivatives based on other cryptocurrencies through the self-certification process as well as, obviously, new applicants.

And so we were very, very interested when the CFTC launched its RFI on Ether. And, of course, we read with great enthusiasm many of the comment letters. And, as we review the comment letters, one of the hot topics that seems to be addressed was the whole issue of the fact that Ether is likely moving from a proof of work to a proof of state consensus mechanism sometime this year. And we thought it would be helpful to better understand what that is. There seemed to across the board a little bit not clarity in some of the answers.

And Peter was kind enough to offer to help explain it a little bit better, talk about, you know, some of the controversies, more secure, less secure. And so, hence, I am going to shut up and let Peter take over and give some real valuable insight.

MR. VAN VALKENBURGH: Thanks, Gary. Thanks to the commissioners and the members of the TAC for having me.

So consensus mechanisms, it is a big-looking word. It is not exactly something a lot of people who are more comfortable with financial markets are going to be comfortable discussing necessarily because it comes from the world of computer science. And these are the foundational revolutions behind cryptocurrencies that I am about to describe. And because of that, it is helpful to start with a meme and a little bit of background. Why do we have cryptocurrencies? Why do we have open blockchain networks? What is their purpose? Because their purpose informs the mechanisms and the designs of those mechanisms that power them.

So just a quick review. Cryptocurrencies en masse, they take centralized services, and they turn those services into peer-to-peer internet protocols. So if you think about your email, there is no company that runs that. It is something that is an internet protocol, the simple mail transfer protocol, and allows

you to send an email from one person to another, even though you might use Gmail, she might use Yahoo!, he might run his own email server, although I wouldn't necessarily recommend that in Washington, D.C.

PayPal or Venmo is an example of a centralized internet service that is actually kind of like Twitter or Facebook, which are centralized messaging services, as compared to a decentralized email. And PayPal and Venmo are, of course, ways of paying people across the internet. So the goal of cryptocurrencies and open blockchain networks is to do the things that PayPal does but do them without the company actually running the show, do them as a peer-to-peer internet protocol. And that is really quite stunning. It is really fantastic.

So how does it work? Well, it works with blockchain-crypto-magic, as we all know, which can solve most of the problems that we are all facing in our lives. What I really mean is it works because of peer-to-peer networks and consensus mechanisms. Now, I am not going to talk much about peer-to-peer networks today. Suffice it to say that you may think of a hub-

and-spoke model of communications where everyone is kind of talking to a central node and then they relay the messages outward, to the edges. That is not peer-to-peer networking. Peer-to-peer networking literally means that this computer could potentially through the internet form a direct connection with any other computer in this room, and they could all connect to each other and propagate messages through the entire network without relying on any one participant.

Consensus mechanisms, however, are the topic of the presentation I am going to give today because they are even more complicated in many ways.

So, just to remind you -- and if you have seen me present before, this slide might look familiar. If we are talking about decentralized applications or decentralized services, money is the simplest one to probably use as an example, but we could talk about identity or file storage or other things. And it basically looks like this. In the normal traditional centralized paradigm, you have got a company like PayPal that does a bunch of things for its customers or its users. And that is things like checking passwords

and login credentials, keeping track of who has paid who, managing their employees to make sure everyone is working together to make this service as good as it could possibly be.

Now, how do you take that and take the company out of it and put it into a peer-to-peer network? You basically need to automate those three big services. And that automation is the process of getting every computer to agree on essential data to the service. And that process of getting all of those computers across the internet to agree is the process of consensus. So when we talk about consensus mechanisms, we are talking about the actual technology to get all of the computers to agree on the sorts of things that PayPal would otherwise be in charge of setting as rote.

So what are these things? Well, the first thing to point out is that, of course, this is distributed ledger technology. This is a particular type that uses an open network. And what that means is copies of the data that is essential to the consensus, the data that we actually are trying to reach consensus

over, is stored redundantly on computers all over the world. Every computer on the network gets a copy of the ledger. And that is very important and gives us some great and kind of neat resiliency features because, unlike having centralized servers, you could imagine one computer being somewhat malicious, hence the horns, or another computer going offline because of some catastrophe or just the loss of electricity. And, yet, the network as a whole is fine because there are copies of this data stored on hundreds, if not thousands or tens of thousands, of other computers. Fault tolerance is what we are talking about here.

Now, another thing to point out is I have a stylized version of a blockchain here or of a block in the blockchain. And you see I have got timestamps. Now, the fact of the matter is we don't actually have a good way of knowing which transaction comes before which transaction if we just have a big, long list of them. And that is because if we were going to actually timestamp each transaction, we would need to rely on a centralized party to do the timestamping. You know, you would need to rely on the United States Government

perhaps to do the timestamping or you would need to rely on a corporation. And that is simply not how we want to build these systems with a single point of failure.

So blockchain and open blockchain networks, instead, we don't timestamp necessarily every transaction. But we can reach consensus over whether a batch of transactions happened before or after another batch of transactions. And we call these batches blocks in the terminology of cryptocurrency, and they are, of course, blocks in the blockchain. And the reason why we can have all of these computers agree that one block happened before another is that a piece of data from the previous block must be used to build the next block. And, really, what you are doing is you are taking all of that data, that previous block, and running it through a mathematical function called a hash function, and taking the output -- the output is just the answer to the equation, if you will -- and putting that output in the next block. The only way to create that output would have been to have that initial data. So you know that if you see that output in the

end of this chain, it must have had the inputs from the previous block, which must have had the inputs from the previous block, which means we know that that block happened after those previous blocks. It is just a really rudimentary way but a foolproof way of ensuring that we have an order that everyone can agree on. So we run this data through a hash function.

And we can actually calibrate the difficulty of how expensive in computing cycles and electricity it is to run that hash function. We can make it more or less difficult to suit our needs. And because it is difficult, it gives us another neat little feature. We can have every computer on the network that wants to -- we call it mining, but it is not the best term -- mine the blockchain run that hash function. And the first person to solve it -- it is sort of like an open-ended math problem -- will be the person that the rest of the network will recognize. So, again, this is part of finding consensus. The first person to solve the equation will be the consensus, the member of the consensus, who will be recognized as authoritative for writing the next block. And so this gives us what you

can think of as a provably fair lottery. Now, there are other blockchain networks, permissioned blockchain networks, or social graph blockchain networks, where the participants are previously identified by a scheme organizer. So we don't need to have this hash function base provably fair lottery because you could basically have everyone have a name on the network and put their name in a hat. And then you pull the names out. And that is how you go around and pick who is going to make the next block. But these networks are open networks. And we can't trust everyone to put in a name, honestly. So we have to have some other mechanism of setting up this provably fair lottery of who is going to write in the next block.

Now, another thing about my stylized version of the blockchain, there are no real names in the blockchain, like my version here. And the transactions are going to be in the cryptocurrency described by that blockchain, so not dollars and not Vitalik, but, rather, a public key transferring a Bitcoin to another public key. And these public keys are basically the addresses where you get paid, and your private key is

something kept on the device that generated the public key that allows you to sign the transactions. And those signatures are what guarantee that the person sending the funds is the person who actually received the funds in the past, they are not trying to send someone else's funds.

And who checks all of these signatures? Well, our lucky miner, who was the first to solve the hash function, they are going to announce their winning lottery ticket, effectively, to the rest of the network, "Hey, I solved the function. Check it. Make sure that I am right." And they are also going to share with the rest of the network the signature data from the transactions in the blockchain. And the network is going to check all of that. And this is what prevents people from double spending, prevents people from putting transactions in the blockchain that would be fraudulent, spending other people's money because when this one miner announces this block, they don't have complete power to put whatever they want in that block. It has to obey the rules of the consensus mechanism, which include only transactions with valid

signatures. And so everyone else in the network checks those signatures and checks the hash or the work that the miner did.

And all of this comes together to form what we call a proof of work consensus mechanism, the thing that Bitcoin uses, the thing that Litecoin uses, a whole bunch of other cryptocurrencies.

Now, you might ask yourself, why do all of this work? Well, you get to give yourself a reward, also based on the rules of the protocol. So in Bitcoin right now, you are allowed to give yourself 12.5 new Bitcoins if you win this lottery and form the next block. And you can give that as a transaction to yourself that has no originator. It is the only time you are allowed to send Bitcoins that don’t come from somewhere because this is the money creation feature in that network.

And, again, if the miner wanted to do something malicious, say give themselves a bigger reward than 2.5 (sic) Bitcoins, which is currently the specified number in the protocol, the rest of the network would see that block, check that work, and say,

"I'm sorry. You can't give yourself that big a reward. You are breaking the consensus mechanism's rules." And so in this case, the block is fine. And this is why the miner did all of this work, this computationally expensive, electricity-expensive-type work. It is because they wanted this reward. And they could also collect fees from transactions in the block.

Now, it is important, it is really critical, to point out that this is an open consensus mechanism, again, different from, say, a permissioned blockchain, as I described earlier, where all of the participants are identified beforehand, or a social graph consensus mechanism.

So what do we have in an open network? We have the possibility of writing the next block in the blockchain. Who can do that? Quite literally, anybody. Anybody who has free software and an internet-connected computer can run this hash function based on the prior data in the blockchain that they can freely download. And if they are lucky, they will win. And their proposed next block will be the one chosen to be added to the blockchain.

And it doesn't matter if this is the first time you have ever turned on your computer and happened to install the software. There is no gatekeeper. There is no one you have to seek permission from. You can mine, too, now if you want. You can help build the blockchain. And this means that these networks can potentially get very big, hundreds of participants, thousands of participants, who are all maintaining the data. And they are open-ended. They can get even bigger. More and more people can join. And that just adds to the resiliency of the system. We have got more people checking other people's work. We have got more people so that if one computer goes down or maybe even a whole country's worth of computers go down, then network is fine. That is pretty revolutionary.

And, of course, different people if they think they are really good at this mining thing might decide to specialize in it, get really good at it, invest more money in their computers that they are going to dedicate to mining. So some participants might be more powerful than others as far as the number of hash functions they can run on their computers at

any given time, as represented, somewhat comically, by my moving gears.

So what does this mean? It means that sometimes if more people join the network, more computing power is dedicated to the network. The network is speeding up. They can solve these hash functions more rapidly. And that could potentially lead to a problem because you can think about the hash function as basically just sort of like sitting and flipping a coin and you want to get heads-up 10 times in a row.

Now, if any one of us started doing this, we would be here for a very long time. But it is an interesting fact from statistics that if every person around the world, all seven billion, started flipping a coin at this moment, about 1,000 people would get a run of heads-up 10 times in a row on their first try. So, in other words, more people solving this function, more people performing this action means you will get the result you are looking for faster. So blocks would start coming around more rapidly if more people were dedicating computing work to solving these hash

functions. And we don't want that.

Bitcoins block times. So the times we want blocks to come around, we want it to average about 10 minutes, a new block every 10 minutes. That is, again, part of the consensus protocol. That is something that helps computers agree. If blocks come around too quickly, we run the risk that half the network might start building on one block that the other half of the network hasn't heard of yet because of just the delay in sending a bunch of data over the internet from, say, North America to China. And this would be a problem if Chinese miners and American miners are mining on different blocks because then you get a divergent history of the world.

So we really want to make sure blocks come around more slowly than as fast as possible if you -- and so with Bitcoin, the difficulty of the hash function simply adjusts automatically if blocks have been coming around too quickly or too slowly. Basically, it says that, all right, if all of the world is flipping coins, there is going to be 1,000 people in the first try that get it. We just want one person.

And we want it to take them about 10 minutes. Now you need to flip a coin and get heads-up 20 times in a row or 30 times in a row. Someone will still probably crack it, but it will take longer and, vice versa, if blocks have been coming around too slowly, we make the problem simpler, heads-up 5 times in a row, instead of 10 times.

And this is actually a very accurate metaphor. We are not going to get into the actual hash function, but coin flipping and looking for a string of heads, instead of tails and a mess, is really right on target.

So that brings me to the next thing I want to talk about, which is in these proof of work consensus mechanisms, what does the mining hardware look like? And what is this term called “ASIC resistance” that we have heard about from some proof of work consensus mechanisms? So, again, this is all just a way primarily of setting up a provably fair lottery to pick who is going to write the next block in the blockchain. And this is actually a quote from the Bitcoin white paper. This is a screen grab from Satoshi’s white

paper describing Bitcoin. And this is a brilliant document. I would just like to point that out first before I criticize it. This little highlighted bit here says, “Proof of work is essentially one CPU, one vote. That idea that Satoshi had was that this would be a very democratic and open system, where people running normal-looking desktop computers around the world would all be participating somewhat equally, one CPU, like that CPU; one vote.

And the reality is a CPU is good at doing just about everything, but it is not great at doing anything specific. It is a general-purpose computer. And the bottom line is once Bitcoin started becoming valuable, people thought, “Okay. I could do better than this. I could use a more specialized type of computer. And I would be able to solve more of these math equations while using a little bit less electricity per equation. And then I would be outcompeting other people who were mining.” And so rapidly we saw the change in Bitcoin miners from desktop computers to sort of these fan-made or hobbyist-made devices that use GPUs or graphics cards.

These are the things that you are going to want to put in your computer if you want to play Fortnite or you want to play a game, you want to play something that has got a lot of rich graphics in it and you don't want it to run slowly.

Now, it turns out that the chips that are good at rendering those videogames are also really good at solving SHA-256. So if you stack a bunch of them on a rack -- and this is a shoe rack that we bought at Amazon. This is a Coin Center office. We have got this fun little GPU rig we built a number of years ago. If you stack a bunch of these cards on a rack, you can solve these equations a lot faster than just a normal CPU.

And then things got even more specialized. So this is already specialized hardware, but you could buy this at Microcenter or wherever.

This is what Bitcoin mining looks today. And this is an ASIC mining farm. This is basically a big server warehouse. And on every one of those racks are a bunch of these, which are application-specific integrated circuits. They are chips that are printed

silicone to do only one thing. They can't play videogames. They can't play Microsoft Word -- play Microsoft Word. Sometimes it feels like that when I am writing papers. All they can do is solve the SHA-256 hashing algorithm, which is that coin-flipping procedure, as I described it earlier. And so they are really efficient at doing just that.

Now, what does this mean from a consensus mechanism standpoint? Is this a good thing? Is this a bad thing? People worry about mining centralization. So this is, of course, not quite Satoshi's vision. Satoshi's vision was a bunch of people with CPUs, desktops, their own computers. And these things are expensive and have to be purpose-built in chip foundries. So what it does mean is that only a handful of people, as compared with before, are going to have the resources and the inclination to actually mine Bitcoin. So that might be a con, but there is also a pro here.

The pro here is that these things are really costly. So if you want to competitively mine Bitcoin, you are going to have to sink a large amount of capital

into the computers and the devices that you need in order to run a Bitcoin miner. And you are going to need to pay a lot of electricity to do it. And this is actually a pretty good security feature. It means if somebody wants to attack the network and they want to obtain a majority of the hashing power on the network so that they are always chosen as the next one to make blocks, they are going to have to dump an incredible amount of money into buying these chips, which can only be manufactured in certain places around the world. And if they tank the price of Bitcoin because they attack the network, which would be the logical outcome, they have just lost their entire investment in the hardware because this hardware doesn't do anything except mine Bitcoin. So there are some neat economic incentives.

Now, of course, that wouldn't protect against someone who wasn't economically motivated who just wanted to attack it for the lulz and had somehow a whole lot of money, but, again, we have got pros and we have got cons here.

On the topic of 51 percent attacks generally,

I just want to say a couple of things. So 51 percent attacks are really not a logical way to attack a large, well-capitalized cryptocurrency. It would be much better to just sort of DDoS or spam the computers on the network, although it is pretty resistant to that as well. And that would be a much cheaper attack. And we see that, and it is not actually usually much of a problem in the Bitcoin network. But a 51 percent attack, where you are really trying to develop and cultivate all of that hashing power is just too expensive. It is a tremendous cost.

Even Google, if they pointed all of their machine-learning servers to mine Bitcoin, it is not the right specialized hardware. So they are working at a disadvantage. And they actually just probably wouldn't have enough of it. So even the massive cloud computing companies of the world wouldn’t be able to attack Bitcoin, at least as currently specified, unless they have something I don’t know about.

Now, 51 percent attacks are a real threat to poorly capitalized or small cryptocurrencies that happen to share a mining algorithm with a larger

cryptocurrency. And this has been evidenced recently in the 51 percent attack on Ethereum Classic, which is a fork of Ethereum, but it is a separate network. And this was a confusing thing for a lot of people. In the news, you saw reports, “Cryptocurrency is not as safe as you thought, 51 percent attacks much more possible.” The bottom line is they are not any more possible with respect to Bitcoin or even Ethereum. But for a small cryptocurrency like Ethereum Classic, they are a real threat. And here is why.

Most people -- so Ethereum and Ethereum Classic use the exact same hashing algorithm in order to choose who is going to make the next block. It is different than Bitcoin, though. And so most people who have computers that are good at running that hashing algorithm, they want to mine Ethereum because it is the more widely used network and the tokens are more valuable and you will get more fees because there are more transactions happening there. So most people are using that hardware to mine Ethereum. But if you are like a middling-sized Ethereum miner and you decide, “Hey, if I switched over to suddenly using my computers

to mine Ethereum Classic," which is easy because it is the same type of hardware that is good at that, "I would suddenly be a huge Ethereum Classic miner." So you go from being a small fish in a big pond to being a big fish in a small pond. And that means that for that moment when you switch over your hardware to mine Ethereum Classic, you could potentially have all of the hardware necessary to 51 percent attack that network, but it wouldn't work in reverse. Do you see what I mean? This is really a question of smaller or more poorly capitalized cryptocurrencies being vulnerable because there is a bunch of miners already hanging out out there who at any moment could join the network and really unbalance the number of persons who are mining.

And that brings me mercifully to proof of stake. Proof of stake, of course, came up frequently in the Ethereum RFI. And I think that the questions from staff and from the commissioners and in the RFI in general have been excellent. And it is an important topic. So I want to give you just a base of knowledge again. And we had to start with proof of work because the easiest way to understand proof of stake is really

the same. We are still trying to build with proof of stake systems a provably fair lottery for picking who is going to be mining the next block or creating the next block in the blockchain.

And so the question is, in a proof of stake system, how do you get a lottery ticket in order to have a chance to participate? So, of course, in proof of work, your lottery ticket was the calculations your computer was doing. And if you solved that calculation, that proof of work function, you have the winning lottery ticket. We don't have these calculations in a proof of stake system. And this is part of the goal, as stated by Commissioner Quintenz, of Ethereum's move to proof of stake, is to reduce some of the energy usage of the system, so no calculations. How do we provably fair pick somebody amongst this network to make the next block? And how do we make the lottery ticket costly? Because if it was free, you could just claim to have a million lottery tickets. And you are going to do a lot better than someone who is honest and said they only have one.

Well, we make the lottery ticket costly

because you will have to sacrifice the time value of money, specifically the time value of cryptocurrency. And what do I mean by that? Well, in order to have a chance to be the miner for the next block, you need to point to the blockchain that you are working on and point to a transaction in the past where you decided to stake or immobilize some amount of cryptocurrency on that blockchain. And so that is a sacrifice. That is saying, “I am not going to be able to access this. I am going to hold it. I am not going to use it in transactions or for other purposes.”

And so that sacrifice is the same sacrifice that we would want in a proof of work system, where you are sacrificing electricity. Instead, you are just sacrificing accessibility of money or the time value of money.

And so if you stake more, so, for example, this person staked 95 coins in a block previously, you will have a little bit more power. Just as if you run more computers, you would have more power in a proof of work system. And so, again, the participants are going to be lumpy. Some of them are going to stake more.

Some of them are going to stake less. And the probabilities should be provably fair. The more you stake, the better chance you have of winning the lottery. It is like buying a bunch of tickets. And there is still a random function to pick the winner, but you increase your odds if you stake more. And every time the blocks come around, in Ethereum, it is only about 10 to 15 seconds, as opposed to 10 minutes in Bitcoin. Somebody will be chosen as the next block maker based on this provably fair lottery.

Now, this does lead to some issues from a consensus mechanism design standpoint. I am not going to go too deep here, but I think you should be aware of them. And they are all probably addressable, but there are issues, nonetheless.

The big one is the nothing at stake problem in proof of stake consensus mechanisms. And this is hopefully an explanation that you will be able to follow pretty readily.

So take our miner who staked these coins in block -200. So I am changing the blocks to negative numbering from the present. So this is a block 200

blocks ago. 1XT03 staked 95 coins and signed so that we know that they are theirs, they are not trying to stake someone else's, with their private key. That is what gives them power on the network. Correct? That is what basically is the equivalent of them having gotten power on the network by mining. They have immobilized some coins.

Now look at block -199. Our same staker has now transferred those 95 coins to someone else on the network, probably not them. So they should rightfully lose their staking power. They will go from being someone with 95 coin power to someone with less because they are not staking those 95 anymore.

But what if they do this? They create 200 blocks from that -200 block. And you might think, well, how could they do that? That is a lot of data to create out of thin air. Well, not really. They just have to take a copy of the existing blockchain, and then they can remove the transaction where they sent the funds to somebody else. And then they present this to the rest of the network as what they think should be the authoritative copy of the ledger. And, remember,

they have got 95 staked coins. So depending on how many coins other people have staked, that might make them powerful. That might make them likely to have their version of the blockchain chosen as the authoritative version, rather than the one that involved them transferring the coins away. And that is a kind of an attack. They convince the rest of the network that they sent the coins away, but then they use their staked coins, which were no longer staked to have power on the network, hence this name for this attack, the “nothing at stake problem.”

And it could get even worse. So our miner could basically say, “Hey, I have got all of these wallet addresses that are now empty, but they were only empty after block 200. Before block 200, they had a lot of coins in them. And then I transferred them away or maybe I will even go and buy private keys from people, people who thought that their wallets were empty because they were, but sometime before block 200, their wallets were full.”

And so you have those private keys. And you could buy them probably cheap because why would anybody

want to hold onto private keys for a wallet that doesn't have any funds in them anymore? And you could credibly make a transaction where you accumulate all of those wallet addresses, and you sign a message saying, "I am staking 2,000 coins now."

Now, in your version of the future, you are just staking those. In the real version of the future, you gave them up or never controlled them. So, basically, this is a way to present to the network that you have a lot more power than you actually do. And that is a problem.

Now, this is surmountable, but this is also a real problem. So Peercoin was the first proof of stake consensus mechanism-driven cryptocurrency. And it ran into exactly this problem of the nothing at stake problem. And it was attacked.

And what they came up with as a stopgap measure was checkpointing. And checkpointing works like this. You say that we are going to regularly as part of the consensus mechanism say that "This is now an established block. We can't have a new proposed blockchain that would reorganize blocks earlier than

this block. It is just a checkpoint. So this block now can't move. And so we put this checkpoint, say, here. And this would invalidate this kind of an attack because this miner went too far backwards in the blockchain in order to provide an alternative history or an alternative future where they are more powerful. And so this prevents this kind of attack where you are able to reach back deep into history and present as more powerful than you actually are.

This does lead to a certain question, who does the checkpointing? Again, we don't want a centralized party to do the checkpointing. And in Peercoin's original design, when they were faced with this problem, it was literally a checkpoint that was established by a signature from a public/private key pair that was held by the developer of Peercoin, just one person. And so that is not really decentralized. It still was fine because they weren't doing anything malicious, but do we really want to have that single point of failure in the system?

In Ethereum's Casper Protocol, for example, as proposed, that checkpointing would happen every 100

blocks, which sounds like a long time, but, again, Ethereum blocks come around every 10 seconds or so. And it would happen whenever two-thirds of the validators in the system all agree on a block. Then it will be checkpointed.

So this raises some interesting implications potentially for market participants having to do with finality of transactions. And this hopefully is a payoff where we can start thinking about some of the regulatory implications and, really, just the implications for market participants and how they can self-police and have good policies inherent to themselves to prevent these kinds of attacks from causing losses and things like that.

So in a proof of stake system, you may need to wait for transaction finality until the transaction is in a block that is prior to one of these checkpointed blocks because at that point, it is no longer vulnerable to this kind of nothing at stake-type attack; whereas, in a proof of work cryptocurrency, there is no checkpointing. So, in theory, the entire Bitcoin blockchain could be rewritten at any moment's

notice, but we don't worry about that because merely rewriting two or three blocks would require an astronomical amount of computing power, really. And when you get to five or six blocks, it is just crazy.

And so the rule of thumb here is proof of stake, you are probably going to want to wait until a checkpoint in the consensus mechanism. Proof of work, you are going to wait until a transaction is in a block old enough that the computing effort to re-create the chain since then is cost-prohibitive, which on average for Bitcoin, just to give one example, is about six blocks, but every blockchain and every proof of work implementation might be different.

And that brings me to my final topic, which I promise to be fairly brief on, which is forks, forks. So consensus mechanisms are designed to prevent forks amongst participants, but they are only designed to prevent forks amongst participants who want to stay together. They love each other. They want to be there. And so under normal conditions, where all of the people who are using Bitcoin want to stay together, forks and reorganizations can happen briefly because,

as I said, maybe the North American networks get out of sync from the Asian networks, just because of the lag over the Pacific Ocean for transoceanic cables or things like that on the internet. But they will resolve quickly. And that is again why, that is another reason why, you might want to wait three or four or five blocks to make sure your transaction is really going to be permanent. You didn't accidentally get stuck in a block that was incorrectly built on by part of the network that got out of sync. It is a pretty surmountable problem. It is not really a real deal killer.

Now, there is another type of fork that people talk about, rather than these little hiccup-type forks. And this is where a group within the community, so some subset of Bitcoiners, for example, people running the computers, they fundamentally disagree with the rest of the Bitcoin community, the rest of the people running the Bitcoin computers. And they don't want to stay together anymore. So they get a divorce. What they do is they fork. And what they are doing, really, fundamentally is changing their consensus

mechanism rules so that they are no longer compatible with the consensus mechanism rules of the original protocol, of the original network. And from that day forward, their computers will only talk to theirs and Bitcoin's computers or the original's computers will only talk to theirs.

And this may seem like a real issue, but in this situation, we don't really have a big problem of confusion and a question of whether transactions are going to be final because in this situation, we now actually have two completely different assets. You have Bitcoin, which is the thing on the original version of the chain; and you have this new thing that decided to fork off. And there might be marketing or branding confusion. Is it Bitcoin Classic? Is it Bitcoin Cash? Is it whatever? And eventually communities will settle on these names, but you really have two distinct assets.

And so what is the best approach to that for an institutional participant, for a market participant? I will get to that in a second.

So, mercifully, I am now at a sort of round-

up part of the presentation, implications for traders and funds for market participants. So this proof of stake/proof of work question, how fundamental is it? It is generally not relevant. Again, proof of stake is just another way to build a provably fair lottery for block creation.

Now, yes, it may impact some of the best practices for finality that we would want to see amongst market participants. So in proof of stake, for example, you may want to look at the consensus mechanism and think, “Okay. There is checkpointing every 100 blocks in this consensus mechanism. We will wait until a checkpointed block comes around to treat a transaction as final” versus proof of work, where we are just doing it based on computational infeasibility. We know that a reorganization of Bitcoin seven, eight blocks deep is literally more computing power than the world has ever seen three times over. And so we are comfortable with that. And, again, there is not necessarily always going to be a hard and fast best rule here, but that is nothing new to market participants. You want best practices. You want them

documented before a problem happens. And then you want steps to be taken to address problems as they arise, hopefully based on what you specified your best practices were.

And so the takeaway -- I think I just said this. Institutional participants should have documented procedures for how risks around finality will be mitigated. And they should be specific to the consensus mechanism of the asset that they are trading, but it shouldn't be too hard, really.

What about 51 percent attacks? Not a major risk for well-capitalized cryptocurrencies. Again, there are much easier ways to attack networks like Bitcoin. I am not saying they are going to be successful, but it would be lunacy to try to attack Bitcoin by buying a bunch of ASICs and becoming a 51 percent miner. It would just be too expensive. They are a major risk for poorly capitalized cryptocurrencies that share a common mining algorithm with a larger cryptocurrency. So this is the Ether Classic versus Ether situation.

And so the takeaway here is that

institutional participants should be wary of poorly capitalized cryptos. And there are thousands of them. There is this long tale of all of these so-called altcoins out there. And many of them may be based on proof of work, on an algorithm that uses something very similar for hardware as Ethereum or Bitcoin. And in the event of that situation, a couple of Bitcoin or Ethereum miners changing their servers over to mine this little coin, it is going to be like opening the floodgates. That person was a minor participant on the Bitcoin network. They are the whole participant of this little network. And they could attack it. So it is something to be aware of with poorly capitalized cryptocurrencies.

Forks. This is the last one. So well-specified proof of work and proof of stake systems may have occasional unintentional forks, where briefly in, say, again, East Asia versus North American miners, they get a little out of sync. And that is fairly simple to deal with. You just again are going to want to have prudent and well-documented procedures over finality. So because of the fact that sometimes blocks

make it out of sync, we are going to make sure that this block is six or seven blocks deep to make sure that the network really has agreed that this is the official block.

But when a subset of community members reach intractable disagreements, as we have seen with Ether and Ether Classic, as we have seen with Bitcoin and Bitcoin Cash, as we have seen in a lot of cryptocurrencies, there could be a more permanent fork. And that does have implications for traders and funds, for market participants.

But the takeaway is this. Institutional participants should have well-documented procedures, again, that describe how they will determine which fork. I always say, “which fork.” I feel like I should be saying which tine of the fork, but that just sounds crazy and weird, too. So I am going to say, “which fork,” so policies and procedures in place to describe which fork they will honor.

So if there is a question over which one is the real Bitcoin, in other words, they need to document, how are you going to make that determination?

It could be any number of things. It could be the amount of proof of work effort dedicated to one versus the other fork. It could be the market price of one versus the other fork. It could be any number of things. But they should be policies that are stated in place.

And then they also need policies in place to describe what they will do with any windfalls from the other half of the fork. So if your fund was holding a bunch of Bitcoin before the Bitcoin, Bitcoin Cash fork, your fund now also has control of a bunch of Bitcoin Cash. Okay? If you are saying, “We are just going to honor the Bitcoin fork,” what happens with all of that Bitcoin Cash you just got?

It could be a lot of things. And, again, there is no hard and fast best answer here. There just need to be clear policies that protect your fund participants or your investors or things like that. And it could be Bitcoin Cash will be liquidated and reinvested back into the fund in the form of more Bitcoins -- that is fine -- or it could be we will hold both. That is also fine. There just need to be

policies about this.

And that is all I have got. Hopefully consensus mechanisms are a little bit demystified.

CHAIRMAN GORELICK: Thank you very much, Peter. That was very helpful.

Before we open up for questions, I think I would like to turn to Ms. Trkla and Mr. Mills to talk about the recent ABA study that was recently released.

MS. TRKLA: Yes, it is. Thank you, commissioners and members of the committee, for inviting us. We are pleased to be here to tell you about the ABA white paper that we recently put out.

I do have to say Charlie and I are lawyers. So our presentation isn't quite as high-tech as the last one. We have got bold points in color, no graphics, no animation.

We are going to go through the first few slides pretty quickly but wanted to provide a bit of an overview about the genesis of the white paper and first explain a little bit about who we are and the ABA Derivatives and Futures Law Committee first, which is a longstanding committee of the ABA.

Our premier event I think is having our winter meetings, usually someplace warm, where we have, you know, two and a half days of substantive conference panels. We have about 500 members of the committee itself. About, you know, 150 to 200 people have been attending the more recent winter meetings. At the winter meeting last year, Chairman Giancarlo was the keynote speaker. And at the time, there was a lot of discussion about Bitcoin futures and virtual currencies. And that was the primary topic of his keynote address to the group. And in his remarks, he challenged the Derivatives and Futures Law Committee to be more proactive in this area and to be sort of thought leaders in addressing issues in this area.

So, of course, we formed a subcommittee shortly afterwards. And we have about 80 members on the subcommittee. Yes, it is a mouthful but Innovative Digitized Products and Processes Subcommittee, or IDPPS for short, which is much more fun to say. So we are the IDPPS. And we have about 80 -- well, actually, close to 90 members.

And one thing I really want to emphasize is

yes, it is a subcommittee of the Derivatives and Futures Law Committee. And many of us on the committee spend a lot of our time dealing with Commodity Exchange Act- and CFTC-related issues. But, of necessity, we are also involved in securities laws matters and related areas. We also have a number of participants, both in the Derivatives and Futures Law Committee and on the subcommittee, who you would probably think of as very prominent securities Bar attorneys, who also deal often with Commodity Exchange Act issues. And then we also attracted to the subcommittee people who are very expert with Fintech and related areas. So it allowed the committee to draw from broad expertise in our work and projects.

We do have a mission statement. I am not going to read the bullet points, but, you know, two things to draw out: one of our missions is to help educate ourselves as a committee but also to be proactive in educating others about the laws that may, sort of broadly speaking, impact digital assets or use of the blockchain technology. And that also includes looking at where laws may overlap and what issues that

may raise. And so I think the white paper that we put out really exemplifies the mission statement that we set for ourselves.

We have three working groups. And the Jurisdiction Working Group, which Charlie Mills chairs and Jonathan Marcus at Skadden vice chairs, is the working group that worked on and produced the white paper that we came out with. We also have a Blockchain Modality Working Group and an SRO Working Group. So we are looking more broadly at other issues in this area.

As I mentioned, the white paper was prepared by the Jurisdiction Working Group. We had 34 contributing authors, which I find amazing that we got that many attorneys together to produce the white paper, again drawing on the broad expertise represented in the committee, and so 31 attorneys from 16 different law firms. We also had two in-house general counsel who participated and one attorney from the NFA who contributed as well to the drafting.

And the white paper had a specific focus on regulation of cryptocurrencies and other digital assets. And so it is sort of one part of our broader

mission of issues that we are looking at as a committee. And so, as has been mentioned, you know, we have attempted to put together a comprehensive survey of how Federal and state laws can apply to basically the offer, creation, trading, and use of cryptocurrencies and other digital assets. The paper also does include a summary of some of the key initiatives outside the U.S. as well. And we really do intend this to be sort of a comprehensive survey of the regulations that can be a resource to practitioners and to policy-makers.

As mentioned, you know, we have got other working groups within the IDPPS. And so we are looking at broader issues that are really outside the scope of the paper.

Now I am going to turn it over to Charlie.

MR. MILLS: Thank you, Katie. And thank you, members of the committee and commissioners, for having us. We are really delighted to be able to talk about our paper. We do, as Katie has said, hope it will be a great resource to practitioners. It is not an advocacy piece. It is not saying, “This is what we think should

be happening in the future," but it really tries to be a collection or a guide to what the law is, what positions have been taken by different agencies, and where there might be overlap and conflicts in them.

I will just quickly go through -- this is just a listing of the topics, which Katie has pretty much relayed already. It starts with a discussion of blockchain technology and the different types of assets that are out there that are being traded and being offered to the public. We then have a section on the Commodity Exchange Act and CFTC regulation. One piece of that that I think for lawyers is valuable aside from -- there is a lot of content there, but we do have a chart at the end that shows the breakdown of different products and the jurisdiction of the SEC and the CFTC over those products. I am not sure that that kind of chart presentation capturing the whole thing is in any other publication that I have seen. So I recommend that to everyone.

Section 3 is the federal securities laws, the Securities Act, and the Exchange Act. And then section 4 of the paper covers the Investment Company Act and

the Investment Advisers Act. Just to continue here, on section 5, we do have a discussion of the overlap and conflicts between CFTC and SEC, which we will address a little later today. That is more talking about how possibly where there is friction or there is lack of clarity between the two agencies on how they will approach these markets, how those might be dealt with aside from new legislation.

And then we have a chapter on FinCEN, the Financial Crime Networks Authority at Treasury. And then I might just quickly go through here.

So these are the final ones. We have international regulation. We cover a number of different countries and what their approaches are. We don’t go into depth, but we do talk about MiFID, Switzerland, Japan, Australia, a number of other countries, as kind of a synopsis of where the rest of the world is going in trying to regulate these markets. Then we have state law considerations, principally focused on New York state, which has the most impact today I think on these markets from a state position. And we do have at the end just a survey of what each

state's regulatory regime is or regulations are that can address these markets.

MS. TRKLA: With the survey at the end, the focus, really, is on the state money-transmitter-type laws. So it is a comprehensive survey. We recognize there are other aspects of state laws that can be relevant for this area. And those are some of the issues that the Blockchain Modality Working Group, for example, is looking at.

MR. MILLS: And so here we will just spend a few minutes here because we thought this might be of greatest interest to this group of the CFTC and SEC regulatory schemes and how they overlap. And section 5 of the paper goes into this in some detail, but you basically have where a security underlies a commodity derivative transaction and how does that have -- what happens there, who has control or input into how that is regulated, the situation also where a commodity may, for lack of a better term, underlie a security. And that can be hybrid securities, which the Commission already has rules on. And that was an area that we talk about as an example of how the both Commissions

came to a resolution of how to deal with these instruments without necessarily having to go to legislation. Eventually Congress did step in, but it was really ratifying what the agencies had already done. And part of that is the exemptive powers of both agencies to exempt out certain transactions and effectively cede principal control and regulation of them to the other agency.

And then you have the issue, which we will talk about -- to me, it is the most complicated one to resolve -- which is where the security, where you have a non-security commodity, like a token on an ecosystem that is going to be used to be a medium of exchange to buy services and goods on that ecosystem that is set up by a private company saying, you know, “This is what we will provide to you. And you can use these tokens to buy and sell our products in exchange for that.”

So that token might be considered a commodity. Probably I think the CFTC/the Commission would consider it so. And it would just be a CFTC issue except for the ICO, the initial coin offering, process, where the coins are also offered to raise

capital in order to build out the ecosystem. And so the SEC has recognized and taken a strong position that these are investment contracts and that they would have plenary authority over the offering of those coins in that context to the public. And the question there is, what is the CFTC's role at the time of initial offering? Does it have none or is there a role?

And then what has been also recognized is that these investment contracts can convert into just a pure commodity at some point when the token is just being used as a medium of exchange and it is no longer being used to solicit funds and raise capital from the public.

And, as I am sure everybody knows, the SEC has taken the position that and has referenced Ethereum as an example that this can happen. And you can have something that might have been. They don't actually declare I think whether Ethereum was a security or not, but they are saying you can have it where it is an investment contract. Eventually it becomes so broadly utilized that it is purely a medium of exchange and something that the SEC would no longer regulate. That

is a tremendous problem for the industry and for this marketplace because there is no system today of regulation or anything else that tells you when something would convert and what are the circumstances when that would happen and are there legacy issues. If, you know, you convert an investment contract, it becomes a commodity. If somebody has a claim that the statute of limitations hasn't run on the investment contract under the securities laws, can they bring that claim if it is no longer considered a security? That is just a simple example of how difficult these issues are.

And I will also turn it back to Katie, but I think one of the points that the paper makes is that there probably will need to be if there isn't, really, ongoing formalized processes between the two agencies to survey what these issues are and to try to grapple with them and figure out how to deal with it effectively for the markets and for the public.

MS. TRKLA: Thank you, Charlie.

I want to go back and just add some basic points. You know, one of the reasons or underlying

sort of causes for there being jurisdictional overlap at sort of a nuanced point, we covered it on an earlier slide for Commodity Exchange Act purposes, securities are commodities. And then the statutory framework has allocated, then, which agency regulates derivates on securities. And then, as Charlie mentioned, the other way you can have sort of both agencies interest-implicated is when securities have commodities or derivatives elements embedded in them.

And so jurisdictional overlap issues are not new. There is sort of a long history of those where they have been resolved in different ways between the two agencies. So the particular type of digital asset that Charlie is focusing on that has the sort of unique characteristic where it may start out as a security may also have derivatives or commodities elements at the outset or aspire to have those in the future. It is a different kind of combination that we haven't seen before when sort of the long-term sort of expectation of those offering the instruments is that the securities features are going to be shut over time. And it will be a commodity alone at some future time.

And, you know, as Charlie mentioned, that is an area where I think there is some uncertainty of how you manage that transition from a security that may have embedded derivatives or commodities characteristics to something that becomes a commodity alone. And the current framework seems sort of ill-suited for that when you look at, say, what does it mean if you start out offering a particular coin token in compliance with the securities laws. You will, you know, treat it as an initial offering of securities. It seems to us and what we point out in the white paper is that some of the requirements that then wrap around a securities offering actually would inhibit the transformation, then, of that coin to a commodity.

So far, the SEC has not allowed any public registrations and public offering of coins as securities. And so today, at least, you would be looking at some kind of private offering, but private offerings of securities also have restrictions that attach to transfers of the securities. And those restrictions or perhaps needing the involvement of a broker-dealer under the securities framework would seem

to prohibit the natural evolution, then, of trading of that coin into a non-security commodity. And so that kind of uncertainty seems to have had a bit of a chilling effect in the markets in light of, you know, the various enforcement actions that have come out of the SEC in this area but without a clear sort of framework in place on how you legally can, in fact, offer the coins starting as securities but facilitate the transfer to something that would basically shed the securities features.

As Charlie mentioned, there can also be sort of issues about each agency's enforcement of its antifraud authority if there is a question over whether a particular token is more properly viewed as a security or as a non-security commodity. The way the statutory framework is set up when it comes to cash market trading activities, the statutory framework basically allocates and assumes that if it is a security, the SEC regulates that activity; if it is not a security, if it is a non-security commodity, it is the CFTC that has the antifraud policing authority over those coins. And so when you have coins where one

agency may be taking action or the other but there is a lack of sort of transparency as to the determination is that really a security or not, there may be some vulnerability to someone subject to the enforcement action perhaps saying, “No. CFTC, you don’t have the authority. It is the SEC” or vice versa. So we think these issues of uncertainty also could have implications for the enforcement activities of both agencies and may sort of frustrate those efforts as well.

And so if there is one advocacy point in the paper, it is these issues exist. And we hope that the two agencies can perhaps work together to try and sort them out. We think the marketplace would benefit by having sort of clearer and sort of public standards on these issues.

We should also note that it is possible that certain digital assets may not be subject to either agency’s jurisdiction. You know, one example that gets sort of passing mention in the white paper is if you have an initial creation of a coin and it confers title to a commodity once it is issued in the future,

depending on the terms wrapping around how it is sold and who the participants are, it is possible that may, in fact, be something subject to the forward contract exclusion. For example, if the transaction is limited to, you know, commercial parties participating.

Then on our last slide and what we examine in this part of the white paper is, are there tools available to the two agencies to try and address these issues without need of legislation? And it may well be that some issues may require legislation, but that would also benefit I think from coordinated views and input by the two agencies.

But, basically, we have got, you know, the statutory authority added by Dodd-Frank, the section 718 provisions, which establish a framework for the 2 agencies to resolve and provide clarity on novel derivative products. This was actually an outgrowth of joint meeting of the 2 agencies looking at these issues in a report in 2009, recommending these statutory provisions.

Each agency, of course, has their exemptive authority. And, in fact, the section 718 provisions

contemplate that one agency could ask the other agency in looking at products that may implicate both their jurisdictions and regulatory missions to exercise their exemptive authority. So that is contemplated as part of that solution.

Finally, I would also note that while the white paper focuses on a particular type of jurisdictional issues relating to, you know, the virtual currencies and other digital assets, there are other areas I think where the marketplace would benefit by coordination between the two agencies. You know, we are both mindful that many FCMs are also broker-dealers. And to the extent there may be issues about custody of coins or procedural matters, the FCM BD community probably would welcome sort of harmonized views between the two agencies on how to address those types of issues.

MR. MILLS: Yes. Let me just say one last thing is that we talk about cryptocurrency and digital assets. It is a wide swath of different types of assets that there are. And how you would approach them from a regulatory standpoint may be different. So they

are not like a unified asset class from my point of view.

You have the example of the Dow token, which the SEC found to look more like an equity interest in an enterprise and look more like a share of stock and giving you certain control rights. And then you have Bitcoin, which is totally different from that. And you have lots of things in between. And you will have more things coming forward as businesses try to incorporate blockchain and tokens into their business models and provide different features going forward. And I think that is another forward-looking issue that both agencies will have to grapple with.

Thank you.

CHAIRMAN GORELICK: Okay. Thank you very much for both of your presentations. I think they were both very informative and helpful. And I appreciate the work you have put into it.

I want to open it up now for questions to the subcommittee and to the committee for both presentations. And please address your questions as appropriate. Brad?

MR. LEVY: Yes, a question, maybe an ask. So the three working groups, Jurisdiction, Blockchain Modality, SRO, and the comment on money transmitters being thought of as part of this discussion, I know there is definitely a focus on securities and futures because that is the mandate here. Has there been a thought about thinking about the OCC as also a regulator that may have an interest in this as you get into the broader payments, whether it is just -- you talked about money transmitters.

And, then, normally in a lot of our markets, something is moving against money. Those could be some form of token or some form of new process. And I would think the Federal bank regulators have some interest there. And I know there have been some discussions about trust, state-level trust, regulations as you get into the custody or money movement and some turf discussions there as well.

So have you thought about the OCC more generally in this discussion as a regulator that is brought into the fold in terms of helping the market get some clarity?

MS. TRKLA: That question specifically, no, but I would say that the Blockchain Modality Working Group, that probably has the most sort of amorphous mission because there is a lot that that can cover. And I do see that particular issue as something most appropriate for that particular working group. And I know they have identified a broad range of issues that they are considering.

Now, I should say a number of the people on the Blockchain Modality Working Group also contributed to the white paper. So they took a little bit of a break from the work of the Blockchain Modality Working Group. But now that we are past the white paper, that working group has another meeting scheduled to get back on focus with the types of issues they are looking at. So we will make sure to raise that with them as something to add to the list of things they consider.

MR. LEVY: Thank you. And just Brad Levy, in --

MS. TRKLA: Yes?

MR. LEVY: -- IHS Markit. Sorry. I violated your rule.

CHAIRMAN GORELICK: Yes.

MR. LEVY: And just one. In the panel at 2:15 on DLT, which I am not presenting on but I am on, there will be some discussion about the payments end of things because it is that same point, a very broad discussion. And we do believe there are some angles there for this group.

MR. MILLS: I would say that we very much appreciate hearing topics that are of interest and people would like to have addressed in future white papers. That was what we were trying to do. And there are lots of different regulations across Federal and state authorities. And trying to figure out which of those to capture in one white paper is important. And hearing if the staff or commissioners, anybody at the table here has a desire for certain issues to be addressed, we would be very receptive to hearing those.

MR. VAN VALKENBURGH: Very briefly, I just wanted to add that when the OCC was going through its Fintech comment process, Coin Center filed a number of regulatory comments describing to what extent we think virtual currency activities fit into core banking

activities. If that is of interest to you, I am happy to share that as well.

CHAIRMAN GORELICK: Thank you.

Chris?

MR. HEHMEYER: All right. Chris Hehmeyer, Hehmeyer Trading in Chicago. I may have a point for you. And I will throw this out to Peter.

In our crypto trading desk with our counterparties, we do a lot of this KYC/AML stuff. You did a beautiful job today of describing blocks and blockchains. It reminded me a little bit of the old days back when I years ago worked in the back office. And the delivery receipts if you turned them over were signed by the companies. And you could track where the delivery receipt had been.

The prospect of know your trade, knowing the history of the block and where it has been and whether a trade or a blockchain, a digital asset has some sort of taint to it, is that going to be possible for the regulators to track that? And is that a good legal thing to maybe have a look at?

MR. VAN VALKENBURGH: So the blockchains we

have been talking about today, things like Ethereum and Bitcoin, have transparent transactions. There is no attempt to encrypt or obfuscate the information there. The information does not, of course, include human-readable names, as I said, but addresses are persistent. And if you can identify somebody as the holder of the private key that matches that address, you can basically look at their full transaction history.

It is actually far more public than, say, the movement of cash, even through the correspondent banking system. And that actually is probably a design flaw that needs to be amended longer-term. You know, crime fighting is important. Financial surveillance laws, like the Bank Secrecy Act, are important. But if we are going to rely on these systems for all manner of important financial interactions, we are going to be building a panopticon where people can see every person's transaction. If you learned the Bitcoin address of the person in the cubicle next to you and they were being paid in Bitcoin or something like it, you could watch their paychecks coming in. Nobody

wants that world.

So as the technology moves forward, we are seeing the evolution of cryptocurrencies. We are seeing proposals to change Bitcoin to make it more private. We are seeing proposals to develop new cryptocurrencies. And some of them are already running, like ZCash and Monero.

And these are real fundamental innovations that Coin Center -- and, of course, we are an advocacy organization. Although we represent the freedom to innovate, we don’t represent any companies. But we believe that these are fundamental to preserving human rights as we move into a future where machine learning and big data will basically make us always subject to surveillance, whether it is corporate surveillance or the surveillance of a good government, like the U.S., or of a not-so-good government.

And so we have recently published a report that describes the level of transparency in some networks and the level of privacy that some newer networks afford users. And we also delve into why that is important, why developing these technologies is en

masse going to be a good thing. And we have another report that we recently published delving into the constitutional law issues of attempts to regulate, say, software developers of these more private networks as, say, Bank Secrecy Act-regulated parties and things like that.

CHAIRMAN GORELICK: Thank you.

Alex?

MR. STEIN: Alex Stein, Two Sigma.

Before I ask my question of Charles and Kathryn, I would like to back up some of what Peter said. Investors need to know that the IP associated with their transactions is confidential. And so in that sense, the design of the Bitcoin ledger raises challenges, problematic challenges, associated with being able to implement the strategy and not have it transparent to the whole world to reverse-engineer. So there ironically is a tradeoff there.

I don’t know that I am totally on board with the need for total anonymity. And that is going to drive my next question to the ABA representatives. Did you think with respect to the underlying cash

instruments about how the rule of law and the ability for recourse plays out in these instruments? Obviously if it is a derivative and it is regulated by the CFTC, the market makers are regulated, but a transaction of Bitcoin or Ethereum, you know, in a smart contract, I don't have all of those mechanisms.

MS. TRKLA: The short answer is yes, generally, not for purposes of the white paper. Again, that is one of I think many issues that would fall under the Blockchain Modality Working Group, but I know that is one of the issues that we have discussed during the calls of that group, so perhaps more to come.

MR. STEIN: I think that is a very important area for the institutionalization of this asset class.

CHAIRMAN GORELICK: Okay. Great. I see three more name cards up. So we will have three more quick questions, and then we will take a break for lunch. So why don't we go around this way, counterclockwise, starting with Larry?

MR. TABB: Hi. I am Larry Tabb, Tabb Group.

Peter, when you were talking about a proof of stake/nothing at stake, you know, and kind of taking

out transactions in the past and kind of manipulating it and, you know, printing a block that you really shouldn't have access to, if that gets accepted, don't I manipulate the chain and, in effect, you know, either take or remove or add coins onto a block that, in effect, where I didn't have money or coins, I now have coins?

MR. VAN VALKENBURGH: So that is the root of the nothing at stake criticism, which is that you would be able to artificially present as having more power than you should because you have gone so far back in the blockchain that you are able to claim as yours staked coins that have since been transferred out of those wallets.

And that is why checkpointing is generally regarded as the right way to build a consensus mechanism that relies on proof of stake because it effectively says once two-thirds of the network, just to take Casper's protocol from Ethereum as an example, agrees on this block and we have been 100 blocks since the last checkpoint, it is checkpointed. And so any miner or staker in this case who presents an

alternative history that goes back further than this block is, per se, violating the rules of the consensus mechanism because we don't allow those deep reorganizations.

And, you know, this sounds scary, I suppose, but it is not my intent to suggest that proof of stake is by any necessary reality any more risky than proof of work. These things are somewhat underdetermined, but there are running proof of stake cryptocurrencies. So, as I said, Ether is transitioning, but there are already running cryptocurrencies that use proof of stake mechanisms that have, to my knowledge, not been attacked. And these are things like Tezos. And I could get you a longer list if you are curious but, you know.

MR. TABB: Thanks. But how difficult would it be to like, you know, "Let's have a checkpoint. Do it" -- you know, have coins, do two transactions, and then, you know, manipulate like the third one or the fourth one or is that just the lottery process would make that really difficult for me to --

MR. VAN VALKENBURGH: Right.

MR. TABB: -- basically ensure that I am going to be the third guy to do a transaction after I have sold my coins?

MR. VAN VALKENBURGH: Right. So the nothing at stake problem arises because you are able to pretend to be an outsized important character on the network, basically, because you claim all of these staked coins that you shouldn't be able to claim because long ago, they were transferred out of those wallets.

With checkpointing, you couldn't do that except with respect to the most recent blocks, which the pool of coins that you could claim to stake and then transfer away ends up being much, much smaller, effectively. It is all a game of theoretical design, but these are surmountable problems. And I think we are seeing really brilliant people surmount them.

MR. WORKIE: Haime Workie from FINRA. This question is also for Peter.

Regarding the 51 percent attack, you mentioned that the higher the capitalization of the digital assets, the less likely it is to be subject to a 51 percent attack. Does that relate to the

concentration of miners that exists within the context of that, digital assets? And if it does, is there a concern? As there are increased levels of concentration, those problems could start creeping up within the context of digital assets that have higher capitalizations?

MR. VAN VALKENBURGH: So you are absolutely right. That would be another factor. One factor would be just the total capitalization because then we can rationally assume that there will be miners who are seeking the rewards, which will be equivalently large. And, therefore, there will be more power dedicated to the network. And, therefore, it will be harder to obtain the power to attack the network. But if all of that power is concentrated amongst one or two participants, you potentially run the risk that one of those participants becomes malicious and tries to attack the network.

Now, I will say on this question, when you see reports of, you know, X Bitcoin miner has close to 50 percent or close to 30 percent, you know, it looks like a big number. Right? More often than not, these

are so-called Bitcoin mining pool operators, in which case they are a server that is talking to the rest of the Bitcoin network and presenting new blocks. But they have got a pool of persons working under them, who they don't even know, who just dial up and talk to them over the internet, who provide them the work. And this is something that these pool members want to do because it would spread out their rewards from the protocol because the pool as a whole will win blocks more often than one miner working alone. So it spreads out the income, but it does mean that the pool operator potentially has the power to determine which transactions make it in blocks or don't and, in theory, the power to 51 percent attack.

But what I will add is when we see pool operators become large fractions of the total mining power on the network, we see the pool members leave the pool and go to other pools because they don't want to run the risk that the person that they are mining under is going to attack the network.

So these economic incentives, they go both ways. And it is a more complicated picture than I

think a lot of headlines often depict.

MR. WORKIE: And I guess the second part of that question is, should there be any concerns from a regulator's standpoint in the context of separate regions, for example? There has also been talk of mining being concentrated in certain types of countries or certain regions. Is that a concern that we should take into account with respect to 51 percent attack?

MR. VAN VALKENBURGH: So I don't think it is a grave threat, particularly, again, because of this pool issue. So you hear headlines about all of the minings in China, things like this. Again, most of the dominant Chinese miners are pool operators. And so it is not necessarily a situation where one person is running this mining farm in China. It is a bunch of people making independent decisions.

And then the other thing that is important to point out is a miner with a lot of mining power is still extremely constrained in what they can do. They can't double spend transactions unless they are able to convince somebody that the blockchain looks like X and then reorganize it by presenting the network with an

alternative history. And that is something that would be very visible to the rest of the network. And you would basically be able to take steps to protect against that. And it is not something that could be surreptitiously done in order to corrupt the ledger. It is something that would be transparent. And then you just need to find ways to fix it, basically. That could still mean that there is a bit of a mess in the short term, but it is not a sort of insurmountable challenge. And that is even under the worst-case scenario.

The best-case scenario, a miner has extraordinarily little power. So when the network is operating as normal, a miner can -- all they can do is validate signatures. And that is all they do do. And they choose to put transactions in a block. They could potentially not put transactions in a block by systematically choosing to ignore transactions from certain participants on the network, but somebody else could pick that up, that transaction up, with trivial ease and put it in their block. So there is a lot of redundancy built into this system, even as we move to a

world with some level of mining centralization.

And then the last thing -- I know I have given you a lot -- is that there are proposals to change exactly how, even in Bitcoin, this mining competition works that could really well-address this issue. So part of the issue here is that the pool operator is able to choose which transactions go in a block, rather than the members of the pool. There is a proposal to actually allow the members of the pool when they provide their work bind the pool operator to including the transactions in the block that the pool member wants included, rather than the pool operator having that power. And that would significantly effectively redecentralize the power to choose or not choose transactions and move that power away from the centralized pool operators while still allowing the pool members to have a smoothed-out rate of return on their mining activities.

CHAIRMAN GORELICK: Thank you, Peter.

Chris, I think you have got time for one last question.

MR. CHATTAWAY: I will make it quick. Chris

Chattaway, Goldman Sachs. This is perhaps more of a comment, general comment, perhaps even to the chair here.

With public interest in trading on virtual currencies being a bit more subdued lately than it was perhaps the same time a year ago, my sense is that people are focusing on tokenization of real-world assets, whether it be fiat currency or mortgage-backed securities. I wonder if it would be helpful for this audience to hear some expert, you know, testimony or views on how that market structure is evolving -- I certainly would find it helpful -- and what sort of considerations the CFTC would have in that arena.

CHAIRMAN GORELICK: Yes. I think that would be a good topic to put on the agenda for the subcommittee going forward. Thank you, Chris.

MR. GORFINE: Okay. Great. With that, let's go ahead and take our lunch break. And we will reconvene right around 1:15, maybe a few minutes after. Thanks.

(Whereupon, at 12:30 p.m., a luncheon recess was taken.)

A F T E R N O O N S E S S I O N

MR. GORFINE: I will turn it back to Richard, and we will be back in session now.

CHAIRMAN GORELICK: Thank you, Daniel.

I would now like to turn to our next panel, in which we will hear from our Cybersecurity Subcommittee members, Mr. Tom Price -- where are we? Okay. There.

MR. PRICE: Yes. Hello.

CHAIRMAN GORELICK: -- Tom Price, Ms. Nina Neer, Mr. Gil Vega, and Mr. Jason Harrell, as well as Mr. Josh Magri from the Bank Policy Institute. We will then open up to our broader TAC membership to explore next steps for the subcommittee and its work.

And, with that, I will turn it over to Mr. Price.

MR. PRICE: Yes. Well, actually, I will turn it over to Josh, who has led the industry efforts working tirelessly over the last few years to develop what is known as the sector profile.

So, Josh, thank you.

MR. MAGRI: Thank you, Tom.

And, before we begin, I would like to thank the commissioners and thank the staff here today and thank you also, Chair Gorelick. And we really appreciate you hosting this meeting today and inviting us to speak on this topic. My remarks and requests are based on over 2-plus years worth of work with over 50 working sessions involving over 300 cyber experts; 150 financial institutions; an open NIST workshop; over 9 Federal regulators and their input, SRO input, and state-based organizations.

And this was all to improve cybersecurity and address challenges represented by these two numbers and a phrase: 40 percent, 3 million and discerning sector-wide risk. That 40 percent number is really the issue statement here.

When we did a survey of the industry in 2016 through the FS-ISAC, which is our information sharing and analysis sector, we found out that chief information security officers and their teams were spending as much as 40 percent of their time doing compliance-related activity as part of their overall daily portfolio.

And one of the things that made this particularly challenging is really the dearth of cybersecurity professionals. I mentioned that three million number. In 2019, we are facing a global shortage of three million cyber security professionals. So, with that, we realized that there had to be a solution that we had to undertake in order to get down that number.

And so we realized that our regulatory and supervisory bodies were appropriately concerned about the cyber risks posed. And this particular slide that I am showing here is actually taken from a Government Accountability Office study post-Dodd-Frank. And this is our regulatory structure.

So all of these agencies, et cetera, were very much interested in the risks that cyber posed and appropriately so. But, as you can see here in this particular graphic, this concern was expressed through the use of different taxonomies and of language by these various agencies. And these semantic differences led to a tremendous amount of time spent on reconciliation and moved us away from a standardized

approach to discern sector risk.

Everyone realized that there had to be a more optimal way forward. So we began with mapping. And we learned that there was tremendous overlap. This graphic expresses that. This is a graphic that we produced using Tableau graphical software after mapping over 300-plus lines of cybersecurity regulatory expectations to the NIST cybersecurity framework and ISO 27000 controls. And while it looks like a wiring closet there, we realized that there was hope. So together with the agencies, we were able to straighten out these lines into this much more I would say succinct architecture. And we did so using the NIST cybersecurity framework for organizational structure along with CPM IOSCO's 2016 guidance on cyber resilience for financial market infrastructure with tailoring to the sectors' cyber and regulatory needs. And we used CPM IOSCO because of its global applicability, but we also used NIST because of its ubiquity and cross-sector uptake.

And because of its increasing global appeal, if not name, in content, we decided to build off of it

and add governance and dependency management as higher-level functions in terms of organizing an overall cybersecurity program assessment methodology. And we extended it to be much more diagnostic in nature because that was something that we saw that the regulatory bodies were truly interested in, was, okay, if you have something like the NIST cybersecurity framework, can you extend it to be more diagnostic in nature? And so we did so.

These are the countries that have been at least interested or involved in taking up NIST. And that is the column on the left. Because of our fidelity to NIST and CPM IOSCO, you have a number of countries that have expressed interest in the profile, with one country even suggesting that they may translate it for their own country's purposes.

In a minute, I will get to the benefits and the development process. And here you go. Here are the benefits. And perhaps the reason that all of those countries and et cetera had been interested is because of these benefits of using such a standardized approach to cyber assessment. So with respect to financial

institutions, the benefits are pretty cognizable and immediate. You will be able to get that 40 percent number down quite a bit and have the frontline defenders getting back to frontline defense.

I work for Bank Policy Institute. And prior to its creation just this past year, I was with the Financial Services Roundtable. And we are a CEO-based organization. One of the things that we heard from the CEOs in terms of cybersecurity was that they were starting to get a lot more frameworks coming at them, and it was very hard to track how they were doing in relation to their overall program. And they would like to use something such as NIST because it was something that was being used across the various sectors. And at its highest level of abstraction, it was only a few functions that they could then really kind of keep track of and then drill down into further.

The supervisory community, what we learned -- and we had conversations with the CFTC, the Fed, the OCC, FDIC, et cetera -- was of great interest was systemic risk and sector risk. And because there was a little bit of a patchwork of assessments within the

regulatory space, they weren't able to see the whole picture across the sector. Because we have utilized a NIST-based CPM IOSCO-based approach, this is now something that could be utilized across the sector. And, of course, for the overall ecosystem because it is based on NIST, there will be more collaboration and understanding. And it allows for collective action to better address risks.

So this is how we went about creating this architecture and the overall profile version 1.0. We, as I mentioned, over 2 years held about 50 working sessions. This was led under the Financial Services Sector Coordinating Council banner. As you can see, these are the trade associations that were very much intimately involved. We had over 300 individual experts participating, 150 financial firms. NIST actually held a workshop specific to developing out the profile. And we had one-on-one feedback sessions and even group feedback sessions with the Federal Reserve, OCC, FDIC, SEC, CFTC, FINRA, et cetera. So with all of this information, we were able to bring it back to that architecture that I showed you prior.

One of the things, though, that did come up during these sessions was, how are you going to scale this diagnostic from those types of entities that are systematically important down to, you know, the 10-person broker-dealer or 3-branch bank. And what we did is we took a lot of the stuff that was available already.

There were interagency guidelines. There was particular rulemakings on sound practices. And we essentially tailored it based on those documents and came up with a tiering system. And it is a four-tier system.

The first tier, those that are the most systemically important are those that would have a global or a National impact if failed by a cybersecurity event. Then there is also tier 2, which would be applicable to those that if failed, they would have a sub-national or regional impact. And then tier 3 is sector-only. And tier 4 is customer third party.

And in creating this, you know, we were able to again get buy-in from a number of the agencies and used a lot of their materials. And since we rolled

this out in October 25th, we have had over 40 firms that have committed to implementing the profile or actively exploring it for the next 2019-2020 exam cycle.

So, getting back to our October 25th launch, we had a National Press Club event; a number of sessions of those that had helped develop it, including some of the folks here to my right; and we also had a number of regulators that came and talked about it and provided positive support.

The Federal Reserve at that event said, “We will welcome any financial institution to provide information to us using the structure and taxonomy of the profile.” We see that as a boon for harmonization.

The OCC said, “If the industry moves to use this profile, that is what we will base our assessments on.”

The FDIC said, “That was one of the things at the FDIC that we were most interested in looking at, is that tiering.”

SEC was similarly supportive.

In terms of kind of around that event, we had

been working pretty much lockstep with NIST and the agencies. NIST got a prerelease review I guess that you would call it. And they sent a letter to our FSSCC chair, saying that the profile was one of the more detailed cybersecurity framework-based sector-regulatory harmonization approaches to date.

And the FFIAC in announcing a webinar for October 31st in an October 30th email said that "These resources are actionable and help financial institutions manage cybersecurity risk, regardless of whether they use the FFIAC cybersecurity assessment tool, NIST cybersecurity framework, financial services sector-specific cybersecurity profile, or any other methodology to assess their cybersecurity preparedness."

So it is with that that we are here making the following request. We really believe that in order to maximize the benefits of the profile for both financial institutions and supervisory agencies alike, we encourage the following: public statements of support similar to the ones that were found on the prior slide, stating that the use of the profile as an

input for examinations and as a mechanism to evidence compliance is acceptable, and also for your support as a common baseline framework for cyber supervision in conversations, both within the FBIIC, which is a collection of financial services regulatory agencies; and with the international regulators.

I am going to pause there. Here are the websites where the profile can be found. And then I am going to turn it over to my colleagues for the next presentation because I believe that we are going to be entertaining questions at the conclusion of all three.

CHAIRMAN GORELICK: Thank you, Josh.

MS. NEER: Good afternoon. And thank you once again to the chairman, the commissioners for hosting us today.

The next several slides, we are going to talk about oversight of cybersecurity as firms move their infrastructure into cloud-based environments. We all recognize the importance of cybersecurity, whether it be for individual firms or the financial markets as a whole. We also recognize that CFTC maintains a good body of system safeguards all ready today.

As the firms move the infrastructure into the cloud, there are some unique challenges that need to be accounted for in a shared-responsibility manner. And our intent is to continue to work closely with CFTC to make sure we address those.

Fundamentally, the same cybersecurity requirements are going to apply, whether infrastructures is managed on premise or managed in the cloud, they just may be implemented in slightly different ways to account for the different architectures. There is still a need for strong governance, education, engagement of boards of directors, risk committees through this journey. And the control requirements that we will talk about can also be supported by the cybersecurity profile that Josh was speaking about.

Before we turn more specifically to the considerations for the group today, this slide provides just a visual reference on the different types of cloud-based infrastructures a firm may adopt. You have got software as a service, platform as a service, and infrastructure as a service, which is where we are

going to focus today: infrastructure as a service. And you can see through the visual that there is a sliding scale of shared responsibility between the cloud provider, with the gray boxes, and the customer or the firms, with the blue boxes, in terms of managing an environment from physical hardware up through application in an end-user environment. And so important to keep in mind that the customer responsibilities, again, remain the same to meet the cyber requirements.

I am going to hand it over to my colleague Gil Vega to take you through the considerations.

MR. VEGA: Great. Thank you, Nina.

As Nina mentioned, we think that the regulation that currently exists today with regard to system safeguard is certainly general, broad enough, and extensible to cloud environments. And we would encourage the Commission to continue down the path of driving examination in these environments in a consistent way, as they do with on-prem technology.

With respect to the recent system safeguard testing requirements from a few years ago, the new

testing requirements related to system safeguard testing, we believe that those are certainly extensible to cloud environments and would encourage the Commission to continue to leverage those in their examination process for our cloud.

I will move this closer. Sorry. There you go. I am a low talker.

So, that said, what we wanted to do today was come to you and talk to you about some of the fundamentals that we think are so important for firms that are considering moving into the cloud. And whether you are a CISO for a systemically important market utility, like myself, or you are running a small FCM shop or broker-dealer, these fundamentals I believe apply in all of those cases. And they should be important to everyone. So we are just going to go through these fundamentals very quickly. And I think we have got about a half a dozen of these.

So it all starts with a strong foundation. And that strong foundation doesn’t begin very quickly in terms of thinking through the process of moving to the cloud. It has to be a slow, deliberate process.

In my estimation or our estimation, as Nina mentioned, there is so much governance around the idea of moving regulated applications, regulated data to the cloud. And in our journey with regard to CME's cloud journey, we spent an awful lot of time with your examination teams, making sure we were both comfortable and that the internal corporate governance had visibility into all of the risk decisions that were taken as we move these applications to the cloud.

So that strong foundation includes, obviously, lots of implications for data protection and encryption for intrusion detection and prevention. You need to be able to make sure that you are protecting your customers' data, your competitive data, your ability to detect anomalous activity, and respond to events and incidents that are happening in a cloud service provider's environment. And then the vulnerability management strategy, obviously, we will get to that a little bit later in the presentation, but it is the same but a little bit different. And you have got to account for these new realities as you move towards the cloud.

One of the things that we feel really strongly about being a key fundamental aspect of any cloud migration is the authentication and authorization, which you could just define as making sure that the right entity has the right access to the right resource at the right time for the right reason. I think it is better than 90 percent of all information security breaches currently involve an identity or access management component to it. So it is important to continue to focus on this as a strong fundamental using things like federation and centralized management of accounts and validation of those accounts as well as verification that those accounts are still necessary, implementing things such as Least Privilege, which is a best-known practice in information security, as well as logging access and making sure that the right people are accessing the right assets.

With the cloud, there are new strategies that you can leverage, including containerization, the development of micro and mini services. Understanding how these systems talk to one another is absolutely critical as you architect these systems because if you

cannot define how these systems engage with one another, it is going to be nearly impossible to respond to incidents that are occurring there and nearly as difficult to monitor appropriate activity.

One of the huge benefits of cloud implementation is the ability to go with full automation to deploying servers and applications. When we move to full automation, we are able to remove some of the human errors associated with manual processes involving technology deployment.

As Nina mentioned, this is a shared responsibility. And as you pick cloud vendors, you are going to inherit some of their underlying controls. And it is important for every company moving to the cloud to understand what those controls are. It is absolutely critical that you trust the controls that are being delivered by that cloud provider but you verify those controls and you compensate where you need to.

For those organizations that find it important to understand exactly where the physical infrastructure is, it is important to work out those

arrangements with the cloud provider to make sure that you have an understanding. It is also important to make sure that you account for operational resilience. Moving to the cloud doesn't automatically add disaster recovery capabilities or high-availability capabilities. Those things need to be understood in great detail with cloud vendors. And cloud vendors vary in terms of capabilities that they are able to deliver.

Monitoring the access to your data is absolutely critical as well. And we would recommend that this continue to be a focus of your examination process, the ability to monitor who is accessing data, for what purpose is an important consideration for companies as they move to the cloud. And with the proliferation of privacy laws and regulations across the globe, it is important to understand exactly how your cloud provider will remove data when you ask them to and validate and verify that they have removed it or sanitized it correctly.

Cloud technology supports the use of open-source technology. And to the extent that you can use

it securely and deliver resilient solutions with open-source, you should. There are lots of good reasons for leveraging open-source, including guarding against vendor lock-in. There are multiple vendors providing cloud services. And it is important to have some semblance of mobility built into your applications and your data storage in the event that it is necessary to move from one cloud provider to another one.

And, finally, before I turn it over to Jason to talk a little bit about TPRM, vulnerability scanning. It is absolutely critical as well to maintain a focus on dealing with vulnerabilities in a cloud environment. There are cloud providers that will sign up for certain levels of service as it relates to patching the underlying infrastructure, but it is important for companies and entities considering the cloud to understand where those differences lie, where the demarcation is between what the cloud provider is responsible for and what the individual companies are responsible for.

And, with that, I will turn it over to Jason. Thank you.

MR. HARRELL: Good afternoon. Thank you to the commissioners and members of the Technology Advisory Committee for allowing me to speak to you on vendor management and giving you a little bit of background on where we are today relative to that.

You know, vendor management is an area that has received significant attention from the global supervisors and standard-setting bodies. During the review of this topic by the subcommittee, we have noted that there have been several supervisory rules, rule interpretations, guidance, and questionnaires that are looking to prescribe either an approach or to understand what firms are doing relative to managing the risk of their supply chain.

In addition, firms have responded to these risks by incorporating information security requirements into their contracts and to either limit liability and to also continue to provide oversight through the lifetime of their contract with the vendor to understand their risk posture through the terms of the agreement.

At this time, the subcommittee continues to

review the existing supervisory documents to understand the current regulatory landscape and the approaches prior to offering recommendation to the committee.

So where are we relative to this? First, the supervisory documents have provided firms and financial market infrastructures with general requirements that should apply to all of their vendors and at the same time have provided more detailed guidance around the same organizations on vendors deemed to be critical.

Second, the supervisory documents provided to firms and FMIs have different breadth of coverage over the vendor management lifecycle. This includes all aspects of the vendor management process from planning by a firm or FMI on how they will use a vendor, all the way to the termination of the vendor contract.

In addition, this looks at activities that are performed or conducted through the course of the agreement, whether that is the ongoing documentation and reporting of that vendor’s risk posture and the independent review of the vendor management program by the firm or FMI’s independent audit function. As part of the initial discovery of documents, there have been

over 15 documents that outlined vendor management control requirements, including most recently the Monetary Authority of Singapore's consultative guidance on technology risk management.

Oh, thank you. Thank you.

To provide a glimpse into the current number of supervisory documents the subcommittee had provided a link of the numerous current guidance that has been promulgated by the different authorities, you will note that some of the standard-setting bodies, such as IOSCO, all the way to certain state regulators, such as the New York State Department of Financial Services, has issued some level of guidance on vendor management.

Oh, thank you.

So, given the amount of current guidance on vendor management, the subcommittee requests additional time to first review the guidance provided from other supervisors and to identify potential opportunities to strengthen the current guidance that has been promulgated. Guidance in this area does go back to 2003. So, at a minimum, it may be time to refresh some of the guidance out there based on the different risks

that have been exploited for vendors since that time and changes to the threat landscape that we have seen since that time period.

The subcommittee can then develop a set of recommendations together with the rationale for those recommendations, which can be used as a proposal to the committee.

I seem to have a little trouble with this thing. Oh, I just scroll? There we go. No. That is good. Thank you. I am getting the hang of this.

Anyway, as we go on this journey, the subcommittee requests input from the committee on two areas. First is given that current guidance provides both prescriptive rules as well as principle-based guidance in the area of vendor management, is there a preference from the committee on the type of recommendation that we provide back to this committee so that we can make sure that we are meeting that expectation.

And the second, we have also noticed that supervisory documents have provided guidance on critical vendors. Yet, there has been evidence that

additional factors may be needed to identify a vendor's criticality. And then is the committee open to a new approach possibly for how criticality may be determined prior to us going and investigating ways where we can improve how critical vendors have been identified?

And, with that, I will turn it back over to the chair, and we will be looking to answer questions.

CHAIRMAN GORELICK: Terrific. Thank you to all of you for those presentations. It was very helpful and informative. And I noticed some common threads between the various presentations. I was particularly struck by Josh's comment at the beginning that we are three million cybersecurity professionals short in the economy this year. And that is a number that seems very hard to fill without putting some real thought behind the types of work that we are asking these professionals to do. So I think this was a very good step.

I want to open it up to questions right now, but before I do that, I just want to put it in a little context. I understand that the cloud presentation today has a series of recommendations. I think what I

would like to encourage people to think about today is giving feedback on those recommendations. And we can get that feedback today at the meeting. We can also have a period of time to follow up with the committee and on those recommendations and then ask the subcommittee to formally propose these recommendations or the next version of these recommendations depending on the feedback for a vote at the next upcoming TAC meeting.

And then it looks like -- Jason asked some very good questions as well to help structure the recommendations of the subcommittee on the vendor management piece. And so I would also encourage people to give feedback on that.

So, with that, I would like to open up the discussion. Aubree?

MR. GREENSPUN: Aubree Greenspun, NASDAQ.

In particular, around the cloud recommendations, did the committee consider recommending or questioning any need for extra consideration from an exchange perspective versus a BD perspective? Certainly from the exchange perspective,

you know, is there a difference of our matching engines being in the cloud versus our surrounding systems and what should the governance be around that?

MR. VEGA: Nina mentioned the absolute necessity to have corporate governance around these decisions, obviously. And there are certain applications for which the cloud has met and there are certain applications for which the cloud obviously has not met. And those decisions need to be internally made with full governance of the risk committees and boards involved in those.

I can’t comment specifically to whether or not a match engine belongs in the cloud or not. And I can’t specifically provide any detailed information about how CME is approaching that in this open meeting, but it is a situation that obviously has to be addressed with a risk-based analysis depending upon a firm’s individual requirements.

MS. NEER: And if I can just add to that, we didn’t differentiate in our recommendations specifically between an exchange’s systems or a broker-dealer’s systems. Again, it is about these practices

are critical to apply everywhere. Taking a risk-based approach in terms of what are the right applications to put there, but when those decisions are made, everyone needs to be protected in order to protect everyone else.

MR. GREENSPUN: I appreciate that. You know, we are all held to the standards and need to make our own risk assessments. Right? I think I was simply asking, should we as the committee be considering if we should have some recommendations in regard?

MR. VEGA: I would say yes. And we will take that back and come back to the committee. Sorry.

CHAIRMAN GORELICK: Thank you.

Tom, I think you were next.

MR. CHIPPAS: Tom Chippas, ErisX.

Did the subcommittee with respect to the cloud content give any thought to the benefits for small organizations? Specifically, a lot of the recommendations have a feel of being very large-scale, very corporate, a lot of focus on vendor lock-in, portability, which are all goals that are reasonable for large enterprises. Yet, cloud operated by large-

scale professional organizations can oftentimes provide more robust and better-controlled infrastructure that small entities would never be able to access on their own. So I am just curious if in the time the subcommittee had, there was any thought to perhaps providing differentiated recommendations, weighing those different benefits depending on organization type.

MR. VEGA: I think that is something we can certainly go back and work on. It was a topic of our conversations early on in our subcommittee meetings. We had members who come from much smaller organizations than many of us participate in these conversations. And we thought what we were trying to do with these thematic recommendations was to address both the smaller firms as well as the larger firms. So if it came off sounding as if these were sort of huge enterprise corporate recommendations, that wasn't the intent. I think maybe there is an opportunity here for us to go back and clarify that a bit.

MR. CHIPPAS: I am sure some of the smaller firms would benefit from that.

And then with respect to the presentation on vendor management, just very quickly commenting, as the chair was looking for feedback, I know that I and we at ErisX would be supportive of a principles-based approach in both instances and definitely a reconsideration of defining criticality.

MR. VEGA: Thank you.

CHAIRMAN GORELICK: Gary?

MR. DeWAAL: Yes. Just following up on Tom's good point, obviously when the NFA came out with the requirement that firms implement ISSPs, they were very mindful of the fact that one size does not fit all and there should be differentiations. I just want to second Tom's very good point that although broad principles may be -- you know, are a good thing, there should be some kind of differentiation between what is expected of a small and big firm because, obviously, the small firms don't have the resources. And, yet, they can benefit by deploying the cloud for storage and other purposes.

CHAIRMAN GORELICK: Paul?

MR. CHOU: Yes. You know, I think I would

like to see also some elucidation as to not just like how to do cloud management but also the certain scale advantages that cloud has, you know, in the sense that they see many, many more vulnerabilities in a much different set of contexts than even a well-resourced individual company would have. And so they happen to have scale effects where they can deploy the lessons learned from a much wider attack service that they didn't see. Like, for example, AWS or all those guys see quite a few more things than any individual company would do. And those licenses are immediately kind of distributed. So I think outside of just managing the cloud infrastructure and where you should put certain things, you know, there should be some discussion as to the pros and cons of both approaches.

CHAIRMAN GORELICK: Mayur?

MR. KAPANI: Mayur Kapani from ICE.

A quick question on the profile. Does the profile take cloud as a first-class deployment strategy for financial applications?

MR. MAGRI: So with respect to cloud, the way that we built in cloud-based assessment-type questions

are in both the governance and the dependency management sections. We are really looking at the profile as more of the diagnostic or assessment for the enterprise. And, of course, you know, cloud is one of the components, but there is a whole suite of other components related to cybersecurity that are integrated within the profile.

And the profile essentially consolidates again that 3,000 rows of mapping of the various agency requirements down into about 300 questions. We were able to synthesize that that much.

MR. KAPANI: Okay. Thank you.

CHAIRMAN GORELICK: Josh, I will add that I was glad that you did not read through all of those 3,000 lines. When I first saw the slide, I was concerned we might need to allocate some extra time for the presentation. But it was a very impactful visual.

So, Haime, I think I am going to put you on the spot a little bit if that is okay. I understand that FINRA in recent years has moved a lot of its infrastructure into the cloud. Maybe you have some experiences you could share with the group on that

experience.

MR. WORKIE: Sure. You know, I guess the one thing I would say is that moving things to a cloud has a lot of potential benefits associated with it, as Paul was pointing out, where you have an entity that could potentially have a bigger look. But there is something also attached to that. Each individual entity that moves their system to a cloud pick the tools that they utilize from that vendor and to integrate into their own system. So I think a lot of that still goes back to the individual entity to make sure that as they are linking up to the cloud, that they are using the tools appropriate for their business and thinking through those issues. So I don't know if the report comments on that, but I think that is really a key determining factor because it is not just offloading all of the issues to another vendor. You still have to think about how you integrate with the system.

MS. NEER: Which is the critical point on the visual of the shared responsibility. Just because you as a customer deploy to the cloud, you are still responsible for making those appropriate decisions

around tools and strategy.

CHAIRMAN GORELICK: Thank you.

Brad?

MR. LEVY: Yes. Brad Levy, IHS Markit. One comment.

It may be worth drawing some distinction between applications, the data, and the calculations, which have traditionally been a system that could be deployed on prem or in cloud. In the future, you may be able to break those apart more. The data getting around is more controversial in terms of protection and deletion and all of that, but you may be able to leverage it more for applications or calculations while the world is getting more comfortable with the data, so drawing those distinctions in a more modular way than a more monolithic systems way, which is more our history. And it may get us there more quickly incrementally if we think about it as more components than a whole system, moving or not.

CHAIRMAN GORELICK: And Chris?

MR. CHATTAWAY: Do you guys think there is sufficient competition in this space? You hear a lot

about AWS, Google, and I think its Microsoft. Is that enough, too much?

MR. VEGA: I think, obviously, it cuts both ways because you work with a single vendor oftentimes to make sure that your controls are meeting the requirements of your internal control framework. Sometimes it is often difficult to use the same teams responsible for identifying those gaps, remediating those gaps, and then designing a new infrastructure for another provider who is providing different services. So I would say that there probably is enough competition, but it is difficult for highly regulated companies and it is probably not as difficult for smaller companies. But for the larger companies, it is certainly more difficult to shift controls from one provider to the other because there is such a difference between these current cloud providers.

MR. CHATTAWAY: I was going to say then the switching costs are also quite high. You know, you get onto AWS, and you are there for life.

MR. VEGA: Well, you know, I mentioned in my presentation the idea of, you know, containerization

and micro services and the ability to use those types of strategies to move away from the danger of vendor lock-in. And at some point in the future, you will be able to field or deploy those micro services in containers to different providers much more easily, but there is still a lot of work to be done with regard to mobility and micro services.

MR. LEVY: And if I could just offer a point? I think the infrastructure as a service, is the first wave, thinking of platform as a service, which is more the micro services architecture and containerization. We have struggled to think about those independently. So thinking about infrastructure as a service and platform as a service, really, as a combined initiative, which if you think past first, it starts to -- you may be able to abstract yourself from any one system over time, although there is a pinning effect.

And on the competition point, I would argue it is not maybe about the number of providers but the business models of the providers in terms of what they are doing with the applications and the data and the calculations that are going through that

infrastructure. Whether it is the right number of three or four, it may be more interesting what those providers do as a core business beyond being a cloud provider.

CHAIRMAN GORELICK: Alex?

MR. STEIN: Thank you. Excellent presentation.

With the focus on the smaller, technically less sophisticated clients, have you looked at some form of certification for the cloud services so that precisely the less sophisticated client, who still has these responsibilities, can rely on the certification of the vendor, rather than opine on things they don't understand?

MS. NEER: We didn't discuss it specifically. We can certainly incorporate that.

I don't know if you have any thoughts, any additional thoughts, on that.

MR. VEGA: Not really. Only to reiterate something that Josh touched on earlier, which is the nature of our industry as we are pulled together through the financial services information analysis,

the ISAC, Information Sharing and Analysis Center. We have got cloud security working groups at a high level that are pulling us all along together in this journey. So you have got large, global, systemically important banks and market utilities and smaller, less sophisticated, less well-resourced financial services firms understanding our experience as we share that with them. So I think we can go back offline and talk about a possible certification approach, but to the extent that we are all sharing our well-earned scar tissue with those smaller firms, you can be sure that that is happening on a pretty regular basis.

I don't know, Josh, if you wanted to add anything to that?

MR. STEIN: I think that one of the problems here is technology and threats continue to evolve at such a fast pace. It is very difficult for most organizations to stay abreast. So a solution that allows the enterprise to rely on the expertise of the experts on an ongoing basis would be beneficial.

CHAIRMAN GORELICK: So one other question for the subcommittee, are there areas where the

subcommittee believes that the current regulatory oversight requirements are insufficient for the risks and the benefits of using the cloud infrastructure?

MR. VEGA: I have already given you my opinion. I say no. I think they are general and extensible enough to address this new environment.

MS. NEER: In different terminology, principles-based, rather than prescriptive, “Do this,” “Do that,” is a good approach.

MR. MAGRI: And to the extent that you are considering any type of guidance, regulation, et cetera, we would ask that you follow the architecture of the cybersecurity profile or at least use it as an informative reference because, again, much of the time spent on compliance has been in that reconciliation process. And the profile provides that organizational structure and taxonomy that is extensible with future guidance and regulation.

CHAIRMAN GORELICK: Paul?

MR. CHOU: Yes. Hi. I am Paul Chou from LedgerX.

You know, one additional thing that I think

might be useful is that while this is a cloud discussion, it is not an either/or kind of thing. And so it might be very useful to say we are not just doing exclusively the cloud. You know, we also have our own infrastructure. And how does that relationship look? If one thing goes down, what do you do to the other? And what might be best practices to have maybe the best of both worlds in a lot of ways?

CHAIRMAN GORELICK: Okay. Thank you very much.

If there are no further questions, I want to thank the subcommittee for their presentation and turn to our final topic on the agenda, in which members of our DLT and Market Infrastructure Subcommittee will share their current efforts and work streams going forward. Our panelists will be Ms. Shawnna Hoffman-Childress; Mr. Charley Cooper; and Mr. Jesse Drennan; as well as a guest speaker, Ms. Tara Kruse from ISDA. We will give a few minutes to get everyone seated, get the nametags changed, and the presentations teed up, and start back in about three minutes.

(Recess taken.)

CHAIRMAN GORELICK: OK, thank you everyone. We are going to continue the presentation now. So I will turn it over to the DLT and Market Infrastructure Subcommittee. And I believe Ms. Hoffman-Childress will be beginning with the presentation. Thank you.

MS. HOFFMAN-CHILDRESS: Yes. Thank you so much, Chairman and commissioners, for having us here today. So I am also joined by Charley Cooper, Jesse Drennan, and also Tara Kruse.

And, well, speak up a little bit more? All righty.

So as we enter into this fourth industrial revolution, you know, I think we all can agree, as we have heard today, it is absolutely an unprecedented time. So we have the ability with today's technology to speed up transactions that used to take weeks. We can speed them up to just minutes and even seconds. So today my esteemed colleagues and I will go ahead and share with you -- I will cover the state of the states, so kind of the current state of blockchain. The technology forward in the DLT space will be covered by Charley. And, also, real-world applications will be

covered by Jesse Drennan and also next steps.

Now, distributed ledger technology is also known mostly as blockchain, but, then, also we hear it called DLT. So blockchain has the potential to disrupt any industry that employs the use of trusted third party middlemen. And it gives direct control back to the end-user. However, with any technological revolution and the paradigm shift that comes along with those, there is a process of trial and error, what works and what doesn't work.

Now, with that process, as you can see with this hype cycle right here, we are just starting to go into what we call the trough of disillusionment. And a lot of us have heard fun things in the media, "Blockchain is here to stay," "Blockchain is going," but, again, just as a reminder to everyone who is here today and those who are listening, we are going into the trough of disillusionment. So there will be some things that are kind of up and down in the marketplace as we continue to move forward.

We thought that it was important to also share the blockchain adoption and how it has been

adopted industry by industry and what we have been seeing over the past few years. You know, it absolutely is undeniable that blockchain is one of the major technologies that is catalyzing the pace of innovation. And it is introducing many new radical shifts in every industry. So, as we can see here, we have awareness.

A lot of the industries are getting educated. We also have many industries who are currently experimenting and creating those proofs of concepts. And then, of course, some are in production. And a few are still a little bit not sure. And so we start to see this adoption really taking place and starting to be a little more of a catalyst within those companies. You know, there is tremendous promise within all of these respective industries when it comes to blockchain.

We also wanted to share a little bit with you about blockchain history. I think one of the questions that I always get is, isn’t blockchain Bitcoin? Well, it is not. So Bitcoin, as we know, is an application of blockchain and blockchain, of course, being created

back in the early 1990s. So as we kind of take this quick walk down memory lane, we are reminded that the first work on a cryptographically secured chain of blocks was described in 1991 by Stuart Haber and Scott Stornetta. Now, they wanted to implement a system where document timestamps could not be tampered with. And in 1992, they incorporated Merkle trees to their design, which allowed several documents or certificates to be collected into one block.

Now, I spoke with Scott Stornetta this morning. And they are continuing their work. They actually recently just started the Blockchain Corporate Governance Foundation. And their mission is to increase integrity and transparency in corporate operations. So we have our initial co-inventors of blockchain still, of course, being very active in the space.

But, as we all very well know, in 2009, the words “block” and “chain” were used separately by Satoshi Nakamoto’s original white paper. Nakamoto improved the design by using a hash cash-like method to add blocks to the chain without requiring them to be

signed by a trusted third party. And, of course, this is the core component of Bitcoin. But it is an older technology. I mean, now we are looking at almost 30 years old. And a lot of things have happened. So we see in 2009, of course, with Satoshi's white paper coming out; we see 2011 to 2012, the deployment of cryptocurrency in application related to cash; 2012 to 2013, current transfer in digital payment systems; 2013 to 2014, financial markets and applications using blockchain beyond cash transactions. Smart contracts came in 2014 to 2015. And then 2015 to 2016, we have seen permission blockchain network solutions. And then 2016 to 2017, we are seeing a large-sized market consolidation with many further subdevelopments.

So, to talk a little bit about the future of blockchain, I am going to pass it over to Charley.

MR. COOPER: Thanks very much. And thank you to the Commission for hosting. As always, it is good to be here.

I guess I learned a lesson coming into this. I should pay attention during the subcommittee meetings because had I noticed that I had to predict the future

today, I might have avoided the presentation. So I am going to try to make some predictive comments, some of which will seem a little less than specific, but we can also talk about not necessarily the past nor the future but what is happening in the moment. And I think that might help. I think that might help frame a little bit what we are looking at in the future and what the CFTC as an agency should be thinking about in terms of what is coming down the pike.

So I am actually going to do one historical note to explain why predicting the future is so difficult, in particular, in this industry.

When Satoshi published the white paper 10 years ago, the white paper itself if you care to read it is in some ways as much a political document as it is a technical document. And much of the white paper is actually talking about a new world of economics; a new world of commerce; a new world of people and entities relating to each other that was a reaction to the financial crisis, the ills, the perceived ills, of the banks, and central governments. And, as such, the paper was written in many ways as a manifesto against

many of the people in this room, including the agency that we are testifying in front of.

And it envisaged this -- but this is actually I think, really, I think interesting but maybe not, but I think it is super interesting. Here we are 10 years hence. And not only are the financial institutions and other global companies thinking about using blockchain, the very companies that Satoshi had hoped to get away from, but federal governments around the world are now looking at ways in which they can incorporate this technology into the way that they do business. And that is a really big deal.

If you think about what would have been predicted in 2009 about where blockchain would be, this is probably the last place that someone might have predicted it. So here I am about to try to tell you where we are going to be in five years. So take everything with a grain of salt.

I think there are a couple of rules of thumb to think about as we are heading into 2019. First of all, this is already real. And to the extent it may not necessarily be on the radar of the CFTC in a

derivatives context -- and Jesse is going to talk a little bit more about some of the things that will relate to the CFTC jurisdiction in those markets -- there are live applications that -- not just R3 but IBM and HSBCs themselves and others are doing and running around the world, where live-transaction volume in different markets is occurring today on blockchain. We have moved beyond in a limited way, beyond the world of proofs of concept and experimentation. And this is real money and real transactions changing hands. And I think that is really important to think about, right? So this is no longer the sort of idea -- this expectation that we hope is going to happen, it is happening.

The second thing I would say is a rule of thumb is if you are trying to figure out to all of the entrepreneurs out there looking to launch a company, if you are trying to figure out where this technology is most likely to be deployed next, look at the things that are the most antiquated and broken and reliant on legacy systems and processes that haven’t been updated in some cases decades, if not years definitely, and in

some cases decades. And there are several examples of that.

I mean, two areas in which we do a lot of business at R3 is trade finance and insurance. And if you think about that, that makes perfect sense. These are entities that still play by rules of multiple different parties signing actual documentation, stamps in different ports of call, the passage of goods between different entities that are recording it in duplicate or triplicate or quintuplicate or whatever the term would be. That is such a way that in many ways is foreign-concept certain markets that in the more advanced markets, they haven't necessarily paid as much attention to blockchain because, at least in their minds yet, they don't have as much to gain from that.

So if you are looking at the types of -- if you are looking at a set of areas where this stuff is already beginning to be deployed, you look at pre-trade and you look at post-trade, more the middle- and the back-office piece because things like the actual match -- I mean, if you think about how quickly a transaction would happen on CME today, in a matter of milliseconds

or microseconds -- I don't know what that number is -- that is not something that blockchain is going to attack and make more efficient right now. But how long does it take to onboard a client? How long does it take to deal with the entire reconciliation process that happens after a trade? There we are still talking days or weeks at some point. And that is the kind of area which is really ripe for innovation.

So, with those rules of thumb, I will just give you a couple of examples of the kinds of things that are happening in real time in the markets that are out there.

HQLAX is a platform for collateral management for high-quality liquid asset exchange. Its major backer is Deutsche Borse. It happens to be built on R3 Corda. We will talk about other platforms as well, but this is a platform that did its first live trade actually last year between regulated entities ING and CS that were moving a basket of securities between them in a digital form, in a tokenized form, although the term was not used at that point by that entity, but that is something that is already happening.

A company called Tradewind out of Canada that works with the Canadian Royal Mint for the trading of gold. That is live. That is already running.

Finastra, which is a massive Fintech company based in Europe but has global remit. Their syndicated lending platform is being migrated over to blockchain within the next several months.

B3i, an insurance company. I mean, there are various different things we could go through, but these are real applications that are happening. And I will defer to Shawnna and Jesse to talk a little bit about HSBC Everywhere and about IBM's we.trade and other initiatives that they have. I am talking about the stuff that is happening on our platform. But that is by no means the exclusive platform that is being used in the marketplace. Many others are being used.

So 2019 to us, or at least to me because I am in the hot seat, is the year that you are beginning to see deployment in markets. Although it is still nascent, I would suggest that over the course of '20 and '21, you begin to see those deployed at scale. There are already large financial institutions around

the world that are deploying blockchain enterprise solutions within their four walls to handle transactions between the various different divisions. That is happening already. That is happening live. And that will continue to happen.

One of the obstacles, but it is actually being worked through and remarkably, impressibly, actually, at many institutions, is the idea of integrating these current systems with the systems that have built up, again, over decades in a lot of these organizations and how they figure out how to integrate with blockchain and ultimately migrate away from what they are currently using onto a full blockchain solution. Those are the types of things that are going to happen within the next two to three years, we would predict.

And then the more sort of futuristic stuff -- and I would defer to Chris Church at DA. I think he is on the line, but I will take this because he wasn't able to be here today. There is this idea of, as he calls it, convergence. But it is the idea that there are other types of massively important and influential

technologies out there. It is not just blockchain. It is big data -- and it is AI and machine learning and a whole bunch of other things -- that you begin to see all of these things come together.

Now, what does that actually mean? Well, let me give you one example. AI is only as good as the data that is being kicked into the system for the machine to think through and do its various different analytics and produce some sort of information in the backend. If the data is crap, the AI is crap. I think it is a term of art that I just used. But if the data is not good, then the AI is very limited in what it can do. So something like blockchain or something like the ability for big data, which is taking reams and reams and reams of data that has been accumulated over in some cases again decades being backloaded into systems and then new data being produced each and every day, the more data that goes into systems, the more the AI can learn and the more the predictive behavior of that can become powerful.

So if you think about it, in many ways, we are all helping to unlock each other that these various

different technology solutions we would envision down the road become interrelated. Now, is it exactly the way we would think about it is now? I honestly don't know. I mean, the reality is technological innovation is inevitable, but the direction of that innovation is not inevitable. And I think what we are talking about here today may make sense a year from now. We may be back here in two or three years, and we are talking about something that we hadn't even conceptualized today. And there will be younger people at the table or at my company, who have been coming up with ideas that I never could have come up with. And that happens pretty frequently.

So I realize that that last piece of prediction is hard to crystallize, but it is more of a conceptual point that these technologies are all related to the maintenance of data that requires massive computing power and the ability for software programs to operate in an intelligent way to make the most use of that data in a way that could be deployed, not just in the financial services industry and certainly not derivatives particularly, but across

healthcare and telco and energy and gas. And you go through the litany of things.

So I will leave it at that and then turn it over to Jesse.

MR. DRENNAN: So blockchain is quite a broad topic. We thought it worth grounding in a few things the Commission, in particular, has oversight on in order to have a little bit more concrete and real conversation. And, in particular, I just want to emphasize focusing in on business outcomes for the firms that are participating around the DLT or the technology because, obviously, if we are not getting any benefit from the technology, there is obviously no point in working with it.

So we wanted to focus in on three areas. The first is around smart contracting. This is the idea of automating the legal agreement between parties and beginning to actually centralize the processing. Some of that may be post-trade, but if you think of things like margin exchange or you think of things about interest rate setting, et cetera then potentially a smart contract, where all that happens centrally

becomes a place to drive efficiencies, particularly in the OTC markets, where we don't have a CCP acting as operational efficiency to all parties in the contract.

The other is trade reporting, which for many years, we have been speaking about in the DLT space.

And, finally, we wanted to talk a little bit about DVP and payment versus payment because, again, we have seen many cases where these are now coming to market or at least fomenting to come into markets in the short term.

So in the example of smart contracts, as I mentioned, what we are talking about here is programmatically defining contracts and actually running them programmatically between the parties to the contracts; for instance, interest rate swap, fixing on LIBOR. Then potentially it is going out to the market. It is reading that LIBOR fix. It is automatically calculating interest accrual. And then it is instructing the parties to move money between themselves, all from one single central point. It facilitates the data entry, the verification, and potentially begins to standardize the information in

order to allow the parties to build out greater automation and, in doing so, to build out greater value in terms of reducing costs and market access.

We put together a very, very simple concept using a credit-default swap, where, effectively, the contract is going out. It is performing mark-to-market. And it is calculating the margin and then requesting the margin exchange between the projection buyer and protection seller as an example of how a smart contract might be deployed and drive efficiencies back into the over-the-counter marketplace.

The second example, which has had, actually, a lot of discussion for many years by many of the providers, is around trade reporting. I want to emphasize, you know, in trade reporting, the challenge internationally has been the lack of standards or agreement or harmonization around the data attributes. And so the thesis here is that by moving two centralized contracts, obviously the firms themselves begin to adopt standards. And so as regulatory bodies taking in that reporting information, it is a chance for you to piggyback off of that standardization

because we are coming there to process, you are coming there to read. We are all motivated, highly motivated, to converge on structured data and standardized data that we all know how to interpret and know how to use.

The next emerging area is in payments. And here we see quite a bit of discussion. Ubin and Jasper, for those who aren't familiar, are initiatives by the Monetary Authority of Singapore and the Bank of Canada around using digital currency within the Central Bank framework, set down as fiat. We have seen private initiatives, like the universal settlement coin, where several banks have gotten together looking to develop coin backed with fiat but acting as a token for things like 24-hour settlement. J.P. Morgan has recently announced the use of a JPMCoin or JPM token for dollar settlement locally. HSBC, ourselves, are using the DLT for foreign exchange, doing cross-border settlements throughout the HSBC organization. IBM has recently announced their payment initiative called World Wire, Blockchain World Wire. And IHS Markit is working on a payments initiative in the structured-loan area called Stax, where, again, people are looking to bring money

in and facilitate real-time delivery or real-time payment amongst the parties. And we can see this is being foundational and extended out into delivery versus payment. If you think of, say, commodities futures coming in, the ability to raise cash in real time as they take receipt of the agricultural goods end up being supplied on the back of that, of that futures contract.

So as a sub-working group, we did have a few steps or recommendations we wanted to put forward and get the TAC's advice on. The first was the idea to study which aspects of derivatives trading can benefit from DLT. Obviously, this allows for a derivative focus where the Commission may want to promote the use or adoption of DLT in reducing systemic risk and/or promoting certain outcomes in the market structure.

We have seen already but we continue to encourage the use of public and private pilots of this technology and other technologies in order to transform the market structure; coordination with the industry to facilitate understanding of the switching benefits, costs and barriers -- in particular, I have noted the

conversation on small firms versus big firms -- the consideration on migration and adoption patterns of the technology, right? We don't want to bring in something to the market structure that, say, only the big firms can invest in and, therefore, all of the benefits accrue to the large firms. But it is really considering if it were to roll out, if it is a benefit, how do we do it in such a way that all firms have equal access or near equal access to those benefits?

It would also be beneficial if the CFTC would give some positive words around DLT and the DLT adoption. It is not that it is being hindered now. But certainly part of the analysis in going live or bringing to production is a review of the regulation. And certainly there is sensitivity to how the regulator may feel about the use of such technology in supporting the activities that the parties are rolling out. So where the Commission could make positive noise, that may accelerate for some firms their ability to bring it to market as it overcomes that little bit of due diligence of just having the conversation around how you feel about the use of the technology to support the

activity that they are pursuing.

Finally -- and I think trade reporting also bore this out, but international coordination, again, to create common standards and ensure interoperability internationally is hugely important, particularly for the OTC markets, to ensure liquidity and ensure cross-border compatibility as we move from jurisdiction to jurisdiction.

And, finally, we would recommend the establishment of criteria for evaluating the impact of the smart contract technologies on safety and soundness of the individual institutions as well as the systemic risk, that it may be reducing and/or increasing. And, in particular, we were thinking about things such as collateral and margin. If we are able to reduce or create more certainty around the movement of funds, the valuation of the product, potentially capital ratios could come down. And, even within clearinghouses themselves, again, if we are able to create more efficiency and greater transparency as to the availability of settlement funds and/or goods, then potentially, again, the capital buffers could be

addressed and/or reduced. But, again, you need to take into account the entire system and stability and role these individual entities may be playing in the marketplace.

And I will hand over to --

MS. KRUSE: Thanks, Jesse.

Commissioners and members of the TAC, thank you for the opportunity to participate in today's session. I would like to introduce you to the ISDA Common Domain Model. Today, I will discuss what the CDM is, why we are doing it, and the benefits for the market participants and regulators who choose to use CDM.

The DLT technology opportunities that my fellow panelists have discussed have one thing in common. They all need a representation for the transactions and the events that impact those transactions through their lifecycles. Each one of the tech providers could develop their own model for representing derivatives transactions and their events, but then user would have to build individually to different languages. These platforms would not be

interoperable, nor would the builds be portable. The CDM can solve this.

So why did ISDA set out on a path to build the CDM? Well, derivatives market participants are looking at ways to increase accuracy, improve efficiency, and reduce the cost of processing their derivatives transactions. There is enormous potential for new tech, as we have heard, to innovate and help meet those demands, but it won't be realized in the same way if you don't have a common blueprint for representing the underlying transactions that ties back to the ISDA legal terminology that underpins those trades. So in walks the CDM.

CDM is a machine-readable and machine-executable data model for derivatives products, processes, and calculations. It is not a document that you read and implement. Rather, it is code that can be downloaded in different languages and implemented directly and formerly as a library for building systems and derivatives markets.

Think of it as the Google Translate for derivatives. Currently firms represent products and

processes in their own languages, which makes it difficult for firms to confirm, verify, and reconcile transactions and difficult for regulators to oversee them. Also, the disparity can be resolved if firms use a common language or a blueprint when they first book those transactions or if different representations can be converted into a common language by using electronic code, like the CDM.

The CDM uses a composable approach. Both the product and the event model provide components from which more complex things are built. So we have simple events that make up more complex business processes. On the far right of the screen, this is an exercise. And you have a before and after representation of the exercise. So CDM has a full lineage of the lifecycle of a transaction and the processes that impact it.

We also have payouts, which are used to create objects which put together make products. If you look at the far right of the diagram, on the top, you can see the different types of payouts. If you put together an interest rate payout and equity payout, you get an equity swap.

We also have ISDA definitions as codes for things like interest rate calculations. On the bottom, you can see the formula for fixed amounts. So you can actually execute that payment amount within the CDM. It is the bottom up approach for the CDM that makes it unique. The model captures the economic components for the payouts of the transaction, rather than looking at the labels that might usually sit at the top of the data model, for instance, asset class or product type. Because you are looking at the underlying elements, you are not going to get caught up in labeling differences that can come from parties booking a trade on a different desk or through a different trading system.

So what is the latest on CDM? We have just published CDM 2.0. That was on March 20th. The previous version, 1.0, was released last year for testing. Now we have a fuller representation of credit and interest rates, a more complete code for ISDA definitions for calculations and day-count fractions, an area that our members break on a lot. But, most importantly, the CDM 2.0 is now open-source. We have made the code available to anyone who wants to download

it. And since last week, 168 new users have registered from 124 different entities.

So why are we making it open-source? Well, the model is ready, frankly, for use by market participants and technology providers. Providing it as an open-source code extends the user community for CDM, which will increase opportunities for applying applications of the CDM and result in additional feedback to us to help us improve the model.

The benefits of CDM. So what can it do for both market participants and dealers? First, it can enhance interoperability and straight-through processing. It is really a key enabler for interoperability between systems and services, laying the groundwork for STP.

It can give regulators better oversight. The CDM promotes transparency and alignment between regulators and market participants. For example, trade reporting, as Jesse was speaking to, or stress testing could be met by specifying requirements via CDM code. This would drastically improve the integrity of the regulatory data by removing the interpretation risk

that leads to differences.

Finally, we can create an environment for innovation for financial markets. Use of the CDM can speed up development of new technology solutions for derivatives because the providers of these new technologies can focus on what they do best, develop those technologies, rather than figuring out a data model for the derivatives they are looking to represent. Also, it provides the opportunity for operability.

Let’s look at a couple of examples. So clearing is just working with several clearinghouses to develop a model for clearing a transaction that works across all CCPs. Having a single data model for clearing reduces the burden and cost of building to multiple CCPs, thus promoting clearing and also allowing for portability between CCPs, if needed or desired.

Collateral management. An ISDA credit support annex might be shared with two collateral management systems, each responsible for different parts of the margin and collateral process. If the

data and processes are defined in the ISDA CDM, it allow for portability and frictionless interchange of information.

Reporting. Again, global regulators have collaborated extensively on the critical data elements through CPMI and IOSCO. And the CFTC, of course, is leading that charge in their SDR requirements, but there remains a risk that regulators will deviate from the CDE values and that reporting entities will interpret and map to them differently, leaving us with unreliable data quality.

ISDA is working with the FCA on a pilot to develop reporting rules into CDM as a code for uniform implementation. Differing interpretations of when and what to report will be eliminated as firms would only need to provide data, not maintain their own implementation of jurisdiction-specific regulatory logic.

So what is next for the CDM? A full model for the data and processes within the collateral agreements, which can integrate CDM into ISDA Create and other collateral services. ISDA Create is a new

platform that allows users to negotiate and execute ISDA documentation online. An expansion in product scope to cover forwards and FX equities, securities for collateral exchange, and financing transactions, and basic commodity products.

Also, we are working with various technology providers to help integrate the CDM into their platforms, firms like R3 and Digital Assets, who are integrating CDM on their end; also, implementation of the reporting rules, demonstrating the power of CDM to improve data quality and remove interpretation risk in regulatory implementations.

In conclusion, ISDA and the community of CDM users will continue to invest in developing the CDM because we see the transformative opportunities to improve accuracy, increase efficiency, and reduce costs for derivatives users. ISDA is happy to meet with the CFTC staff, solution providers, or any market participants to explore how CDM might be leveraged to address specific processes or business cases.

Thank you.

CHAIRMAN GORELICK: Thank you for your

presentations.

I will now open the floor for questions and discussion with an eye towards evaluating the current approach to the subcommittee's work and whether there are additional elements that the subcommittee should consider as they go forward.

Again, we had some discussion of recommendations here, particularly in Jesse's presentation. And I would urge the members of the committee and the subcommittee to think about those recommendations and make suggestions and comments for possible consideration down the road in formal recommendations that the committee as a whole could vote on.

So, with that, I would like to open it up. It looks like Jennifer has a question. Thank you.

MS. PEVE: Thank you, guys.

So, Shawnna, I have a question for you. In terms of one of the recommendations that was made around adoption, given your expertise in terms of looking or IBM's opportunity to look across sectors, right, in businesses in terms of the different

implementations and adoption rates for DLT and, in particular, in one of the slides that we shared today, it is clear that, you know, financial services, healthcare, and I think oil and gas commodities have a lower actual implementation, adoption rate, versus something like consumer products and manufacturing. So are there any insights that you could bring from your experiences in looking across sectors that would help the financial services industry understand where we might be able to improve our rate of adoption of the technology?

MS. HOFFMAN-CHILDRESS: So as we started to look at the blockchain adoption slide again, the number one thing is to take it in bite-sized pieces. Anything that requires a middleman, start to look at the processes from end to end and see where you can start to add the advanced technologies. Blockchain sometimes is not the answer for everything, but there are answers in other technologies. Maybe it is databases that are local to speed up that process. But, you know, it is kind of that end-to-end that we are all looking at.

And financial services, I think that the

number one step that I would make is to start to look at those processes and see which ones actually end up making sense. So good.

MS. PEVE: So just to follow on on that, I think for me, it is not so much about finding the right use case. I think Charley made a really good point that the use cases that are most applicable are ones where either there is an end-of-life problem with technology, legacy technology, or they are incredibly manual, et cetera. I think finding the use cases is somewhat easy. I think the market behaviors around adoption, particularly in our industry, which is why I think Jesse had brought up if there was some promotion that the CFTC could do around adoption, that that might be helpful. What I am more interested in -- and maybe this is for just the comeback for the subcommittee to talk about -- is, is there something in the manufacturing industry that in their use cases kind of highlights that, you know, they did something that got them to adopt and implement that we haven't necessarily tried in financial services?

MS. HOFFMAN-CHILDRESS: I think the number

one -- well, and we can jump at this, but I think the number one thing that we have seen, especially in manufacturing, is the start-up consortiums where we see many companies coming together and building out those blockchain communities together.

But go ahead, Jesse.

MR. DRENNAN: Yes. I think there are two points to make. One is, if you look in the financial services sector, in particular, I mean, we talked about this, actually, in the sub-working group last week. Basically, blockchain enables collaboration. And the challenge for financial services is we have data barriers and data protection in place, right? As a financial firm, there is just information we are not allowed to share. It is meant to be kept filed away. But this is meant to break that down and start to bring that together, right? So there is that barrier, in particular. And what can we share? When do we share it?

The second thing is the business benefits in DLT are a network effect. And so if we are an early adopter in the network, we are basically betting that

the network is going to be successful and then it is going to have an uplift and we are going to get the benefit from it. So if you turn it around and just say, “I have a business problem. It is a network problem. And, therefore, DLT is applicable in that context,” then forgetting use case and turning up with your DLT box and saying, “Deploy it,” then, actually, the business has an outcome it is looking for. It gets real business benefit. It is an obvious adoption pattern to follow.

The challenge today is that many people are coming and saying, “Look how cool the tech is.” They are not coming in and saying, “You have got a problem. Here is a solution.” And, therefore, the business can adopt it, regardless of how it actually gets implemented.

CHAIRMAN GORELICK: John?

MR. LOTHIAN: So this is a little -- John Lothian, by the way.

This is a little off-the-wall question, which is always kind of expected of me. This is for Charley. I want you to look back in history and look forward

since you have the opportunity to look forward. Take the Bernie Madoff fraud case. How would an implementation of DLT, how it could be in the future, and then how would that case, you know, multi regulators or whatever, how would that have played out differently in a new DLT world?

MR. COOPER: Okay. I haven't seen the Robert De Niro movie on Bernie Madoff. I have to think about it. And I would be happy to come back to the committee with more of an answer. I mean, the question that I would need answered before I answer the question is the extent to which in the ponzi scheme that was the Madoff scandal, were they actually doing real trades and misallocating funds? Were they not doing any trades and just putting out fake financial statements to people?

MR. LOTHIAN: Not doing any trades.

MR. COOPER: So there was no activity going on?

MR. LOTHIAN: The amount of trades that they should have done was in far excess of the number of options in those strikes that actually traded.

MR. COOPER: Got it. Okay. Yes. I mean, I defer to anyone else who has got a thought on that.

I mean, in an event like that, I mean, the CFTC, for instance, is looking at activity on markets. So if they were able to juxtapose next to their market activity sheets, the alleged market activity that the Madoff organization was claiming, they could see the difference. But I don't know the extent to which the CFTC would actually see only one side of that equation. So then the question is, does DLT provide -- so depending on the DLT system you are talking about, many of us have built in the idea of regulator nodes so that they are able to actually sit there as an observer and watch the activity happening in a particular market. But even that would only tell them what was going on in that particular market. And unless they also had an eye on the financial statements or the "audited" financial statements that were being provided to investors, they might not actually see that there was an out-trade, I would guess.

MR. DRENNAN: I think it is slightly different.

MR. COOPER: Go.

MR. DRENNAN: So you have a immutable record, right? So presumably Madoff would have executed at the exchange. That record would have been passed through to him as the custodian but then through to the investor as well. Right? So there is one record that exists, and it is being traced all the way through the ecosystem. And so it should have been or, in theory, it would be impossible for him to have spoofing the records unless he was actually in there and able to spoof the entire blockchain in terms of the transactions he was doing. And it was being certified by the exchange and by any of the other parties in the ecosystem that were supporting that ecosystem.

MS. HOFFMAN-CHILDRESS: And I think that this is also where we start to see the convergence of blockchain and also artificial intelligence. The beauty of artificial intelligence is to be able to automatically predict if and when that is going to happen. So we start to see these technologies working very closely together.

CHAIRMAN GORELICK: Alex?

MR. STEIN: So just a quick follow-up. Except for SMAs, clients don't know all of the trading activity. So you are presuming a visibility to something that doesn't typically exist today.

MR. DRENNAN: Right, but they should know their own, right? So you get your broker's statement. There is no reason why you wouldn't get a fraction of that data record, which is your piece of the execution going through the order. No?

MR. STEIN: But if you have pooled assets, then all you would know is the trading activity accounted for X gain or Y loss.

CHAIRMAN GORELICK: Tom?

MR. CHIPPAS: I have a question for Jesse and a question for Tara. Jesse, with respect to the concern noted in the presentation regarding potential new regulatory views on the outputs of smart contracts, I always find a thought exercise helpful. So if we pretend it is 1999 and the outputs of the data-processing system were Sybase via Store procedures sent on a Mercator messaging agent, would we be asking for the sort of clarification? If we are the output of a

CORBA object, would we be asking for this sort of clarification? I am just curious if in the work the subcommittee did, there were DLT smart contract-specific aspects that drive us to seek this clarity or is it simply because there has been an overload of expert views in the media and other conferences about smart contracts that drove the inquiry?

MR. DRENNAN: I think that -- so that is possible. What we are talking about is moving to centralized processing, really. Right? And when you move to centralized processing because we always talk about distributed ledger but central processing, the issue is actually one of central governance. Right? And so, really, what we are looking at is governance models that the regulators need to opine on where if the code were actually wrong -- and I think we have all seen systems where the code was wrong -- how does the bug correction make its way through? What do you do when parties to the contract actually disagree and don’t want to see that change effected on the contract, which is live? And how does that work its way through? Right?

And so some of that is going to be market practice, but some of that may also require regulatory view on -- I don't know how that goes about happening in order to ensure that it actually happens and it happens in a manner that is safe and sound in terms of the impact on the overall financial market.

MR. CHIPPAS: "Governance" I think is the key word there. And I am going to suggest that a lot of it could be solved through governance. You know, it is an immutable record. It doesn't mean it is an unamendable record, correct, for some of the things you have described. It would be interesting to just think about what is technical versus what is governance because the governance probably will be more long-lived as the technology evolves, as opposed to focusing on the specific technology.

MR. DRENNAN: Sure. I think we found, at least at HSBC, as we looked at the business outcomes many of these are driving, but a number of them can be addressed through policy changes by the regulators. The technology is just a vehicle for facilitating those types of conversations.

MR. CHIPPAS: I agree with that.

Tara, with respect to the CDM, I just want to clarify one point. You mentioned that there are a few vendors implementing the CDM. Those both happen to be DLT vendors. Is the CDM exclusively for DLT or can it be used in other technology bases?

MS. KRUSE: Not at all, right? That is really the value of the CDM, is that it can work across different platforms. But, you know, regardless of whether it is DLT or another type of platform, they can use the same language. And they could still be interoperable if they needed to be.

MR. CHIPPAS: Okay. And then a second question related to the licensing. I think IP has come up in another context today, in other topics. But as we start to merge business process and ownership and technology more and more together, I think it is likely to come up more often.

MS. KRUSE: Yes.

MR. CHIPPAS: Is the concept of the open-source license that has been selected by ISDA such that vendors and other third parties can develop their own

IP on top of it and continue to own that or is it a more non-permissive license whereby any work a third party does has to be contributed back in or maybe you could state which license it is under?

MS. KRUSE: Yes. So it is an open-source license. The end IP, right, stays with ISDA, but what we want to do is allow people to develop CDM and hopefully bring that back to us, right, so that it becomes part of the CDM itself. And then that goes back out to other users so that they are all using the same version of CDM and we retain that consistency.

MR. CHIPPAS: Which open-source license is it?

MS. KRUSE: Say that --

MR. CHIPPAS: Which open-source license is it? Is it GNU or is it Apache or --

MS. KRUSE: No. It is just through ISDA, just, yes, open-source.

MR. CHIPPAS: It might be interesting to clarify that because there are IP ramifications --

MS. KRUSE: Yes.

MR. CHIPPAS: –-- based upon the license that

has been selected, the end result of my questions being that we probably want to encourage third parties to do exactly what you are asking --

MS. KRUSE: Yes.

MR. CHIPPAS: -- but the selections of license and then the support for the open-source project will have a dramatic impact on their desire to invest. And certainly there are many firms, both around this table and not here, that have spent hundreds of millions of dollars over decades developing their platforms. They are probably going to be keenly interested in understanding where open-source and their contributions would lay.

MS. KRUSE: Thank you.

CHAIRMAN GORELICK: Haime, I think you were next.

MR. WORKIE: Thank you. Haime Workie from FINRA again.

This question is for Tara. So with respect to the CDM system, one of the things I found really interesting about it is how it could assist with interoperability. I assume this relates mainly to the

database and not to two technology platforms talking to each other. Can you just clarify that a little bit? In what sense does it help with interoperability? And what challenges are still left?

MS. KRUSE: Yes. So it is about the underlying representation of the derivatives transaction itself and what an event looks like and how that is processed. So that part of the transaction representation would be aligned, regardless of how the platform works or functions.

MR. WORKIE: Is there any instances where this is actually being used live now to help, you know, two systems talk with each other in terms of being able to look at the underlying data that you are aware of?

MS. KRUSE: Not yet. We are getting there. There is a number of platforms who have built it out and are starting to get to that point.

CHAIRMAN GORELICK: Larry?

MR. TABB: Larry Tabb.

Kudos, Tara, on CDM. I just wanted -- you know, there was a discussion on network adoption. I want to ask Jennifer, have you guys worked with the

CDM? Because you have got the information warehouse, which is really kind of the data repository there. And how do you guys think about integrating that enhanced data reporting?

MS. PEVE: Yes. So when ISDA started discussions with the industry around CDM, we were certainly engaged. We were also pretty far down our development road in terms of our work with Axoni on our trade information warehouse transition to DLT and cloud. So we have been working with ISDA. We have shared our data model with ISDA to incorporate what made sense within the CDM and take feedback so that over time, we can reversion data model so that it becomes more and more like CDM over time, that we couldn't stop our progress in terms of our existing development work, but we are working very closely with them.

CHAIRMAN GORELICK: Thank you.

Brad?

MR. LEVY: Thank you. Brad Levy, IHS Markit.

And along the lines of Tom, Tara, I applaud ISDA for the open-sourcing of CDM. And the licensing

is critical to that in terms of the industry getting comfortable building on that. It is nontrivial, very knotty.

Has ISDA considered a contribution to an open-source foundation for both maintenance and management and governance of the protocol or the open source going forward? There are several. I happen to be involved in one of them, but, you know, a captive open source will only take entities so far, which is this is that version. It is open source, but it is still very pinned to an entity, ISDA, versus something maybe more broadly accepted.

MS. KRUSE: Yes. We have had some discussions with FINOS on that front. So it is something we are going to explore further.

MR. LEVY: Okay. Excellent. To be clear, I am chairman of FINOS. So that is full disclosure. There you go.

(Laughter.)

MR. LEVY: Not set up, just truly --

(Laughter.)

MR. LEVY: Really not. That was an open

question and a -- thank you. Appreciate the engagement.

CHAIRMAN GORELICK: Gary?

MR. DeWAAL: Gary DeWaal.

Tara, a quick question. I remember reading the paper when it came out with CDM1 and CDM2. And my recollection is that ISDA is not contemplating that all aspects of the ISDA master agreement are suitable for putting on a smart contract. And how do you anticipate parties dealing with a relationship where some of the aspects are subjects of smart contract, some of the aspects are not? How in the end operationally does that work?

MS. KRUSE: I mean, I think it is an iterative process, right? We do hope and envision that eventually, we would have all aspects that we need, right? We are looking at the collateral that would sit behind it. We are looking at, you know, expanding to different product types. So I do think that it would be possible to do all aspects of those terms, you know, via the CDM. It is just a matter of when we get there for parts of it.

MR. DeWAAL: Okay. Then a follow-up on that. So to the extent that things happen automatically -- so, for example, let's assume that there is an assumption of what constitutes an event of force majeure and it is programmed. Obviously something happens immediately because that is the nature of a smart contract. Suppose afterwards people just dispute that things happened the correct way. I presume normal dispute resolution will occur. I am just curious. How do you see that process playing out in real life?

MS. KRUSE: Yes. I mean, it is not a scenario that I have considered yet. And it is something we can look at. But, I mean, one of the good things about CDM is, really, the chance to look at events that sit behind it. And then the question is, you know, could we? You know, could we take into consideration an event like a force majeure that is under the master agreement, acknowledge that as part of the underlying contract? Perhaps. I mean, it is something that we haven't looked at yet.

CHAIRMAN GORELICK: Okay. Any further questions or comments?

(No response.)

CHAIRMAN GORELICK: Okay. Well, thank you, everybody, for the discussion we have had today. We have had a lot of good updates and feedback from our subcommittees. I thank everyone on the phone for their participation. We look forward to the ongoing work of our subcommittees and efforts of the broader Technology Advisory Committee.

I would like to now turn back to Commissioner Quintenz so that he can facilitate closing remarks.

COMMISSIONER QUINTENZ: Thank you so much, Richard.

Let me turn to my fellow commissioners and the Office of the Chairman and see if Mike has any closing thoughts.

MR. GILL: No, no. Just thank you very much for everyone's participation. It has been very, very helpful. So I appreciate it.

COMMISSIONER QUINTENZ: Great.

Commissioner Berkovitz?

COMMISSIONER BERKOVITZ: Thank you, Commissioner Quintenz.

This has been a very informative day. All the panels were extremely informative and educational from my perspective. So I thank all of the participants for your time and travel and energy to help us out here. And I thank Richard and Dan as well for your assistance in making this meeting successful. Thank you.

COMMISSIONER QUINTENZ: Thank you very much.

I would just like to add a couple of comments. If you think about where we started the day and all of the information and thoughts and research and questions that we have been able to elicit out of the discussion and put into the public sphere, I mean, I think it is -- not only is it remarkable, but it shows the value of having advisory committees within this context and advising this Commission, if not the government generally. So thank you for proving that out today.

There is a lot more work to be done, as I think we have seen through the presentations. There were a lot of questions asked. There were a lot of requests for additional feedback. There were

recommendations that the full committee members will need to process and hopefully get their thoughts back to the subcommittees so that we can in our next meetings maybe take some votes of the full committee that can actually make official recommendations to the CFTC, which is yet another prove-out of the expertise here.

So one last thank you to all of our presenters, who were very well-prepared and did a lot of work in advance; all of our subcommittee members for participating in those discussions; you our full committee members; and the staff and how hard they have worked to prepare for today; and our new chairman, Richard Gorelick, who I think did a great job facilitating the discussion. So thanks to all of you.

I will now turn it back to our DFO, Dan Gorfine, to execute the remainder of his official duties.

MR. GORFINE: Thank you for all attending. The meeting is now adjourned.

(Whereupon, at 3:13 p.m., the meeting was adjourned.)