1   U.S. COMMODITY FUTURES TRADING COMMISSION (CFTC)

2

3   TECHNICAL ADVISORY COMMITTEE (TAC)

4

5   Wednesday, February 26, 2020

6   9:58 a.m.

7

8   Commodity Futures Trading Commission - CFTC

9   Three Lafayette Centre

10   1155 21st Street, N.W.

11   Washington, D.C. 20581

12

13

14   BEFORE:

15   Brian D. Quintenz, TAC Sponsor and

16   Commissioner, CFTC

17   Richard Gorelick, Chairperson

18   ALSO PRESENT:

19   Rostin Behnam, Commissioner, CFTC

20   Dan M. Berkovitz, Commissioner, CFTC

21

22

1   AGENDA

21

22

17

18

19

20

21

22

1   P R O C E E D I N G S

2   MS. TENTE: Good morning, everyone. As the

3   TAC designated Federal officer, I am happy to call this

4   meeting to order.

5   Just three logistical items before we begin.

6   First, please turn your microphone on and off to speak.

7   Second, for anybody on the phone line dialing in,

8   please mute your phone until you are ready to speak.

9   And, third, when you are ready to be recognized during

10   a discussion, please flip your name tent so Richard can

11   recognize you and give you the floor.

12   We have a lot of panels for today. And

13   before we get started, Commissioner Quintenz, sponsor

14   of the TAC, will give his opening remarks.

15   COMMISSIONER QUINTENZ: Thank you, Meghan.

16   And good morning to everybody. Welcome to our fifth

17   meeting of the Technology Advisory Committee. It is

18   wonderful to have all of you. Again, I would like to

19   thank all of our guest presenters today for their work

20   leading up to this and the valuable information and

21   dialogue that their conversation is going to generate

22   here as well as afterward within the Commission. I

1 would like to thank the members of the committee for

2 being here, members of our subcommittees for traveling

3 in and being with us today, as well as my fellow

4 commissioners. And Commissioner Berkovitz is -- I did

5 receive the sincere regrets of both the chairman and

6 Commissioner Stump, who are traveling overseas today.

7 I know that they would like to be with us.

8   As Meghan said, we do have a lot of ground to

9 cover. We are going to hear presentations on wide-

10 ranging and timely topics, including audit trail

11 requirements, stablecoins, specific applications of

12 ISDA's common domain model, the latest in

13 cryptocurrency insurance and custody best practices,

14 updates regarding a cryptocurrency self-regulatory

15 organization effort. At the end of the meeting, the

16 Cybersecurity Subcommittee is going to present its

17 recommendation that the CFTC join with other

18 organizations in making a statement of support for the

19 Financial Services Sector Coordinating Council

20 cybersecurity profile. The TAC will then discuss and

21 vote on that recommendation.

22   So, first, on audit trail requirements, audit

1 trail requirements are designed to provide the

2 Commission with information necessary to reconstruct

3 how a transaction was executed after the fact. These

4 records are critical to the Commission's ability to

5 conduct surveillance inquiries and investigations in

6 order to protect customers and ensure market integrity.

7 However, the Commission's current audit trail

8 requirements are in some respects redundant, placing

9 similar recordkeeping and review obligations on FCMs,

10 exchanges, and exchange members. Those overlapping

11 requirements impose significant costs on market

12 participants and exchanges, which must each store and

13 maintain massive amounts of duplicative transactional

14 data.

15   To address some of these issues, the FIA

16 formed an audit trail working group. The panel before

17 us today, our first panel, is going to present that

18 working group's recommendations regarding how current

19 audit trail requirements can be streamlined and made

20 more cost-effective.

21   Our second panel is going to present on the

22 stablecoin landscape. Although the definition of a

1   stablecoin is still evolving and I am not sure it is

2   actually the correct terminology, stablecoins are

3   commonly thought of as a class of digital currencies

4   that seek to offer price stability against another

5   asset, frequently by being backed by that asset in

6   reserve, like fiat currencies or certain physical

7   commodities. In the furtherance of providing such

8   correlated value, stablecoins have the potential

9   through tokenization to function as a viable, liquid

10 medium of exchange and serve as powerful enablers of

11 smart contracts. Stablecoins are early in maturation,

12 and our panel will discuss several developing

13 stablecoins.

14   First, we are going to hear from Mr. Charles

15 Cascarilla, CEO and founder of Paxos. Mr. Cascarilla

16 will discuss two of Paxos' current stablecoin projects:

17 the Paxos Standard, or PAX, which is a digital dollar,

18 backed one-to-one with the U.S. dollar; and PAX Gold,

19 which is a digital dollar backed by gold.

20   We will also hear from Eddie Wen, global head

21 of digital markets, about the JPM Coin currently under

22 development. JPM Coin is designed to be a digital

1   representation of U.S. dollars held in designated

2   accounts at JPMorgan Chase. They can be used for

3   instantaneous payment transfers on the blockchain

4   between institutional JPM clients.

5   Third, Mr. Steven Becker, president and chief

6   operating officer of the MakerDAO Foundation, will

7   provide an overview of decentralized finance, or DeFi,

8   including some of the benefits and misconceptions

9   associated with decentralized protocols, as well as

10   MakerDAO's Dai stablecoin.

11   And, finally, Mr. Tomasso Mancini-Griffoli,

12   the division chief at the IMF in their Monetary and

13   Capital Markets Department, will provide an overview of

14   some of the public policy considerations implicated by

15   stablecoins: financial stability, monetary policy

16   control, privacy, competition, efficiency, consumer

17   protection, and financial integrity.

18   Next, on our next panel, Ian Sloyan, a

19   director of market infrastructure and technology at

20   ISDA, will present on some applications of the ISDA

21   common domain model, or CDM. Mr. Sloyan will

22   demonstrate via a live run how a swap trade could be

1 reported using ISDA CDM to satisfy regulatory

2 requirements of the CFTC. By providing market

3 participants with an openly available digital code that

4 they can then implement in their own reporting engines

5 and technology platforms, CDM aims to increase the

6 consistency and integrity of reporting.

7   Mr. Sloyan is also going to present on how

8 the CDM is being applied to improve efficiencies in

9 collateral management.

10   Our fourth panel will discuss how insurance

11 underwriting standards are driving best practices for

12 cryptocurrency custody. First, we will hear from James

13 Knox, managing director and technology and

14 communications industry regional practice leader for

15 Aon. Mr. Knox will explain how the need to secure

16 affordable insurance policies for digital assets is

17 leading to an understanding among insurers,

18 intermediaries, and platforms about cryptocurrency

19 custody best practices.

20   We will also hear from Mr. Itay Malinger,

21 co-founder and CEO of Curv, who will discuss some of

22 the current challenges associated with cryptocurrency

1 custody. Mr. Malinger will discuss how multi-party

2 computations or the ability of multiple parties to

3 jointly perform mathematical computations without any

4 party revealing confidential information to others may

5 assist firms in developing custody solutions.

6   The presenters on our fifth panel will

7 provide updates on their efforts to create an SRO-like

8 governance structure for the digital asset and

9 cryptocurrency trading marketplace. Given the lack of

10 Federal market regulatory oversight in the digital

11 asset-trading environment, I have long called for and

12 been a vocal proponent of a private sector, multi-

13 platform-based solution to furthering market integrity

14 through an SRO-like organization. Today we will hear

15 from three groups which have made substantial progress

16 in advancing this concept and furthering this dialogue:

17 the Virtual Commodity Association, represented by their

18 president, Mr. Yusuf Hussain; Global Digital Finance,

19 represented by their board member Jeff Bandman; and the

20 Association for Digital Asset Markets, represented by

21 their founding board member Brad Vopni. Each group has

22 their own membership and focus, and I am excited to

1 hear about their progress, their goals, and ongoing

2 challenges in promoting market integrity in the digital

3 asset-trading environment.

4   And, finally, the Cybersecurity Subcommittee

5 will present a recommendation for consideration to the

6 full TAC that the CFTC should issue a statement of

7 support for the FSSCC cyber profile.

8   Before concluding, I would, as always, like

9 to recognize Meghan Tente, Jorge Herrada, John

10 Coughlan, Scott Sloan, and Phil Raimondi for their

11 tireless efforts in making today possible and leading

12 all of the dialogue throughout the year that leads up

13 to our meetings. And I would like to express my deep

14 appreciation to Richard Gorelick, the TAC chair, for

15 his leadership, expertise, and willingness to give so

16 generously of his time to this committee's work.

17   Thank you, Meghan. I will turn it back over

18 to you.

19   MS. TENTE: Thank you, Commissioner Quintenz.

20   We will turn it over to Commissioner Behnam

21 for any opening remarks.

22   COMMISSIONER BEHNAM: Thank you, Meghan.

1   Good morning, everyone. Great to see

2   everyone here at the CFTC. I don't have any major

3   remarks, but I do want to thank Commissioner Quintenz

4   for his leadership, Meghan and Richard also for your

5   leadership here, certainly a full day, a very

6   interesting day, one that I think we will all benefit

7   from. And, as I say many times at these advisory

8   committees, it cannot be said enough how much the

9   Commission benefits from this dialogue, from your

10 engagement, and us learning from you about what is

11 going on in the marketplace and how we need to be

12 flexible and also need to adjust on the fly, really, in

13 order to keep up with the market and the evolution of

14 technology.

15   So looking forward to today's discussion and

16 certainly looking forward to future engagement. Thank

17 you again.

18   MS. TENTE: Thank you.

19   And now Commissioner Berkovitz for anyopening

20 remarks.

21   COMMISSIONER BERKOVITZ: Thank you, Meghan.

22 And thank you, Commissioner Quintenz, for sponsoring

1 this meeting. Meghan, I hope you got some sleep in the

2 past few days. This is out of the frying pan into the

3 fire. And thank you also, Richard, for your work on

4 this committee. And thanks, of course, to all of the

5 committee members and the presenters today for the work

6 you put into this. It is absolutely critical, in

7 particular with respect to technology, obviously with

8 respect to areas, too, but technology and some of the

9 topics that we are going to be discussing today are so

10 fast-moving. And for us to keep up with it, it is

11 really critical that we have the most up-to-date

12 information from the most knowledgeable people. So we

13 really do appreciate the time and the volunteer effort

14 you put into making these presentations.

15   I think many of the topics here are

16 extraordinary, timely. And, Commissioner Quintenz, I

17 want to thank you for setting forth an agenda full of

18 things that would be very informative. Obviously many

19 developments we read about every day regarding a

20 stablecoin and other developments in cryptocurrency

21 issues, self-regulatory organizations. So these are

22 very timely topics.

1   And, coming on the heels of our meeting last

2   week with respect to data standardization and

3   reporting, several of the other topics here are also in

4   my view extremely important with respect to improving

5   audit trail data, making sure that we collect the best

6   data in the most useful and efficient manner for the

7   market participants. Also, I am very interested in

8   hearing about the ISDA common domain model and

9   standardization on the backend processes and how that

10 can help industry participants and maybe foster

11 compliance in our ability to oversee these markets.

12   So I think these are all very timely topics.

13 I strongly support many of these initiatives. And I am

14 looking forward to the discussion today. Thank you all

15 again.

16   MS. TENTE: Thank you, Commissioner

17 Berkovitz.

18   Now we will turn the meeting over to TAC

19 Chair Richard Gorelick.

20   CHAIR GORELICK: Thank you, Meghan. Thank

21 you, Commissioner Quintenz and Commissioners Behnam and

22 Berkovitz and everyone participating today. We have an

1   interesting lineup. And I would like to get right to

2   it and get the meeting started with the first panel.

3   Our first panel, as Commissioner Quintenz

4   mentioned, is a presentation from the Futures Industry

5   Association on an overview of their recommendation to

6   streamline existing CFTC audit trail requirements.

7   From the FIA, we have Natalie Tynan, associate general

8   counsel and head of technology documentation strategy;

9   Tammy Botsford, the executive director and assistant

10   general counsel at JPMorgan; Mark Fabian, the vice

11   president for market regulation for ICE Futures U.S.;

12   Jeff Ramsey, the managing director and general counsel

13   at Geneva Trading; and Andrew Vrabel, executive

14   director and global head of investigations at the CME

15   Group.

16   And, with that, I will turn the meeting over

17   to the panel.

18   MS. TYNAN: Thank you. Thanks to the TAC,

19   Commissioner Quintenz, and CFTC staff in general for

20   having us today.

21   I will skip introductions since we just ran

22   through that and get right to a little bit of the

1   background about FIA's audit trial working group.

2   So our working group is comprised of

3   representatives from FCMs, DCMs, and principal trading

4   firms.

5   In October of 2018, representatives from our

6   group met with Commissioner Quintenz as sponsor of the

7   TAC as well as senior members of CFTC staff in the

8   Division of Enforcement and Division of Market

9   Oversight to share our concerns about audit trail

10 recordkeeping as it currently stands and, you know,

11 offer some recommendations.

12   Since then, we have continued to work on

13 those recommendations internally. And in January of

14 2020, we submitted a letter to the CFTC, to

15 Commissioner Quintenz, as well as the directors of

16 DSIO, DMO, and DCR laying out our recommendations. And

17 that is what we will walk through with you here today.

18   So as a brief overview, I guess I would say

19 there are a few high-level thematic points. Right?

20 One is that we are interested in trying to streamline

21 the audit trail requirements generally. That involves

22 making things more efficient and eliminating

1 redundancies. And we have four primary recommendations

2 in that regard.

3   The first is to amend regulation 38.553 to

4 eliminate the requirement that DCMs conduct annual

5 audit trail reviews. The second is to amend regulation

6 38.552 to remove specific elements of an adequate

7 transaction database. The third is to confirm that

8 DCMs may maintain records of tier 1 data on behalf of

9 FCMs and other trading participants. And the fourth is

10 to recommend that DCMs should amend their rules to

11 confirm that clearing FCMs don't have to maintain

12 records of orders that are transmitted directly into

13 the DCM trading system by direct-access customers.

14   It is important to note at the outset that we

15 are proposing modifications to Part 38, but we are not

16 proposing changes to the existing recordkeeping

17 requirements under regulations 1.31 and 1.35. And we

18 will walk through that in a little more detail.

19   I am going to turn it over to Mark now to

20 walk through our current regulatory requirements and

21 kind of give us the lay of the land.

22   MR. FABIAN: Thank you, Natalie.

1   So our next slide talks about the existing

2 requirements. Currently Commission rule 1.31 and 1.35

3 require the retention and maintenance of records

4 required to be made and kept in accordance with the CEA

5 for a period of no less than five years, including

6 order message and transaction data. All FCMs, retail

7 foreign exchange dealers and certain introducing

8 brokers and members of DCMs are still required to

9 maintain their respective audit trail records in

10 accordance with regs 1.31 and 1.35.

11   Regulations 38.551 through 553 pertain to the

12 audit trail requirements specific to DCMs. So that is

13 the key point here today. We are not looking to make

14 any changes to 131 or 135. The specific target here is

15 the regulations under Part 38 and specifically Part

16 38.552 and 553. We are not recommending any change to

17 551, which basically requires DCMs to keep and maintain

18 an audit trail that is sufficient to conduct their

19 regulatory requirements under the act in conducting

20 investigations and thorough investigations. This

21 requires, this part of the rule requires, that DCMs

22 maintain records of the audit trail from the time of

1 receipt of an order message by the DCM to any messages

2 that are then returned from the FCM to any

3 participants. So, again, this part of the rule is

4 specific to the DCMs and what their requirements are in

5 terms of audit trail. We have confirmed this with the

6 DMO folks to make sure that, you know, we have a clear

7 understanding of the audit trail records that are

8 required to be maintained by the DCM. And today we are

9 not proposing a change to 551. It is 552 and 553.

10   So regulation 552 states that a DCM's audit

11 trail must include an electronic transaction history

12 database. An adequate transaction history database

13 includes a history of all trades executed via open

14 outcry or via entry into an electronic trading system,

15 and all orders entered into an electronic trading

16 system, including order modifications and

17 cancellations. This regulation also lays out specific

18 pieces of information that are required as part of that

19 history database, including a CTI codes, or customer

20 type indicator code.

21   Regulation 38.553, enforcement of audit trail

22 requirements, requires that a DCM enforce its audit

1 trail rules by conducting at least on an annual basis a

2 review of all members, firms, and persons subject to

3 the recordkeeping rules to verify compliance with the

4 DCM's audit trail and recordkeeping requirements.

5 These audits must include reviews of randomly selected

6 samples of frontend audit trail data and order routing

7 system data; a review of the process by which the

8 identifications are assigned to users and maintained;

9 and a review of usage patterns associated with user

10 identifications to monitor for violations of user

11 identification rules; and reviews of account numbers

12 and customer type indicator codes to test for accuracy

13 and improper use.

14   Currently, we conduct these annual reviews

15 and they may be conducted slightly differently by the

16 various DCMs. We have rules that prescribe exactly

17 what the DCMs require from our participants.

18 Generally, it is the same information. However, the

19 format that is requested or the DCMs required to be

20 maintained can be slightly different across the DCMs.

21   And, just for example, when ICE does an

22 annual audit trail review, we basically do a sample by

1   going to each clearing firm and asking them for a

2   sample order from every pathway that they receive an

3   order transmission through. So we go through our

4   systems. We identify order records from each of the

5   different pathways. And we send that request to the

6   clearing firm, who then is responsible for pulling that

7   data, either from their own records or from clients

8   that they have that are direct-access clients, and

9   providing it to the exchange in the format requested by

10 the exchange. So what that sometimes requires is that

11 they have to modify the records that they maintain in a

12 native format to fit each of the different DCMs'

13 requirements in terms of the types of audit trail.

14 And, specifically, I will give you a good example.

15   The CME has an operator ID tag that it refers

16 to as tag 50; whereas, ICE has the same operator tag,

17 but we refer to it as a tag 116. It basically

18 identifies the same type of individual. And that is

19 just the way our systems are set up and different,

20 although, actually, that piece of information

21 represents the same requirement to identify who the

22 operator or the button pusher is entering an order,

1   whether that be a manual trade or an automated system.

2   So through that process, it takes our

3   compliance staff a significant amount of time to

4   compile that information and send out the requests to

5   the various clearing firms to have them produce the

6   information to us. And on the other side of that coin,

7   it takes them a long time to pull the information and

8   then convert it to the standard format that each of the

9   various DCMs is looking at.

10   So what we are looking at today is to try and

11   relieve that annual audit trail requirement for a

12   couple of reasons: one, because the DCM already has

13   most of that data that they need; and, two, it is very

14   detailed information.

15   So just to kind of set the stage for what we

16   are going to be talking about here and what we have

17   done, the working group has done, is tried to identify

18   and differentiate the data that the DCM maintains

19   versus the data that the DCM does not maintain. Now,

20   as we have said from the onset, reg 1.31 and 1.35

21   require entities to maintain their audit trail. That

22   is inclusive of what we are going to be calling tier 1

1   and tier 2, but specific to DCMs, the data maintained

2   for audit trail purposes by DCMs is defined as tier 1.

3   And if we change to the next slide, this is a

4   schematic representation. And, basically, tier 1 data

5   is electronic order messages transmitted from the

6   client application servers connected to the exchange

7   electronic system to the exchange system and from the

8   exchange electronic trading system to the connected

9   client application server. So that is going to be the

10 red highlighted oval on the righthand side of your

11 screen or your slide package.

12   Tier 2 is all other order messages not

13 included in the definition of tier 1 that are

14 additionally required to be maintained under regs 1.31

15 and 1.35. So the tier 1 data that the exchanges and

16 the DCMs maintain is highly detailed. And we use that

17 for our investigation research on a daily basis. In

18 fact, it serves the purpose of us being able to conduct

19 investigations and complete them based on our own DCM-

20 stored information in 99 percent or better of the cases

21 that we bring, either to a variety of committees or

22 otherwise. So there is a very, very small piece that

1 would be considered tier 2, which the exchange does not

2 maintain and for which it would go to participants,

3 specifically clearing members to or FCMs to get that

4 information.

5   I think I will turn it over. I think we have

6 done a pretty good job of defining what tier 1 is. It

7 is basically within the DCM domain, and it is the audit

8 trail the DCM has now. It collects and maintains

9 consistent with reg 38.551. I think I would like to

10 turn it over to Jeff just to give us an idea of what

11 types of things would be covered in a tier 2. And we

12 can also provide you with the example of, a basic

13 example of, what tier 2 is.

14   MR. RAMSEY: Thanks, Mark.

15   So tier 2 data I like to think of sort of the

16 backstage activity before the orders are actually sent

17 to the exchange, so things like if a trading system at

18 the trading firm or at the user is -- say, for example,

19 using an iceberg strategy, where it is going to send in

20 a one-lot and then refill that up to 50 times as it

21 gets filled there. The log and the programming behind

22 that sequence would be tier 2 data. The tier 1 data

1   would be the moment that that order is actually

2   launched to the exchange. That would be captured by

3   the DCM and put through, captured through the tier 1

4   retention.

5   Another example would be, for example, like a

6   stop-loss logic, where there is a certain price

7   threshold or a loss threshold within the trading system

8   that then determines it is time for me to launch an

9   order to resolve this issue or to get out of the trade.

10 So I like to think of it as what is sort of housed

11 within the trading system, the logic there that then

12 triggers that data that the exchange sees in terms of

13 cancels, modifies orders and fills.

14   MR. FABIAN: Thanks, Jeff.

15   So, as an example, if you don't mind flipping

16 to the next slide, we have used the iceberg scenario,

17 where a firm offers a front-end trading application to

18 its clients. The trading application has functionality

19 that allows the client to synthetically create an

20 iceberg order, where one portion of the total quantity

21 is displayed to the market at a time.

22   So, for example, a client electronically

1 sends an instruction to the trading application that

2 sits outside the DCM to sell 1,000 contracts. This is

3 referred to as a parent order. It is then designed to

4 display only 50 contracts at a time to the market,

5 which is referred to as the child order. So in this

6 scenario, the 1,000-lot order is maintained at the tier

7 2 level. When it sends each of those child 50-lot

8 orders, the 50-lot order is the record that the DCM

9 receives, maintains that. It goes through the

10 transaction process. And the confirm is then sent back

11 to the firm submitting it as a 50-lot transaction

12 assuming it is filled in its entirety.

13   Then the client instruction to the trading

14 application to sell the 1,000 on the iceberg is the

15 tier 2 piece of data, where each of those 50-lot

16 pieces, or child orders, rests in the DCM world. So,

17 theoretically, you have got 20 -- if the entire order

18 gets filled, iceberg order gets filled, you have got 20

19 50-lot order records in the DCM or tier 1-level data

20 and 1,000-lot record in the tier 2 data. I hope that

21 is an example that -- we tried to figure out one that

22 we thought would be most relevant an example. And,

1   also, the stop-loss example is a very good one as well.

2   So at this time, I think I would like to turn

3   it over to Andrew to go through our proposed changes to

4   the regs.

5   MR. VRABEL: The first recommendation of the

6   working group is to eliminate the requirement that DCMs

7   perform annual recordkeeping reviews of firms. It is

8   the position of the working group that these reviews

9   don't add value to the DCMs' existing processes for

10 identifying market abuses, customer abuses, or other

11 trading infractions. But to underscore what Mark said

12 earlier related to the identification of market abuses,

13 customer abuses, or trade practice violations, at CME,

14 we do not have a single trade practice program for

15 electronic trading that is reliant on tier 2 data in

16 order to find a violation, not a single program.

17 Everything is reliant on tier 1 audit trail data, which

18 is data the DCMs' already possess because it is the

19 messages that the firms are sending to the DCM and the

20 DCM is sending back to them.

21   The one other thing to note about this that

22 Mark highlighted is that we are not recommending

1   changes to the existing recordkeeping rules 1.31 or

2   1.35.   In the event the DCM does need tier 2 or a

3   higher level audit trail data during the course of a

4   trade practice investigation, we would be able to make

5   that request to firms, just as we do today.

6   There was a question that was presented

7   during the course of the working group's stream of

8   events related to the types of violations that the DCMs

9   today are identifying through their audit trail

10   reviews.   Obviously, each of the DCMs today because of

11   38.553 are required to have from an audit trail

12   examinations of firms.   So let me take a moment and

13   highlight some of the things that we identify in these

14   reviews because it does address our perspective that

15   these are nonvalue-adding types of reviews.

16   Last year, the CME DCMs issued summary fines

17   or letter of warnings in six instances for front-end

18   audit trail errors.   And those errors related to

19   information such as the firm failed to maintain

20   millisecond-level timestamps on their tier 1 trading

21   information.   To us, this is unimportant because we

22   already have timestamps down to the nanosecond level in

1 the exchange of systems. So the fact that a firm

2 failed to maintain that for its own records does not

3 impact our ability to review trade practice violations.

4   Another sort of violation that we brought an

5 action against last year is the firm failed to keep a

6 record of when individual lags of a trade were executed

7 as part of a sprut. Now, obviously, on our side, that

8 helps us reconstruct the trading activities. So we

9 know if a lug was part of a sprut instrument.

10   We have that data because it was executed on

11 our platform. So we obviously know if the order was

12 submitted as a sprut or was it submitted as our rights

13 and filled as a sprut. So, again, that type of data

14 inaccuracy doesn't add value to what we are doing from

15 the DCM perspective to identify trade practice

16 violations.

17   Now, we do have value-adding portions of our

18 audit trial reviews. And these are done through

19 programmatic reviews to identify data anomalies. So

20 this is aside from our annual reviews of firms' audit

21 trail recordkeeping. We have programs that operate

22 across all of our participants that are subject to

1 recordkeeping violations to validate the accuracy of

2 the data they are actually submitting to us.

3   So an example, one of those programs, one of

4 our most recently implemented programs, is we are

5 validating the country of origin that firms submit on

6 order messages. The reason why it is important to us

7 is that we have trade practice programs and reviews

8 that are dependent on the country of origin that the

9 firm is submitting. So we need to validate or we have

10 an interest in validating the accuracy of that

11 information.

12   That is not something that is covered in the

13 frontend audit trail. That is covered in the trade

14 practice or an audit trail program specifically

15 designed to identify violations. Other types of these

16 programs that we employ relate to the inaccurate use of

17 a tag 50 or a user identification. So we have programs

18 that are designed to identify instances where someone

19 may be using another person's user ID. That is

20 critically important for us when it comes to

21 reconstructing the transactions in the marketplace and

22 identifying customer and market abuses. Again, those

1   are things that we do not propose changing. Those will

2   continue to exist in the new model.

3   This is highlighted in the second bullet,

4   where we believe that the regulatory focus should be on

5   the DCMs' programs that are designed to identify data

6   anomalies or violations from a data integrity

7   perspective, rather than going out to the firm and

8   validating that they have the same data that we already

9   possess. Obviously, industry benefit from doing this

10 is that it eliminates the burdens of complying with the

11 exchange from audit trail examinations.

12   If we can go to the --

13   MS. BOTSFORD: So from exchanges' point of

14 view, they have to go out to every member and everyone

15 who is required to retain audit trail and actually make

16 sure not to duplicate what we already have. And that

17 is largely just an exercise in is it copied properly.

18 And it is not discovering anything that they typically

19 would come to us for an investigation, but on top of

20 that, they are going out to every member. We have got

21 them all coming in to us as well once a year and tying

22 people up, saying, "Hey, have we copied this from here

1   to here? And are we retaining it?" when I think there

2   is a lot more value-add to be had from taking those

3   resources and putting them into data integrity, rather

4   than are we a good monkey scribe for this kind of

5   thing.

6   MR. VRABEL: The second proposal relates to

7   making modifications to 38.552. Just a little bit of

8   background. This revived effort to evaluate the audit

9   trail reviews actually began back with Project KISS

10   several years ago where there was an interest in

11   reducing regulatory burdens that aren't adding value to

12   the reviews of the DCMs. And one of the first things

13   that was identified across the entire industry was the

14   existence of CTI codes, the customer type indicator.

15   That is actually where all of this began. The customer

16   type indicator historically -- and this is decades ago

17   had value in helping the DCMs reconstruct trading

18   activity, particularly in the trading floor, where the

19   DCMs had obligations to identify instances of

20   customers' orders being abused by brokers who had dual

21   trading privileges.

22   Nowadays the CTI code is largely irrelevant

1   to not only the DCMs' trade practice reviews, but it is

2   also a field that the exchanges can impute and

3   determine what the CTI codes should be based on the

4   membership status of the person submitting the order or

5   the ultimate account where that trade is submitted. So

6   that is where this started. What the working group

7   identified is there are other portions of 38.552 that

8   are redundant to other portions of the CBC's

9   regulations.

10   So just for some background, 38.552 requires

11 that the DCMs maintain an adequate transaction history

12 database and that that database has to include

13 information such as all data that is input into the

14 trade entry or matching system for the transaction to

15 match the customer type indicator code, the timing and

16 sequencing of data, and the identification of each

17 account into which fills are allocated.

18   Now, we are not here to say that those other

19 fields aside from the CTI codes don't have value.

20 Obviously the exchanges have to have the timing and

21 sequencing in order to reconstruct the trading

22 activity. What the working group is positing is that

1 those particular provisions are redundant to other

2 portions of the regulations.

3   For example, 38.551 that Mark touched on

4 briefly at the beginning, specifically provides that

5 the DCMs' audit trail must be sufficient to reconstruct

6 all transactions. So one could read that you would be

7 required to have timing information in order to

8 reconstruct all trading activity.

9   38.551 also requires the DCMs to track

10 customer orders from the time of receipt through filler

11 allocation. So, again, the component of that

12 transaction database requiring that there be

13 information sufficient to identify where trades are

14 allocated is redundant to what is already in 38.551.

15 It is for that reason that we would propose to strike

16 those provisions that specifically proscriptively

17 require the DCMs to maintain particular elements in the

18 audit trail.

19   MS. BOTSFORD: And to give you a further

20 example of why you should be principles-based, rather

21 than proscriptive, aside from the fact that these

22 things go obsolete from time to time and we don't know

 1   what trading will be in another 20 years, as we didn't

 2   know back when this list was put together, the industry

 3   comes together from time to time to create new elements

 4   of the audit trail. And so, for an example, the

 5   industry came together to create tag 1031, which is now

 6   a uniform tag, as opposed to everyone having their own

 7   tag. And that is a designation that tells everyone,

 8   "Was this an electronic order or was this a voice

 9   order?"

10   And there is a difference in the processing

11   in the records that might be retained and the

12   information that the exchange in tier 2 might come to

13   us to look for, and by knowing if it is electronic or

14   voice, they know what to look for. If you are too

15   proscriptive, that kind of thing wouldn't necessarily

16   be mandated as retention.

17   Because we see it as part of the audit trail,

18   we want it to be principles-based so that we would

19   retain it automatically, we do retain it, but we don't

20   know what is going to grow out of blockchain. We don't

21   know what is going to grow out of processing in the

22   future that might be even more efficient than this.

1 And we don't think you should try to describe it and

2 miss the mark.

3   MR. VRABEL: The third matter -- and let me

4 preface this by noting again that the DCMs are required

5 to maintain tier 1 audit trail data. And today the

6 persons subject to 1.35 are required to maintain tier 1

7 audit trail data. This should be the exact same data

8 that two different groups of registrants are required

9 to maintain. There has been an interest expressed to

10 have the CBC confirm that the DCMs could offer a

11 service to firms where the DCMs would be the

12 recordkeeping custodian for the tier 1 audit trail data

13 for whoever would subscribe to that particular service.

14   I would note that this is not a novel

15 concept. Back in 2012, when the CFTC adapted

16 regulations 1.31 and 1.35 to incorporate the definition

17 of swaps or recordkeeping rules related to swaps, the

18 CBC specifically recognized that a person subject to

19 1.35 and 1.31 could rely on a DCM or a SEF to maintain

20 audit trail records. To the extent that the person or

21 the person subject to 1.35 had an agreement in place, a

22 surmising agreement in place, requiring the DCM to

1   maintain those records on their behalf. That was the

2   first thing that an agreement exists.

3   And the second requirement or the second

4   provision was that the person subject to 1.31 and 1.35

5   is still ultimately liable for compliance with those

6   regulations. So they cannot shift the burden to the

7   custodian of records for purposes of 1.31 and 1.35.

8   MS. BOTSFORD: And, just to expand on 1.31, a

9   few years ago when the CFTC made the great step to go

10 and update 1.31 retention requirements to recognize

11 that electronic retention is here and that there is a

12 way to retain it without hiring a technical consultant

13 to keep duplicates of everything that we have, it was

14 streamlined. And it made it a lot easier for FCMs to

15 be able to use an outside vendor or retain it in-house

16 without having to maintain duplicates beyond our BCP,

17 which, of course, we have to do and we have to make

18 those records available. And I think that breaking

19 tier 1 and tier 2 apart and taking tier 1 and having

20 the DCMs retain that on behalf of the industry, it

21 would still be our regulatory requirement, just as it

22 is for the rest of our 131 retention, is just

1   furtherance of the same streamlining and getting rid of

2   the same duplicative cost to the industry, not only in

3   just the cost of retention but the resources in going

4   and reviewing again that this copy matches that copy,

5   which we are never going to be asked for.

6   MR. VRABEL: I will introduce the fourth and

7   then turn it over to Tammy. The current DCM rules put

8   the obligation on the clearing firms to maintain audit

9   trail data on behalf of, at least for purposes of CME,

10   to maintain the audit trail data on behalf of any

11   connection that the clearing firm ultimately guarantees

12   to the clearinghouse, which means that the clearing

13   firms are responsible under exchange rules for

14   maintaining the audit trail for any of those

15   connections.

16   There is an interest from the industry if the

17   DCMs eliminate or if the regulations are adopted to

18   eliminate the requirement the DCMs perform annual audit

19   trail examinations, that there be similar relief for

20   the clearing firms to not be required to maintain that

21   tier 1 data on behalf of the connections that they

22   guarantee.

1   So I will turn it over to Tammy for more

2   insight.

3   MS. BOTSFORD: So essentially what happens

4   now is nobody gets direct access to the exchange

5   without a clearing member authorizing it and

6   guaranteeing it. And as part of that guarantee, we

7   either arrange for some kind of drop copy after the

8   fact for us to try to retain it or for it to go to a

9   third party to retain it on our behalf or for the

10   entity that has requested direct access to retain it

11   for us, all of which is permissible under 131. And

12   this is all electronic.

13   The problem is every time you transfer data,

14   that is an opportunity for loss or corruption. Every

15   time that we get data back in and try to process it, it

16   is an opportunity again for some kind of error or

17   omission. Having this all be at a source that is

18   subject to their own retention requirements and already

19   has that information in-house would be particularly

20   helpful.

21   MS. TYNAN: So I think we will pause there

22   with maybe a little over five minutes left in our time

1 for questions.

2   CHAIR GORELICK: We have got a question from

3 Tim. We will start there.

4   MR. McHENRY: Did you attempt to quantify the

5 costs associated with these audit trail reviews, the

6 duplication that is involved, and all of the

7 infrastructure that is necessary to do it, process it?

8   MR. FABIAN: We did not. However, I can tell

9 you that on the surface in a broad sweep, it takes

10 several of our staff members quite a number of weeks to

11 send out the requests, get the information back,

12 analyze the information to determine the comparison

13 between what we see and what they maintain. And I

14 would say it is several people, multiple manhours. And

15 it can take several months to complete that process.

16 And there is often back and forth with the firms

17 supplying the information as well because in some

18 cases, quite frankly, we request fields 1, 2, 3, 4, and

19 5 and they will send us the information except they

20 have got 4 and 5 or 5 and 6 and there is a process of

21 where you have to kind of sort that out and figure out

22 why it ended up in the wrong field. It is just a

1 matter of different terminology and things of that

2 nature.

3   MS. BOTSFORD: To add on to that, we don't

4 just take the native file format and send it to them.

5 We have to take it, put it in the format required by

6 the exchange, try to make sure we have it all right.

7 Depending on whether there has been a change since the

8 time that was retained and the time that it was

9 requested, the translation table may need to be a

10 different translation table if elements have moved

11 around or been added or been subtracted. So it becomes

12 kind of a little bit of a forensic exercise sometimes.

13   MR. VRABEL: And just from CME's perspective,

14 we have two and a half full-time headcount allocated to

15 frontend audit trail reviews.

16   MR. FABIAN: From the ICE perspective, we

17 don't have dedicated employees. Our analysts do this

18 in addition to their other investigative processes. So

19 if we were able to eliminate this annual review, they

20 could be dedicated to doing other investigative work or

21 to doing further targeted audit trail reviews, such as

22 periodic reviews of authorized trader IDs as the person

1   submitting the order is an individual. So, in other

2   words, the authorized trader ID that we get, does that

3   actually represent an individual or does sometimes that

4   ID operates - identify several individuals, which is a

5   problem for us? So we do spend quite a bit of time

6   focusing on the key elements that we believe are

7   subject to potential issues when supplied to us, as

8   opposed to, is it a five-lot order in the March

9   contract? That is the type of thing that gets covered

10 in conformance testing when a participant connects to

11 the exchange.

12   MS. BOTSFORD: And for the FCMs, typically

13 this is part of someone's job on top of their daily

14 book of work inquiries come in and then need to be

15 prioritized ahead of whatever the daily work is to get

16 it back out on time.

17   CHAIR GORELICK: Larry?

18   MR. TABB: What I would be kind of concerned

19 about -- and I am not sure because I am not that

20 familiar with the audit trail process -- is, you know,

21 there could be problems in three or four places. One,

22 you know, a customer sends an order. And somehow the

1 FCM screws it up and then gets it to the DCM. There is

2 some sort of fraud or some sort of, you know, crazy

3 thing going on within the FCM to the DCM that may be

4 overlooked or whatever. In terms of sponsored access,

5 I am using your ID and you don't know what I am doing.

6   I just want to make sure that if we wind up

7 backing away from some of these rules, that we can

8 backtrack and make sure that, all of a sudden, we don't

9 get a customer inquiry and we can't actually track it

10 back and figure out where the problem is or there is

11 some sort of spoofing going on in the market or

12 somebody is using your MPID and they would call in the

13 equity side. You know, can we be guaranteed or sure

14 that we can cover all of this stuff if we wind up

15 modifying these things?

16   MR. FABIAN: So again, this kind of goes to

17 the tier 1/tier 2 discussion. Right now, tier 2 is not

18 something that -- the audit trail is not something that

19 the DCM has natively in its systems. So as it exists

20 today, even if these proposed changes were to occur, we

21 would still go to the FCMs to get that information. So

22 if that issue exists today, it is going to exist

1   tomorrow if these proposals are undertaken, not that

2   that is a good thing, but it is something that we would

3   have to pursue tier 2 data --

4   MR. TABB: So if we make these changes, the

5   challenges or issues of tracking down these problems or

6   issues would not be any significantly different today

7   as it is tomorrow?

8   MR. FABIAN: No.

9   CHAIR GORELICK: Supurna?

10   MS. VedBRAT: I just had a question about the

11 information that you collect at time of transaction,

12 the tier 1 data. It seems like you are not really

13 dependent just on what the clearing member may have

14 because the actual risk exchange is what has happened

15 on the DCM itself, right? So if they are thinking

16 about the market, the information that you have

17 collected and that is in your system is what is going

18 to, you know, identify the risk that has been

19 exchanged.

20   Now, that information should -- it has

21 multiple checks and balances because I am talking from

22 a client perspective. Once a transaction is done, you

1 are confirming it. You know, there is settlement or

2 what have you, which makes me pause to see that this

3 annual review -- this is just about going in and making

4 sure that there has not been any data alteration or

5 something like that between the periods. But the real

6 information that we need you are getting at time of

7 transaction, you know, perhaps any amendments to it the

8 day after by the time it settles.

9   MR. VRABEL: Well, just to clarify, what we

10 are talking about are billions of order messages

11 submitted to the exchange. From that, you get the

12 cleared transactions and the allocations and the

13 account changes, et cetera. None of that is going to

14 change.

15   MS. VedBRAT: Exactly. So, I mean, what you

16 are requesting on removing the or eliminating the

17 requirement just to ensure that the data is maintained

18 properly and matching whatever you have. Like given

19 the advancements that we have had, you know, in

20 technology in the way these trading strategies have

21 progressed, you can figure out if there has been any

22 type of market abuse because of the information that

1 you gathered when the risk exchange or, you know, maybe

2 a day or two after that. I assume at this point like

3 you do have triggers that should highlight if something

4 out of the ordinary is happening.

5   MR. VRABEL: That is exactly right. I think

6 what you have seen from the DCMs over the course of

7 time is that we move far faster than any regulatory

8 changes.

9   MS. VedBRAT: Yes.

10   MR. VRABEL: So when you look back at the

11 status of DCM audit trail reviews in 2010, when 38.553

12 was proposed, or 2012, when it was adopted, the DCMs,

13 at least CME, did not require an automated versus

14 manual tag on an order submission. You know, that came

15 after the fact, you know, from the DCMs' own

16 initiative.

17   Country of origin. We required that to be a

18 mandatory field populated with accuracy. So I think we

19 have to trust the DCMs are going to require data

20 elements that are necessary for us to preserve the

21 integrity of the markets, irrespective of what the

22 regulations require.

1   CHAIR GORELICK: Okay. I think we have time

2   for one more question. We will go with Tom.

3   MR. CHIPPAS: I will keep it quick. Andrew,

4   with respect to your recommendation number 3, could you

5   just clarify? Is the intent that the DCM tier 1

6   recordkeeping service would be a commercial product of

7   the DCMs or given it is stated the DCMs already have

8   something that you would just take on? It would be

9   probably helpful for participants to understand the

10 intent.

11   MR. VRABEL: It would be a commercial

12 offering. I think that the DCMs today, to be perfectly

13 frank, are still evaluating what the legal and

14 regulatory risks would be to be the recordkeeper or the

15 custodian of records for the entire industry. It may

16 come out that, you know, from a legal perspective, you

17 know, the risk of us being that repository is too great

18 relative to the commercial value of that.

19   MR. CHIPPAS: It might be worthwhile to after

20 you consider that further perhaps make additional

21 recommendations so that the Commission, the staff can

22 think about that because perhaps, you know, joint

1 action could be taken there to both alleviate some of

2 those risks and attendant costs if it doesn't impugn

3 integrity. That is a good suggestion.

4   MR. RAMSEY: If I can just add, too, you

5 know, as a trading participant, we spent a lot of

6 resources maintaining our audit trails as well. And to

7 have a commercial offering, particularly at the DCM,

8 where it is the depository of record, would be very

9 nice to have. It would allow us to streamline a lot of

10 what we do as well.

11   CHAIR GORELICK: Okay. Thank you, everyone

12 from the FIA. And thanks for the questions. We will

13 move now into the second panel, on stablecoins.

14   Good morning. We are going to now continue

15 with an overview of stablecoins followed by

16 presentations on three stablecoins: Paxos Standard,

17 Dai, and JPM Coin. Our presenters are Charles

18 Cascarilla, chief executive officer and co-founder of

19 Paxos; Steven Becker, president and chief operating

20 officer at the MakerDAO Foundation; Eddie Wen, the

21 global head of digital markets at JPMorgan; and Tommaso

22 Mancini-Griffoli, deputy division chief in the Monetary

1   and Capital Markets Department at the IMF.

2   I will now turn the meeting over to the

3   panel. Thank you.

4   MR. CASCARILLA: All right. Great. So I am

5   going to give a quick overview of Paxos and then talk a

6   little bit about the stablecoin that we have. And the

7   we are going to move down the panel.

8   And I think it is important to understand

9   some of the background at Paxos. I know some of you

10 are familiar with it when I look at some familiar faces

11 here. But it is going to be helpful because we have

12 certain attributes to our stablecoin that are made

13 possible by the way we have set up our business. And

14 so, you know, when we think about Paxos, we really

15 think of ourselves as creating financial market

16 infrastructure for an open financial system. And, you

17 know, we have been around now for almost seven years,

18 and we have raised quite a bit of capital. We have

19 employees and a global presence. We have put together

20 an independent board. And we have really tried to make

21 sure that we have set ourselves up as trying to follow

22 regulation and with a regulatory-first approach to

1   everything that we have done and all of the products

2   that we have created. We have created a number of

3   different products. We don't just have a stablecoin.

4   We have tokenized a variety of different types of

5   assets. That includes dollars. We have also created a

6   white-label version of a stablecoin for partners. Our

7   stablecoin is regulated. I will talk about what that

8   means in a moment. We have also created a regulated

9   gold-backed token. And we are also a custodian holding

10 assets that are crypto assets, cash assets, gold

11 assets, other commodities, and as well as securities.

12 And from a post-rate perspective on the security side,

13 we have created automation tools and a settlement

14 platform. So there is quite a bit to what we do at

15 Paxos.

16   We are just going to talk, really, around

17 what we do from a cash stablecoin perspective. And I

18 think we have constructed this, and we will hear

19 different versions of how to construct stablecoins

20 differently from others. We have quite a few different

21 types of customers. They are institutional in nature.

22 We are generally an institutional platform. And so we

1   have set it up with a regulatory foundation that

2   enables us to create a regulated stablecoin.

3   So we created a trust company in the State of

4   New York in May of 2015. We are the first firm to be

5   approved to operate in the blockchain and crypto space

6   as a trust company. And so we are very proud of that.

7   It was a deliberate effort that we went through. It

8   took us a number of years. And that then has allowed

9   us to receive other approvals. We have full SWIFT

10 access, access to Federal Reserve, NSS, vaults around

11 the world. We are in the process of actually applying

12 for a clearing agency registration with the SEC, so a

13 whole number of regulatory approvals that are sitting

14 on top of what is our trust company status. And that

15 trust company status is really the foundation because

16 it allows us to hold assets, custody assets, and then

17 to be able to tokenize them.

18   So when you think about the stablecoin, the

19 Paxos stablecoin, this is one dollar equals one Paxos

20 stablecoin. Assets are sent to Paxos. They are held

21 in bank fully segregated reserve accounts. They are

22 generally held in T-bills or overcollateralized repo of

 1 T-bills that are maturing in a day or less than a week.

 2 So there is no duration risk that we are taking. We

 3 are taking no credit risk. We are simply holding

 4 dollars in a reserve account. And those equal on map

 5 one to one with a token. And that token happens to be

 6 issued in our case on Ethereum, though we will likely

 7 add other chains over time.

 8   And so that one-to-one mapping is really

 9 important. It is verified through independent

10 auditors. And so we have an independent auditing firm

11 that makes sure that at all times, the dollars equal

12 the number of tokens.

13   So there is no fluctuation. There is no

14 attempt. There is no attempt to create a profit from

15 anyone who holds this token. And it is always

16 redeemable for one dollar.

17   Now, if you come to Paxos and you send us

18 dollars, you have to be a customer. Because we are a

19 trust, we are incorporated under New York banking law,

20 chartered under New York banking law, we follow the

21 practices for AML/KYC that you expect out of a bank.

22 We have a BSA officer. We have four to six weeks of

1   audits every year from the DFS coming in from an exam

2   perspective. We have Grant Thornton as an independent

3   auditor of our internal audit controls. Deloitte

4   Touche is our external auditor. We have an independent

5   board of directors. All of this is done in order to

6   create a lot of confidence amongst all of our customers

7   that our dollars are held in these segregated reserve

8   accounts. And then we have a separate auditor that

9   just audits the bank account. All of this oversight is

10 really meant to create a lot of confidence that, unlike

11 certain other examples in the stablecoin space, that

12 you might have an unbacked token.

13   And so one dollar equals one token. That

14 token is then issued to a customer that has been

15 onboarded and which is following our compliance

16 programs. And they now have this token they can onward

17 send us.

18   If someone comes to Paxos and wants to be

19 able to redeem, they can do this. They have to be a

20 customer or they have to be again onboarded. And they

21 can come to us with that token. We will burn the token

22 and then give them a dollar. And so that is the way in

1 which we manage this process.

2   I think there are a lot of benefits to

3 creating tokenized dollars. There has been a lot of

4 talk about this for central bank digital currencies and

5 other ways of creating so-called stablecoins.

6   Putting a token onto a blockchain I think

7 really changes the utility curve of the dollar. It is

8 able to move 24 hours 7 days a week. I mean, it is not

9 tied to a 9:00 to 5:00 banking hour. It is able to do

10 this instantaneously. So you are not talking about

11 hours or days in the case of ACH or multiple days in

12 the case of international wires. And you are able to

13 do this much more cheaply.

14   In the case of Ethereum -- there are many

15 other chains this can be done on, but in the case of

16 Ethereum, it is about three cents to five cents to do a

17 transaction. Imagine that. You know, that is two

18 orders of magnitude or maybe even three orders of

19 magnitude less than a bank wire, international bank

20 wire.

21   So you are able to move money in a completely

22 different way. And you can program it. So it is

1 important you can create programmable money. And so

2 this is really important. And where this became very

3 clearly needed was in the blockchain space because

4 assets are moving 24 hours 7 days a week very cheaply.

5 And you didn't have a way of moving money across it.

6   And, then, the last point is it creates

7 access. If you have a smart wallet, you can now have

8 access to digital U.S. dollars. That is important for

9 global use of the dollar. It is important for

10 underbanked and underbanked persons who don't have

11 access to a bank account because today the only way to

12 have digital dollars is through a bank.

13   And so these are I think some of the real key

14 benefits. And that is why we set the Paxos Standard

15 token up this way. And, importantly, not only are we

16 regulated. The token itself is regulated. So in order

17 for us to issue this, we had to take the token and the

18 proposal to our regulator. They saw the proposal in

19 its totality. And they then approved us to be able to

20 do this. So this is a completely different standard

21 from, really, how anyone else is operating in the

22 space, which is something we are very proud of. And we

1   have been able to leverage this in a number of ways.

2   So we have created stablecoin as a service.

3   So we can do this not just for ourselves but

4   very traditionally in financial services, there is a

5   concept of white labeling where you can add a partner

6   who might be there from a branding or a marketing

7   perspective, but we are still running the entire

8   process. It is still regulated. It still has the same

9   exact controls. Everything is being done in the exact

10 same way.

11   And so we have done this for a number of

12 different partners, but Binance is probably maybe the

13 most notable in the way they are doing it, which is

14 having the Binance name on what is this Paxos

15 infrastructure. And so that gets to maybe the very

16 point of what we are trying to do at Paxos, which is

17 create this financial market infrastructure that can be

18 utilized by many different firms but, yet, doing it in

19 a way that is regulated, that has all of the right

20 controls and has all of the right type of oversight and

21 opening it up to a much broader market.

22   So we are really proud of this stablecoin as

1 a service, the process that we have done. There are a

2 number of conversations for other firms that want to be

3 able to take advantage of this very same service.

4   And so I talked a little bit about how we are

5 regulated. There are monthly attestations on our

6 website. You can go and take a look and see that, you

7 know, we don't just have this auditor. You can

8 actually verify it yourself through independent

9 reports. And I think the use cases for stablecoins,

10 which I am sure we will all about it here, are really

11 around trading, settlement, and payment movements,

12 being able to trade real-time movements of money. And

13 this works for a number of different types of

14 businesses.

15   We have partners and I think conversations

16 that we will be talking about as the year goes on

17 around payment firms, around banking firms, around

18 remittance firms that find us to be of significant

19 utility for their businesses. And so we tried to make

20 sure that we approach this in a way that is creating a

21 significant level of regulatory oversight without

22 losing the utility that blockchain brings. And that is

1 always a challenge because blockchain can be open and

2 there could be a perception that anyone can use it.

3 But the way we put it in place, really, I think solves

4 many of those underlying issues.

5   So, with that, I will stop and turn it over

6 to Steven. Sorry. I am actually also dovetailing his

7 technology here. We are a technology firm.

8   MR. BECKER: Thank you very much, everyone,

9 Commissioners, thank you very much for inviting me to

10 speak here today. I just wanted to acknowledge my team

11 as well: my GC, Brian Avello; head of comms, Mike

12 Porcaro, and our advisor Allen Slover (ph), here

13 supporting me today. So this is really a joint effort.

14   This is a panel about stablecoins. You have

15 to consider decentralized stablecoins in order to be

16 very complete in your consideration. And it is

17 decentralization that is really important.

18   Decentralization is inherent in a free and

19 open-market economy. And it also happens to be the

20 underlying structure of a public blockchain. So my

21 contention is that the U.S. is in the best position to

22 extract the best possible value out of public

1   blockchains.

2   The decentralized finance space, otherwise

3   known as DeFi, has this critical element as well. And

4   it is through DeFi that MakerDAO enables the

5   developments of an un-blockchain economy. And it is

6   not just only an un-blockchain economy, but it is one

7   that dovetails and intersects with the traditional

8   world.

9   In order to figure out how that happens, we

10   need to take a bit of a step back and ask a really

11   tricky question. What is decentralization? So I have

12   been mulling about decentralization for quite some time

13   and decided to make it simple, let's have a look at

14   some definitions. What I found was when you looked at

15   the definition of decentralized, this became

16   interesting. No matter where you looked, it really

17   came down to, to be decentralized means not to be

18   centralized.

19   (Laughter.)

20   MR. BECKER: Very helpful.

21   But what I did find is that decentralization

22   as a more objective process becomes more practical,

1 becomes more pragmatic. It is the dispersion and

2 distribution of functions of powers. This is something

3 you can work with. So when you think of

4 decentralization, it is more about a framework. They

5 are looking at a definition. So if we considered a

6 framework, what do those attributes of that framework

7 look like? How would you be able to put your finger on

8 something and say, "Yes, that thing can become

9 decentralized"?

10   The first attribute -- I am keeping this

11 fairly simple -- is that decentralization must be

12 possible. If I am an asset originates and I tokenize

13 my assets, I am in the position to become

14 decentralized.

15   The second attribute is that decentralization

16 must improve over time. You can look at this from sort

17 of a technical point of view and say to yourself,

18 "Architecturally and from a technological standpoint,

19 how many computers are in this network, in the system?

20 The political side of it, how many folks are

21 controlling these computers? And what about the social

22 aspect? Who is ultimately guiding all of these folks?"

1   So decentralization is very important in

2   terms of it has to constantly be improving.

3   And, then, last but not least -- and this is

4   a bit of a tip of the hat to Commissioner Hester Peirce

5   Is that decentralization should ultimately support the

6   intended function. If it doesn't, you end up having a

7   misappropriation of resources and really looking at a

8   whole bunch of scams as well.

9   But why does decentralization matter? We

10 framed the argument, at least framed a construct around

11 decentralization, but, really, at the end of the day,

12 why does it matter?

13   Well, it is about accessibility and

14 independence. If you can create independent access to

15 the financial global system, what does that mean? And

16 this is a statistic that I am sure you have heard a

17 couple of times already, that there is 1.7 billion

18 unbanked. And blockchain, the DeFi space, can help

19 engage and bring those folks on chain.

20   But, to be honest, that is a large number.

21 And it is a very remote statistic. So I am going to

22 try and bring it a little closer to home. The Center

1   for Financial Inclusion has stated that 68 million

2   Americans are currently underserved. That means over

3   20 percent of the population cannot afford to be a part

4   of the financial system.

5   Generally, I end my sort of value proposition

6   there about DeFi, but let's take it to the other side

7   of the spectrum. What about Citibank? Citibank has

8   around about 200 million accounts that it services

9   around the world. Why would it be interested in the

10 permission of this public blockchain? Why not just

11 create a permission blockchain? It is a good idea.

12 You have a lot of control, a lot of speed. That is

13 fantastic. But you don't have access. You don't have

14 access to that 1.7 billion. You don't have access to

15 that 68 million. If you try to do it any other way,

16 you are asking those folks to trust you. And that is

17 the blocker.

18   Again, keep in mind that when you have a look

19 at stablecoins, Charles has given us a very thorough

20 idea of what I call a centralized stablecoin. And what

21 we are presenting here today is the counterpart to

22 that, the decentralized side. And let me make it quite

1   clear right now they are complementary in my view. We

2   need as many centralized as decentralized projects as

3   possible. So if you have a look at the space that

4   Citibank would be involved in, well, you know, they

5   have access to all of these folks. They could turn 200

6   million accounts into a billion. That means that they

7   are not going to be by themselves. You are going to

8   have so any folks in that space.

9   With the access to such a client base, you

10 are going to have opportunity, which, you know, gives

11 rise to innovation. You are going to have a race to

12 the bottom in terms of consumer costs. That is really

13 the driver of competition and efficiency, which

14 ultimately ends with growth. This is boots-on-the-

15 ground jobs. This is the development of the current

16 industries that we have and the development of new

17 industries that come from, importantly, the

18 intersection of blockchain, decentralized blockchain,

19 and the traditional economy.

20   With decentralization, like everything else,

21 it is not all flowers and rainbows. You know, there is

22 always an issue. There is always an aversion to

1 change. And currently there is this misconception that

2 decentralization is unmanageable. It is not capable of

3 being regulated.

4   I would like to sort of point back to

5 previous statements I made about the fact that

6 decentralization is inherent in an open, free-market

7 economy. That means we actually have the tools

8 available to us to apply it appropriately. We just

9 need to change our perspective in terms of how we

10 actually apply it.

11   If you imagine for a second decentralization

12 as an ocean, it is really impossible to try and

13 regulate the ocean. But you can certainly regulate the

14 ports, the harbors, the ships, and the shipping lanes.

15 So that is really what I call regulation at the edges

16 and the ships in the shipping lanes looking at the

17 regulation of these walled gardens.

18   So what this really requires is looking at

19 the current tools we have and just simply saying,

20 instead of trying to control for the ocean, why don't

21 we try and control for how we interact or engage with

22 it? It really comes down to looking at the control of

1   the activity, not just the entire structure.

2   So let's come down to a subspace of

3   decentralized finance, or DeFi. Really, what is it? A

4   couple of definitions are out there, but this is the

5   one that really resonates with I think the broader

6   aspect of what MakerDAO is involved with and what DeFi

7   is trying to do. It is trying to create a new monetary

8   and financial system built on public blockchains.

9   Importantly, it is a system that augments. It does not

10 replace or substitute the traditional one. I can't

11 emphasize this enough. You do have naysayers on both

12 sides, where they say, "Blockchain is ridiculous.

13 Let's not have it" and folks from the blockchain

14 saying, "The traditional world is rubbish. Let's burn

15 it to the ground." But ultimately there is a

16 realization that the value to this whole equation is at

17 the intersection of the blockchain economy and the

18 traditional one. And, then, finally, this is a system,

19 as I mentioned before, that creates value by enabling

20 this independent access to the global financial system.

21   Now let's get to MakerDAO. You know, what is

22 MakerDAO? And, importantly, I need to stress that I am

1   introducing MakerDAO now, as opposed to the beginning

2   of the presentation, because we really need to set the

3   stage of what decentralization is, have a working

4   concept of what DeFi is because then MakerDAO makes a

5   lot more sense.

6   And, strictly speaking, MakerDAO actually is

7   made up of two components: one, a protocol; and, two,

8   a community. And this is of the utmost importance to

9   understand. It is the community that creates the

10   value. We are talking about a decentralized system.

11   It is the community that is engaged with a

12   decentralized system that gives it the value and also

13   permeates the value into the traditional space.

14   So what is DeFi? Sorry. Once you make it

15   down, where does it fit in DeFi? So if we have a look

16   at just the Maker protocol, simply speaking, it is a

17   decentralized protocol layer on top of the Ethereum

18   blockchain. So it is a layer that is applied on top of

19   the Ethereum blockchain. It is an open-source protocol

20   that is blockchain-agnostic. Very important, Charles

21   mentioned that the consideration of Ethereum is really

22   important, but being open to other blockchains really

1   is vital as well. It also presses the idea of

2   interoperability, which, you know, that is a

3   conversation for another time.

4   The fact that you also open-source leads to

5   the underlying robustness that you have with general

6   open-source software and how you can ensure that it has

7   a certain level of integrity and quality.

8   And finally, most importantly, MakerDAO

9   provides the necessary tools for the DeFi space to

10 enable this growth of the blockchain economy. And this

11 is something we need to dig into. And I think most

12 folks would be taken aback by the fact that these tools

13 that are provided by MakerDAO are the primary function

14 of the Maker protocol, where the stablecoin Dai is

15 actually the byproduct.

16   So if you have a look at the tools of these

17 functions, they really break down to three parts.

18 There is the ability to collateralize the transfer of

19 assets into the protocol, the ability to generate

20 credit. This is how the stablecoin Dai is created.

21 And then there is a rewarding tool. In other words,

22 there is the ability to stake your Dai and earn Dai or

1 get rewarded with Dai on the back of that.

2   Now, again I need to sort of emphasize that

3 the Maker protocol's primary function is to provide

4 these tools to the DeFi space because with these tools,

5 products and services can be created on chain. That

6 developing economy that I have been speaking about,

7 that gets further enhanced. But in order to facilitate

8 the transactional value, it requires a stablecoin. And

9 that is where decentralized stablecoin really takes

10 full effect.

11   But let's get to the point. How is Dai

12 actually generated? We are talking about a

13 decentralized system. And the best way I know in terms

14 of explaining this is through a wonderful analogy. So

15 let's pretend that you have got $15,000 of gold in your

16 vault in your basement, hard thing to do, but let's

17 pretend. You go down to the basement. You take that

18 gold out, and you go into your study, where you have

19 just procured yourself a very nice smart vault. You

20 stick that $15,000 of gold into that vault and close

21 it. That vault is smart. It realizes the value that

22 is inside the vault and, in turn, generates for you

1   $10,000 of credit.

2   You want to go on vacation. What do you do?

3   You go, "Well, this is a great idea. I am going to

4   take $5,000 out, go on vacation, enjoy myself."

5   When I come back, I will go back to work. I

6   will earn my $5,000. And with a small fee, I take that

7   money and put it back into my smart vault. The smart

8   vault opens and allows me access to the gold.

9   I want to pause there for a moment because

10 there is something critical here. The gold belongs to

11 you. The vault belongs to you. The cash belongs to

12 you. This is the ultimate expression of

13 decentralization. In fact, if we take this analogy and

14 have a look at how it is applied on chain, substitute

15 ether for gold. And that smart contract, the vault, is

16 really just, you know, a production of code on chain

17 that accepts that value and assesses that generation of

18 credit, which is Dai.

19   So here is the important thing. Where does

20 Dai get its value from? And this is critical. You

21 need to start off with $15,000 in your pocket to

22 purchase this digital asset called ether or whatever

1   digital asset you wish to put into this vault. That is

2   critical. Dai does not get created from nothing. And

3   that is really essential to not only policy, but it is

4   also essential when you refer to CBDCs and look at

5   stablecoins as the private market counterpart to CBDCs

6   and, by extension, in a central bank cash.

7   To that end, you have purchased this asset,

8   put it into the vault. You have generated Dai. And

9   that Dai sources its value from a dollar-denominated

10 asset. That is where the value comes from. That is

11 where the source comes form. You use it as you would

12 any other stablecoin. And when you are done with it,

13 you bring it back to the vault. And, in exchange, you

14 get your collateral back. I made that sound binary

15 when, in fact, you have a lot more versatility. If you

16 only use a little, you can extract collateral out if

17 you wish and balance and manage your vault as you see

18 fit.

19   An important, another important, distinction

20 to make is Dai is a decentralized stablecoin. It is

21 not algorithmic. It still requires the engagement of

22 the community to make sure that it operates

1 appropriately. That is why it is so important from a

2 DeFi point of view is that DeFi is finding its value at

3 the intersection of the real world, where people exist

4 and they do need to interact.

5   So what are the takeaways? What are the

6 conclusions from this that I wish you guys to think

7 about after this presentation? And that is MakerDAO is

8 a subset of the DeFi space. And, in turn, the DeFi

9 space is a subset of decentralization. And

10 decentralization requires a change in perspective to

11 see the value inherent in it and available to everyone

12 and that value is and does come from an open and free

13 system that embraces this accessibility and

14 independence.

15   And, on that note, I would like to thank you

16 very much for your time and consideration. Over to the

17 pilot.

18   MR. WEN: Hello. Thank you for that.

19   I first thought I would kick off the thank

20 you to the commissioner for inviting me to speak on the

21 panel.

22   I was advised by counsel that I should lay

1 out a brief disclaimer that the presentation I am about

2 to give is a reflection of my personal views, not

3 necessarily the views of those of JPMorgan Chase.

4   That said, look, my name is Eddie Wen. I am

5 the head of digital markets at JPMorgan. I am here to

6 talk briefly about the JPMorgan coin. This is a

7 prototype stablecoin developed by my colleagues in the

8 wholesale payment business in conjunctions with our

9 Blockchain Center of Excellence. BCOE was a group

10 founded in 2015, really designed to explore the

11 applicability of blockchain technologies for the bank.

12 While I am part of the Capital Markets Division in the

13 sales and trading businesses and I am not a subject

14 matter expert on blockchain and DLT, I have worked with

15 the team in examining the applicability of distributed

16 ledger in blockchains for the bank. And we have

17 concluded largely the most viable applications of this

18 technology lies within either our payment space or the

19 settlement of transactions in the back of it. I think

20 that is kind of reiterated with some of the earlier

21 discussions.

22   Now, I would also emphasize that the product

1 I am about to describe has not gotten full regulatory

2 approval. It remains as a prototype and not yet live

3 as a live service. Now, we have done production

4 parallel testing with customers on various different

5 implementations. The results are promising, and I

6 think there are a lot of benefits to a JPMorgan Coin

7 that would help in enhancing some of our

8 infrastructure.

9   Lastly, there were also previous

10 conversations on the panel discussing JPMorgan Coin.

11 And we felt that some of the discussions did not

12 properly reflect what the product offering does. So

13 this is a good opportunity for me to kind of clarify

14 how the product works.

15   So, with that, I will move on to the next

16 slide here. Look, some of this may be a rehash of what

17 my previous speakers have talked about. So I will try

18 to make this brief.

19   In short, the digital coin, the JPMorgan

20 Coin, is a digital coin designed for instantaneous

21 payments using blockchain. It is built on top of the

22 Quorum protocol-based blockchain network, but it can be

1 adapted to interoperate with other protocols, subject

2 to client demand. And this product is only available

3 to JPMorgan customers who have gone through our AML/KYC

4 process; it is a permission blockchain and is not

5 available for retail use.

6   So I think it is also good to pause here to

7 give you a little bit of backdrop of why we think this

8 is a very useful product. And some aspect of it

9 probably looks more like software infrastructure, which

10 I will talk about a little later. So the backdrop is a

11 lot of times in our merchant services business, a lot

12 of times when a merchant provides the good and services

13 that are sold, oftentimes they issue a bill for the

14 clients to pay and some subsequent ladder process.

15   So now both on the client and its operations

16 side have to deal with accounts receivables and

17 payables. And the process of handling that is very

18 intensive from a technology perspective and human

19 resources perspective. And, largely, I think we think

20 that the ability to bundle in a ledger the transaction

21 which involves procurement of the goods instantaneously

22 with payments, we think that ultimately is a huge

 1 value-add and a cost savings for the payment business

 2 overall. So, hence, we think why this like the

 3 JPMorgan Coin is an important infrastructure component

 4 to allow that to happen efficiently.

 5   Now, you may ask, is this coin currency a

 6 legal tender? Well, it is not money per se, right? It

 7 is a digital representation of our clients' money at

 8 JPMC. In short -- right? -- it always has a value

 9 equivalent to U.S. dollars. And it is backed by the

10 faith and credit of JPMorgan Chase. It currently is

11 applied to the U.S. dollars, but conceptually the

12 technology is currency-agnostic, and we can apply it to

13 other currencies beyond the U.S. dollars provided the

14 pilot continues.

15   Now, we listed here a couple of use cases.

16 Again, they are kind of in the payment space as well as

17 the settlement space of various different applications.

18 We feel that the common theme here is that having a

19 digital asset like JPMorgan Coin represents the

20 essential payment leg of a blockchain transaction. And

21 it is applicable for building a variety of different

22 applications. If you look at it, you could call it a

 1 crypto asset, but, really, does it look more like a

 2 software infrastructure to support the business that we

 3 do? And I think ultimately if we are successful in

 4 making ubiquitous deployment of JPMC Coin internally

 5 within the bank, a lot of the applications and systems

 6 that we built in JPMorgan could be substantially

 7 simplified.

 8   So this is a relatively simplistic

 9 illustration of how a particular use case with the coin

10 will work. And, as I said, these coins are a digital

11 representation of the clients' money at the bank. We

12 could break it down into three steps. One is the

13 issuance process. Second is the coin transfer. And,

14 finally, then there is a redemption process, which

15 converts the coins back. So in the issuance process,

16 the clients can instruct the debit of his JPMorgan

17 deposit account, certain amount of U.S. dollars. And

18 those dollars will turn into blockchain-based digital

19 U.S. dollars housed by JPMorgan Coins.

20   Upon the clients' instructions who wish to

21 make a payment to another JPMorgan client on the

22 blockchain, a new ledger entry is introduced

1   representing the debit and credit of JPMC Coins between

2   the two clients.

3   And, finally, if the client chooses to redeem

4   the coins back to U.S. dollars, they can do so and

5   convert the coins back into their money in the deposit

6   bank.

7   So you could see that the repeated use case

8   of this could be very powerful. Now, it does not use

9   the traditional payment rails, which could be very

10 costly and time-consuming. Blockchain provides

11 atomicity, traceability, 24-by-7 operations, ease of

12 reconciliation, and lower cost, and what traditional

13 means of payments would have been. Operational staff

14 may not have to spend as much time tallying up netting

15 transactions and reconciling that with client balances

16 upon the tally transactions. This is the core value

17 proposition of what the coin is and how it makes it

18 more efficient for our business.

19   So I thought it may be helpful to kind of

20 give a brief overview of the taxonomy. And I think

21 Tommaso may actually touch upon this in the subsequent

22 conversation. This is actually a report that was

 1 published by the G7 working group recently on the

 2 taxonomy of stablecoins. There currently is a lot

 3 interest in stablecoins, though the market participants

 4 recognize the inherent volatility of cryptocurrencies

 5 make it very difficult to build a payment platform on

 6 top of. As a result, there are many variants, as we

 7 heard some today, having created, but there are

 8 important distinctions between the various different

 9 flavors.

10   As I mentioned, the G7 working group

11 published a paper. And it largely classified the

12 stablecoins into three different

13 categories -- right? -- a depository coin; a value

14 redemption asset-backed coin, a very low-redemption

15 asset-backed coin; as well as a fixed redemption asset-

16 backed coin.

17   The JPMorgan Coin is a variant of the

18 depository coin. It is simply just a digital

19 representation of clients' money at the bank and is

20 readily redeemable at par. Now, other types of

21 stablecoins may have variable or fixed redemption

22 values. They are subject to the credit quality of the

 1   issuer. And they may be openly traded in a market

 2   price that fluctuates away from the underlying asset

 3   values of the asset pools that are in there.

 4   So that brings me to kind of discussions

 5   around our regulatory views and some of the core

 6   principles we think it is important in the guidance and

 7   oversight of digital assets, including the stablecoin.

 8   We feel very strongly that that regulation should be

 9   activity-based. Now, digital assets are subject to

10   activity-based regulations. It should be regardless of

11   the type of financial institutions that are conducting

12   those transactions.

13   Secondly, minimum standard for DLT networks

14   should be established. Blockchain networks should be

15   subject to minimum standards to reduce systemic risk.

16   Examples such as cybersecurity risk, data privacy, and

17   resiliency, those types of guidelines on guard rails

18   for those would make sense to regulate the space.

19   We also believe global consistent oversight

20   is important in these borderless markets. We have

21   tried for global consistency to avoid cross-

22   jurisdictional arbitrage. If you create a service in

1 one jurisdiction versus another, you should be subject

2 to the same rules.

3   And, finally, ongoing regulatory engagement.

4 I think this is part of the reason why we are on this

5 panel. As the pace of technology evolves, regulators

6 should have a means of engaging market participants on

7 an ongoing basis to appropriately calibrate the

8 oversight process.

9   So I would close by the following. So the

10 JPMorgan Coin is not an attempt to replace the global

11 payment system. It is a mechanism designed to improve

12 it.

13   JPMorgan's payment business is subject to the

14 same regulatory oversight. With or without the

15 JPMorgan Coin, it is a highly regulated business and

16 will continue to be that way. However, JPM Coin could

17 reduce the operational paying points, providing greater

18 traceability, less time and effort, and spent on

19 reconciliation and other operational activities.

20   Overall, this will translate into lower cost-

21 of-service provisions for the bank as well as for our

22 customers. And it provides an infrastructure for us to

1 build the next generation of digital applications and

2 services. Right?

3   And, with that, I will hand it over to the

4 next speaker.

5   MR. MANCINI-GRIFFOLI: Thank you very much.

6 It is a pleasure to be here. Thank you for the

7 invitation.

8   I will speak about my own views, not those of

9 the IMF or its executive board.

10   And I have been invited to speak about

11 stablecoins. I will speak about stablecoins more

12 generally. And this is based on a paper that I

13 published last summer with Tobias Adrian, also at the

14 IMF, which was the foundation, actually, for the G7

15 paper, of which I was also an author, that Eddie just

16 mentioned.

17   So I am going to try to give you a bit of an

18 overview of what stablecoins are, at least how we see

19 them, with my coauthor.

20   So the question I would like to start with

21 is, how do you pay for coffee? And this is really

22 not -- I am not trying to start with a joke. This is

1 very serious. How do we pay for coffee? I chose

2 coffee maybe because I am an Italian. So that is the

3 most important part of the presentation: good coffee.

4 Right? And the answer is really with a stable store of

5 value. So we like stable stores of value. We like to

6 hold stable stores of value in our pockets because when

7 the coffee costs one dollar, we want to be able to pull

8 out that amount to pay for it. Vendors like to be paid

9 in a stable store of value because what they receive,

10 they don't want to be able to transfer immediately into

11 something else.

12   And so the serious parts of this slide is,

13 what is a stable store of value? We can't just take it

14 for granted. And what I would like to suggest is that

15 a stable store of value is rooted, first and foremost,

16 in a real good; in this example, coffee. We want to be

17 able to pay for something. What we hold as a stable

18 store of value needs to have identity that would allow

19 us to pay for something.

20   Now, that something has a price, which is

21 expressed in the unit of account, say one dollar. And

22 we pay for that good, one dollar, with private money

1   unless we pay with a dollar bill. When we pay with a

2   bank account, when we transfer a bank deposit, it is a

3   private form of money.

4   Now, the fact that one dollar, that face

5   value of one dollar, allows us to pay for coffee today

6   and tomorrow and hopefully next year has to do with

7   price stability. So price stability is part of what we

8   intend with a store of value, with a stable store of

9   value.

10   But there is another element to a stable

11   store of value, and that is exchange stability,

12   something that we take for granted. We take for

13   granted the fact that if we have one dollar in our bank

14   account, we can pay for coffee that costs one dollar.

15   But we shouldn't take it for granted because there is

16   this notion of exchanging the private money into a

17   government-backed form of money, into cash essentially,

18   to pay for coffee.

19   Now, you would find this perfectly reasonable

20   if the private form of money were foreign currency.

21   And then we could speak about foreign exchange between

22   the foreign currency and the dollar before we can pay

1 for coffee. And what I would like to argue is that

2 that notion of exchange stability also holds true for

3 dollar-denominated private forms of money, such as bank

4 deposits and stablecoins. So what I would like to do

5 is focus on this notion of exchange stability and leave

6 price stability for the central bank to worry about.

7 But, nevertheless, in the context of this presentation,

8 it is important to keep in mind that both price

9 stability and exchange stability are part of what we

10 intend by a stable store of value.

11   So there are two types of private monies:

12 collateralized and non-collateralized. So

13 collateralized types of money are forms of money that

14 are backed with collateral and which you can redeem

15 against that collateral. So a bank deposit, for

16 instance, is a collateralized form of money. And so

17 are stablecoins.

18   Uncollateralized types of money are crypto

19 assets, bitcoins, for instance, or, frankly, cash.

20 Cash is not a private form of money, but it is a good

21 representation of a non-collateralized form of money.

22 You can't redeem cash against anything else. You would

1 come to the bank with a $20 bill. You can get 2 10s,

2 but you can't get anything else for it.

3   So let's focus on collateralized forms of

4 money. And what I would like to do is explain what a

5 stablecoin is by comparing it to a bank deposit along

6 these five dimensions: denomination, exchange pledge,

7 backstop, settlement technology, and backing asset. I

8 will clarify what each of these is throughout this

9 presentation.

10   So let's think of a bank deposit that we call

11 for simplicity B money, bank money. So a bank deposit

12 is denominated in the domestic unit of account. It is

13 in dollars. It can be redeemed or exchanged at fixed

14 face value. So if you have $10 in your bank account,

15 you can redeem that against $10 bills, against a $10

16 bill. You can do that. And you believe that you can

17 do that because there is a government backstop:

18 deposit insurance, lender of last resort, emergency

19 liquidity assistance, supervision, et cetera. The

20 government plays an important role in making that

21 exchange pledge credible to you.

22   When you transfer B money, when you transfer

1 accounts, deposits held at a bank to another bank, the

2 technology is centralized. It is an account-based form

3 of money where there is a check of your identity. Are

4 you the rightful owner of this account? If so, yes.

5 And then we will transfer the money. And that transfer

6 is settled centrally, through the central bank

7 ultimately.

8   The backing assets that the bank holds

9 against this claim that you have can be mixed because

10 of the government backstop. So this is pretty simple,

11 pretty straightforward. We understand that that is the

12 world we live in. How do stablecoins compare? And

13 what I would aim to do is emphasize that there is no

14 single stablecoin and there is no single form of

15 alternatives. They vary according to exchange

16 stability.

17   So that concept of exchange stability that I

18 had up there on the slide is important. And what I

19 will discuss now is first what we call E money and then

20 another form of money that we call investment money.

21 And I will suggest examples that vary according to

22 exchange stability.

1   So the first example is what we call sCBDC.

2   Don't worry about the name. What is important to

3   understand is that this is a form of digital money that

4   is also denominated in the local unit of accounts that

5   has an exchange pledge. So you can redeem this at face

6   value against cash.

7   But the backstop is private. The government

8   is not involved. So the company that issues this

9   liability, as CBDC that you use for payments, has to

10   rely on only itself to create trust. And how does it

11   do this? Well, it does this by backing the assets.

12   So we will jump now to the last step here.

13   Backing the assets was something that is very, very

14   safe and very, very liquid. And in the most safe and

15   the most liquid case, that is central bank reserves.

16   So this is a narrow bank. That whole central bank

17   reserves and issues a liability to be used for payments

18   by you and I.

19   And the settlement technology in this case is

20   mixed. It can be centralized. It can be account-based

21   or it can be decentralized. What I intend by

22   decentralized is token-based, blockchain-based if you

1 want, where your identity is no longer important but

2 the validity of the token is important.

3   That is sCBDC. The next step is what

4 currently exists and are very popular in other parts of

5 the world: closedloop systems. This is what Alipay

6 and WeChat Pay are, for instance, in China. So the

7 denomination is again in the domestic unit of account.

8 There is a pledge for exchangeability. Reading ability

9 at face value, there is a private backstop just as

10 sCBDCs. But the only difference is that this is a

11 centralized account-based system. So you have an

12 account at Alipay or WeChat Pay. And the assets that

13 are held, well, are safe and liquid, not quite central

14 bank reserves, although in the specific case of Alipay

15 and WeChat Pay in China, the central bank has deemed

16 the setup with, you know, safe but private assets as

17 too risky and has asked Alipay and WeChat Pay to hold

18 only central bank reserves. So that example has now

19 migrated over to sCBDC but started out as closed-loop

20 systems.

21   And there are others around the world.

22 M-Pesa in Kenya is one that is extremely popular that

1 90 percent of people in Kenya use for things.

2   Now, the last is what I call coins for lack

3 of a better word. You might come up with something

4 better. And if so, let me know. It is very much the

5 same as all of the other examples I have described

6 except that it is not decentralized. It is token-

7 based. And the assets held against this claim that you

8 hold are safe and liquid assets. And they can be

9 government securities. They can be deposits in a large

10 bank or other types of assets.

11   The last type of money is what we have coined

12 investment money. And that is a liability that is

13 issued in its own denomination. The redemption is no

14 longer fixed at face value. In fact, there is no such

15 thing as face value in a unit of account that

16 we -- such as the dollar or the euro, et cetera, the

17 government unit of account. The redemption is variable

18 at market value. So, essentially, you get back the

19 value of the collateral at market value whenever you

20 decide to redeem.

21   And here the settlement technology is

22 decentralized, and the assets that are backing this

1   claim are mixed. So this is very similar to an

2   investment fund, where you simply hold a tokenized

3   share of the fund.

4   There are some schemes that are very similar

5   to this and that we have labeled I-money. In fact, we

6   were public about this in our first paper. The first

7   iteration of Libra we thought corresponded to I-money,

8   as opposed to E-money, because the redemption was a

9   variable rate. And you were only going to get back the

10 market value of the underlying assets at the time of

11 redemption.

12   Very well. So what is a stablecoin, having

13 laid out the environment here? Well, basically, a lot

14 of stuff can be labeled as stablecoins. And that is an

15 important takeaway, if anything, from this

16 presentation, is that stablecoins is an extremely,

17 extremely diverse term that captures a lot of different

18 types of schemes: both E-money coins, so E-money, that

19 is token-based, and I-money as well. So never think of

20 stablecoins as one type of product. Always look at how

21 the underlying product is actually constructed.

22   So, of course, we are concerned by public

1   policy objectives and by how stablecoins might or might

2   not satisfy these objectives depending on the design.

3   And, again, it is very important to look at stablecoins

4   on a case-by-case basis.

5   We think about consumer protection. And let

6   me just jump to the next slide here to illustrate why

7   there can be concerns about consumer protection.

8   Stablecoins are, after all, issued by a private company

9   with private backing. There is no government backstop,

10 as we suggest, I suggested earlier. So there is always

11 the question of whether a stablecoin represents a

12 claim, a legal claim, against the underlying assets.

13 There is the question of what happens when the issuer

14 of the stablecoin defaults, whether the access to the

15 claim on the underlying assets is protected from

16 bankruptcy. And there is always, of course, the

17 possibility that the underlying assets are exposed to

18 market for an exchange and liquidity risks. So there

19 is a question mark about consumer protection.

20   I think that, because of that, there is also

21 a question mark about financial stability. If there

22 were very large redemptions out of stablecoins or

1   movements of capital out of countries into stablecoins,

2   whether stablecoins might facilitate bank runs in

3   countries, in weak countries, out of their currency.

4   There is also a question mark that is very

5   important for the IMF. And that is whether stablecoins

6   might undermine monetary policy control in countries

7   with weak institutions and high inflation, where there

8   is partial dollarization in those countries already.

9   So people hold dollars and transact in dollars already,

10 but doing so is relatively expensive because they need

11 to either hold them under the mattress or hold a dollar

12 bank account. And the question is whether

13 dollarization in those countries might become a lot

14 easier with stablecoins and, as a consequence, whether

15 those countries will lose monetary policy control

16 entirely.

17   There are also questions about data privacy

18 and confidentiality, obviously, who holds the data that

19 is generated when the coins are transferred.

20   There is a question about competition and

21 efficiency. I think the most important term here is

22 "interoperability." Are these new coins interoperable?

1   If I hold coin A, can I exchange? Can I pay somebody

2   who holds coin B? If not, there is a question of fair

3   competition, obviously.

4   There is also a question mark about financial

5   integrity. To what extent are wallets KYCed? To what

6   extent are transactions, subsequent transactions, in

7   stablecoins actually monitored? To what extent are

8   these stablecoins compliant with FATF standards?

9   So these are the questions that we raise at

10 the IMF with regard to stablecoins and in the

11 regulatory community. And I think I will end with

12 that. Yes. Thank you very much.

13   CHAIR GORELICK: Okay. Thank you very much

14 to the panelists.

15   And, with that, we will open up to any

16 questions. Since I didn't get to Gary last time, I

17 will start off with Gary.

18   MR. DeWAAL: A question for you, Steve. So

19 it is intuitive to me why either a private or a

20 decentralized stablecoin backed by an asset in one way

21 or another would make sense. What is the use case for

22 a stablecoin backed by a budget digital asset that has

1   tremendous volatility? What is the use case for that?

2   MR. BECKER: Well, the first thing is you

3   have -- using just ether as an example, you have a

4   limited-use case. But the idea here and with respect

5   to MakerDAO is to consider the fact that any collateral

6   type could be possible to use. And that is why

7   MakerDAO is incredibly important in terms of the

8   intersection between the decentralized space and the

9   traditional economy because if you think about

10 something like dead factoring, you might be able to get

11 into a point where you can tokenize invoices and you

12 can get your financing from a decentralized space a lot

13 quicker than you could from a traditional space. You

14 might have better terms because the collateralized

15 comes with different parameters.

16   This is not – - this doesn't live in the

17 world of imagination and potential. Right now, there

18 is an organization called dexFreight that is doing that

19 for truckers. You know, someone who is sitting behind

20 the wheel is pulling a payload they invoice. And at

21 the same time, they could flip over to another app and

22 go, "Let me go and factor this invoice." I mean,

1 again, it is in its infancy, but it is happening right

2 now.

3   So what MakerDAO does is it gives this broad

4 capacity for everything from creating brokering

5 services on top. You have got to be a registered and

6 regulated loan originator. You can wrap your business

7 around that functionality and offer that service. In

8 effect, imagine this entire protocol integrating into

9 the backend of -- sorry to say this -- JPMorgan,

10 Citibank, and whatever the case may be. It takes the

11 efficiency of the blockchain. It takes the execution

12 and settlement elements that happen at the same time

13 from the blockchain and applies it to the ability to

14 finance. So the use cases, working capital, capital

15 structuring, general trading. Really, everything you

16 can think about in terms of finance and insurance you

17 can apply using the Maker protocol.

18   CHAIR GORELICK: Thanks. Tom?

19   MR. CHIPPAS: So regarding some of the

20 stablecoins -- maybe this is more appropriate for Chad

21 and for Eddie -- the presentation from you, Chad, said

22 that reserves are held in the safest financial

1   instruments. Do those instruments pay interest?

2   MR. CASCARILLA: Yes.

3   MR. CHIPPAS: And do the coin holders receive

4   any of that interest?

5   MR. CASCARILLA: No.

6   MR. CHIPPAS: It would be interesting to

7   understand why.

8   MR. CASCARILLA: I think as soon as you were

9   going to pay interest, it might look like a financial

10   instrument. And that could raise potential securities

11   issues. And so by having it tied directly one-to-one

12   but not having any interest rate component, the value

13   would not fluctuate versus, you know, a physical

14   currency dollar.

15   And so it is not clear that you would

16   cross -- that alone would let you cross into a

17   securities framework, but it is certainly a potential.

18   MR. CHIPPAS: And I guess extending that

19   concept, then, you are talking about the U.S. dollar,

20   where, thankfully, we haven't seen negative interest

21   rates, but there have been G20 countries with their

22   currency operating in the negative interest rate

1 environment. How would a stablecoin react? What would

2 be the impact to the coin holder in a negative interest

3 rate environment?

4   MR. CASCARILLA: I think you are going to

5 have to deal with it in a different way. I mean, the

6 means of replicating the coin started to get a little

7 bit tricky. And so I think that is part of the reason

8 why you have seen a limitation in terms of stablecoins

9 being created in other G7 and G20 currencies versus the

10 dollar. I think that the mechanism in order to be able

11 to manage that would be around transaction fees. You

12 can create a mechanism to be able to do that when it is

13 out in the wild, so to speak, against what would be the

14 negative interest rate.

15   So it is definitely, you know, doable. I

16 don't think that it is confounding per se, but it would

17 definitely be a change from the way the token operates

18 right now.

19   MR. CHIPPAS: One last question, if I can.

20 With respect to the instruments that are being utilized

21 to generate interest for the issuer, would you describe

22 those efforts as -- and this is coming from a comment

1 about security concerns or becoming a security. Are

2 those any more than just making sure that you don't

3 have erosion due to inflation and things of this nature

4 or are these active investment activities being

5 undertaken to generate outsized returns?

6   MR. CASCARILLA: The goal is really safety

7 and liquidity. And so when you think about having

8 basically one-week maturing T-bills, for instance, that

9 is basically the safest thing that you could own. So

10 in that case, I would actually argue that you are safer

11 than a bank because these assets are being held

12 bankruptcy remote. They are not being used for loans

13 for any kind of duration risk, interest rate risk,

14 credit risk. You actually have essentially zero risk

15 by holding your dollars from an investment perspective

16 with us.

17   MR. CHIPPAS: Got it.

18   MR. BECKER: So if I may add here, the dollar

19 implementation of JPMC coin is intended to be more of a

20 digital representation of the client's money at the

21 bank. So the questions you ask regarding negative

22 interest rate environment, et cetera, I would make that

1   to be no different than if they were holding the money

2   at the bank directly.

3   MR. CHIPPAS: Thank you.

4   CHAIR GORELICK: Thank you.

5   Commissioner Berkovitz?

6   COMMISSIONER BERKOVITZ: Thank you. I

7   apologize for the extremely fundamental nature of my

8   question here, but why do we need -- why can't

9   JPMorgan, for example, do all that you are laid out to

10 do for a stablecoin for JP Coin? Why do you need JP

11 Coin to do it? Why can't you facilitate all of these

12 customer-type transactions simply with the customer and

13 all of the deposits and just have dollars go back and

14 forth on the blockchain? Why do you need this

15 intermediate thing called JP Coin to do that?

16   MR. WEN: Well, I think partly a lot of it is

17 technology-driven. If you look at the traditional

18 payment rails that we have, the infrastructure to

19 facilitate payment, much of that may not necessarily

20 can operate on a real-time basis. Nor is it a natural

21 fit for that on a distributed ledger transaction.

22   So by representing a coin, now, all of a

1   sudden, on a cash leg of any transaction in the

2   distributed ledger, you are able to accommodate that

3   capability to a lot easier.

4   So some people think of it as more this is

5   more like software architecture to maintain our

6   existing systems and make it more agile. I think there

7   is some truth to that, and it makes it a lot easier to

8   do.

9   From a client's perspective, you want to be

10 able to get a transaction done quickly and with

11 atomicity. And this is the capability that allows us

12 to do that.

13   CHAIR GORELICK: Charlie?

14   MR. COOPER: Thanks a lot.

15   I think this is a question for Tomasso, but

16 it may also be a question for Steven. Tomasso, in your

17 definition of stablecoins, it seemed broader than I

18 guess I traditionally think of it. And you had said

19 that there might be a variety of different coins that

20 would fall into that bucket.

21   I am wondering how you would view the Dai

22 example because, if I understood, Steven, you

1 correctly -- and I might not have -- the argument was,

2 "As long as it is collateralized, therefore, Dai

3 becomes a stablecoin." Even if the collateralization

4 is in a highly volatile non-fiat-backed digital

5 currency, that to me strikes me as a bootstrap into

6 stablecoins that isn't right.

7   Would you, Tomasso, from the IMF or your own

8 personal point of view? Does that fall into the bucket

9 as represented here back I guess ultimately by ether as

10 becoming a stablecoin or is that not a stablecoin?

11   MR. MANCINI-GRIFFOLI: I am hesitant to

12 comment on this particular example of MakerDAO, which I

13 don't understand fully. But I think a lot hinges on

14 whether there is a guaranteed redemption at face value,

15 if you buy MakerDAO or any other coin, whether you are

16 holding a coin that has a face value expressed in the

17 domestic unit of account and whether there is a

18 guaranteed redemption at face value. If there is that

19 guaranteed redemption, it would fall under the E-money

20 category. And the question is, what guarantees? What

21 stands behind that guarantee? What type of assets?

22 How risky are they? How much capital is kept against

1 in the balance sheet? That will determine the

2 riskiness of that scheme. Nevertheless, I think the

3 important factor is whether there is that guaranteed

4 redemption or not. If there is not a guaranteed

5 redemption, it would be what we call investment money,

6 which is much more like a tokenized ownership share of

7 an investment fund. So maybe I should let --

8   MR. COOPER: Yes, Steven based on that.

9   MR. MANCINI-GRIFFOLI: -- Steven elaborate

10 based on that.

11   MR. COOPER: Based on that because the

12 analogy, I would argue gold is not ether. So I don't

13 know that the analogy holds. So I am trying to figure

14 out, what is the face value of $15,000 worth of ether

15 if the price is moving a lot? I don't get --

16   MR. MANCINI-GRIFFOLI: Let me just – one

17 small thing. Gold since you brought up gold, we would

18 categorize that as I-money -- right? -- because a coin

19 that is collateralized by gold doesn't have a face

20 value. What you get when you redeem that coin is

21 today's value of gold. You have an ounce of gold as

22 collateral. And when you redeem it, you get your ounce

1   of gold back or whatever the dollar value of that ounce

2   of gold is. So that is I-money for us.

3   MR. BECKER: Essentially there are two parts

4   of this that we need to investigate. The first

5   one -- and I did bring this up to Tomasso in a previous

6   panel that we were on -- is that the idea of guaranteed

7   payment and the consideration of underlying assets, the

8   very centralized point of view. It really is a case of

9   saying you are constructing something independent of

10 the person or the organization using it.

11   What I am trying to express here today is

12 that a centralization is very much pointed at the fact

13 that it is you and the protocol. There is no

14 counterpart. There is no counterparty risk. From the

15 collateral point of view, the idea of looking at gold

16 just becomes a lot more tangible. It gives you a sense

17 of what this asset is.

18   As to the analogy that gold is ether, you are

19 correct. I am not trying to make that equivalence.

20 What I am trying to say is that you have a dollar-

21 denominated asset. That is, in essence, what we are

22 talking about. A dollar-denominated asset that you own

1   that you put into your own vault, as it were, a smart

2   contract on chain that you own and to generate credit

3   that is yours is really the point that is trying to be

4   made here.

5   Now, the previous question from Mr. DeWaal

6   was what are the use cases here? Well, ether is a good

7   example because we are familiar with it. And that

8   familiarity brings us to this blockchain space. But

9   what if for a moment, you did have a crypto native

10 asset that did have a good sense of stability and did

11 represent some sort of commodity? Let's say you had

12 on-chain nickel or on-chain cobalt and you could use

13 that as the asset that goes into this particular vault.

14 Again, this is really where it comes down to the

15 spectrum of choice where on the one side, you have

16 centralized capability.

17   And I really want to emphasize again this is

18 about consumer choice. If you wish to go to the bank

19 and use a bank account and stay with the system, great.

20 If you wish to have the ability to do this yourself,

21 that also should be now a consideration. What DeFi

22 does, it brings that. It brings that with

1 transparency. It brings that so that when you consider

2 how you are going to raise working finance for

3 yourself, how you are going to capitalize your

4 organization on chain, all of this becomes, you know,

5 very much a possibility. But it is dependent on the

6 protocol and its stakeholders to figure what collateral

7 type should be used and under what parameters and under

8 what conditions.

9   CHAIR GORELICK: Thanks. Now I will go to

10 Yesha for the last question.

11   MS. YADAV: I thank you very much for an

12 excellent panel. So my question is really I think for

13 Chad and Eddie and in terms of thinking about how you

14 deal with fragilities in the underlying blockchain. In

15 particular, when we see ether, for example, it is very

16 popular. It is used widely for various types of coin.

17 And it has created concerns about potential

18 difficulties, latency, delays that might exist within

19 the blockchain itself to put pressure on that

20 blockchain. So when you have so much dependence on the

21 ether blockchain for Paxos, in particular, how do you

22 deal with the fact that potentially there may be

1   fragility in the underlying blockchain, that users may

2   default in large volumes to using the dollar-

3   denominated system as a whole?

4   And the second question I had was in relation

5   to the fact that we do have an immutable blockchain for

6   ether and the fact that you are regulated. How do you

7   deal with errors that exist, for example, fat-finger

8   trades or Herstatt risk or fraud and clawback that

9   might be necessary from time to time? How do you

10 account for that in your own systems and, in

11 particular, with respect to the calibration of the

12 collateral that you keep to back up the Paxos coin or a

13 JPM?

14   MR. CASCARILLA: Yes. So I think there are

15 two components. Certainly Ethereum has a network

16 effect to it right now. And so most people are using

17 Ethereum as a smart contracting layer. It is by no

18 means the only protocol for this. I think there is a

19 tremendous amount of capital and intellectual work

20 being done on how you can both increase the speed of

21 Ethereum but around other chains as well.

22   And ultimately for Paxos as an issuer, we are

1 being responsive to our customers. If they would like

2 us to issue in other chains -- and we certainly have

3 gotten interest to do that -- we will. And so we are

4 by no means tied to Ethereum.

5   I think from a practical perspective, at 17

6 transactions per second, which is where Ethereum is at,

7 that couldn't run all of the world's transactions. I

8 don't think anyone believes that. It certainly needs

9 to do a lot of maturing in order to be able to be more

10 useful. But, on the other hand, you haven't really hit

11 capacity constraints in a way that has been truly

12 debilitating. There have been examples where

13 bottlenecks have happened and increased block sizes.

14 And so certainly if there was a big adoption, which

15 would be great -- I think we all think that is

16 fantastic -- there will have to be either some

17 solutions around what are so-called second layer and

18 lightning networks and channels or usage of other

19 chains. And we are certainly very open to both of

20 those.

21   I think 17 transactions per second to put

22 that within some kind of a framework, Visa is at maybe

 1 1,700 transactions per second. Stellar, which is

 2 another chain, is at like I think it is 150. So you

 3 couldn't run. Just to be really clear, you could not

 4 run the entire world's payment economy or otherwise on

 5 a centralized, open public blockchain right now. And I

 6 don't think anyone believes you can, but I do think

 7 this is an engineering problem that is solvable. And

 8 there is a lot of headway being made every day, every

 9 month. And so I think it will be a question of

10 adoption versus innovation here in terms of being able

11 to match that in the case of Ethereum, but there are a

12 lot of different chains that could be used. Some of

13 them are built specifically around solving the problems

14 of payments, as opposed to maybe solving the problem of

15 smart contracting, which Steven has been talking about

16 here. And so you might not even be in a world where

17 one chain does it all. I think that is fine because

18 you create interoperability.

19   I think your second question was around how

20 are we managing risk around compliance and other

21 things. So just to go back -- and Herstatt risk, et

22 cetera -- so we don't really have -- we are not trying

1   to take bank risk here. We have some limited bank risk

2   for the onramps and offramps. When people send us

3   money, we are taking that money, and we are sweeping it

4   either into a network of banks, where you have FDIC

5   insurance, or into T-bills or into T-bill over

6   collateralized reverse repo. So in any case, you are

7   taking almost no risk, just really U.S. government

8   risk, and no interest rate risk. This is very, very

9   safe. This is far safer than money held in a bank. We

10 have done that very specifically because we want to

11 make sure that it is a dollar on a blockchain that you

12 know you could always redeem. And so that is how we

13 tried to manage that risk.

14   Now, there is a second risk, which is the

15 money is moving out from Paxos onto the public

16 blockchain. We monitor the blockchain. We have tools

17 to do that. They are very advanced. You can

18 understand what is happening.

19   And then there is a second component, which

20 is we have a specific feature in our smart contract

21 that allows us to seize and freeze, which we

22 deliberately put in with our regulator, that allows us

1 to freeze a wallet and seize funds in it if we receive

2 a jurisdiction from a lawful subpoena. We can't do it

3 on our own. It is very clear, you know, in the terms

4 and conditions. By the way, this is true of almost

5 every smart contract. Whoever trades a smart contract

6 has a lot of control over it. We have just been very

7 explicit about when we would adjust a smart contract.

8 And it would only be if there was a lawful subpoena

9 from a jurisdiction. Otherwise, it is able to be moved

10 around. And we try to monitor to make sure that

11 everything is being used correctly. I think the

12 onboarding/the offboarding provide a lot of that,

13 protections as well.

14   MR. WEN: If I may add, look, the capacity

15 constraints questions is an interesting one. And we do

16 do work on making sure that the infrastructure can cope

17 with the capacity and the utilization we have. And

18 that is no different than many of the applications the

19 firm builds for processing client transactions.

20   To Charles' point, it is an engineering

21 problem. And there are ways to kind of optimize,

22 parallelize, and achieve greater scale. But the usage

1   can be incremental in how we onboard more customers,

2   and the load factor can be controlled. So it is not

3   that we will turn on everybody all at once onto the

4   platform, whether they will be gated and onboarded

5   accordingly based on the capacity that is available.

6   Further, the implementation is technology-

7   agnostic. You can actually reimplement it to different

8   types of protocol underneath. We have discussed some

9   of those. We haven't done it, but the ability for it

10   to be protocol-agnostic is also an important aspect of

11   these tools so that we can adapt as needed.

12   Now, the second question in regards to kind

13   of the onramp is, how do you make sure that those fat-

14   finger issues and controls do not affect this? Well, I

15   would say because it is a closed-permission network we

16   are trying to construct, it is no different than how a

17   person building a digital application, submitting a

18   payment would interact in the same control processes

19   these would apply for us in our case and how an

20   importation will work. And a lot of times, part of the

21   reasons that we are waiting for regulatory is

22   essentially the process of verification and making sure

1   things work and can scale, you know, is onerous. And

2   we would be subject to the same level of controls we

3   have for JPM Coin versus any other applications that we

4   know.

5   CHAIR GORELICK: Okay. Thank you, everyone.

6   And now let's move on to the third panel before we take

7   a break for lunch.

8   This panel will be presenting on some

9   applications of the ISDA common domain model. And

10 presenting on behalf of ISDA will be Ian Sloyan, the

11 director for market infrastructure and technology at

12 ISDA. Ian, the floor is yours.

13   MR. SLOYAN: Thank you very much. And thank

14 you to the committee for inviting me here today.

15   Before we get to the applications of the CDM,

16 I am going to start from the start and explain what it

17 is because I have already had that question this

18 morning. So let's get started with that.

19   We think about the market infrastructure that

20 we - - that exists. This is a very basic diagram of

21 how we see the sort of infrastructure of the

22 derivatives markets but any markets, really. We have a

1 number of different entities with relationships, a

2 trading venue where trade might be executed, a bank

3 facing corporate hedging, transaction clearinghouse,

4 securities depositories, custodian bank, trade

5 repository. The problem we have is that all of the

6 information that has been exchanged is on different

7 formats and different standards. There are some

8 standards that are used for exchanges' information, but

9 at every point in the chain, we see people storing

10 information in different ways. At the same time,

11 whenever changes are made to this data through the

12 lifecycle of the trade, we see that those changes are

13 made in different ways, which causes a lack of

14 consistency to the records. We have many different

15 agencies and services involved in this part of the

16 market.

17   So the CDM, I want to put it in context of

18 what ISDA is doing. So ISDA provides standards for the

19 derivatives markets through our well-known legal

20 framework and the master agreement, the definitions, et

21 cetera.

22   In order to sort of digitize these markets

1   and make standards work better, we need to see things

2   in sort of a flow of three steps. We need to

3   standardize the legal documentation and best practices

4   in a way that then can be digitized. And then once

5   they are digitized, we need to distribute them so

6   people use them and implement them consistently. So in

7   that vein, we have a number of initiatives at ISDA at

8   present on the legal side to try and standardize some

9   of the clauses found in certain parts of the

10   documentation where bespoke language is typically

11   negotiated.

12   Then on the digital front to digitize these

13   clauses and best practices, we have the CDM, which I am

14   going to talk about today. We have ISDA Create, which

15   is a platform for negotiation of ISDA documentation,

16   primarily the credit support annexes required for the

17   new initial margin rules. We also have an FpML data

18   standard for messaging, which is used to send

19   information to trade repositories for other purposes,

20   such as confirmation.

21   So the CDM is what I want to talk about

22   today. The key sort of aspect of the CDM, well, it is

 1 the distribution mechanism. The CDM is not supposed to

 2 be a new standard, a new format. I's a model. And it

 3 is a model which we want to distribute in as many

 4 languages as possible so that people will be able to

 5 implement it. So let's talk about the CDM in a bit

 6 more detail.

 7   So, as I said, it is a model. The key part

 8 is the third word of the CDM. It is a model for the

 9 products, calculations, and events that happen in

10 derivatives markets. It is presented as data and

11 functions in the model. And then we present it in --

12 in what is called a composable model. We use basic

13 components to build more complex things. That is as

14 deep on the technical design that I will go into. And

15 the key aspect, as I mentioned, was that we want this

16 model to be used and implemented as natively as

17 possible. So we try and distribute the model in

18 different languages for ease of implementation and

19 consistent implementation because that's the purpose of

20 the CDM, is to try and get the legal clauses and best

21 practices on the left-hand side of the previous slide

22 to be implemented consistently. And that is the main

1 goal.

2   So how do we do that? Well, I am going to

3 call out a legal definition here from the 2006 ISDA

4 definitions. The green text is copied and pasted from

5 the definitions. It tells you how to calculate the

6 floating amount on an interest rate swap. And then at

7 the very bottom, which is in blue, highlighted, is the

8 code for implementation of our calculation. I am not

9 sure Maybe reading the green text is easier for a

10 lawyer, but the implementation is more consistent if we

11 use code. So this is the CDM code, which can drive

12 consistent implementation of the floating amount, which

13 may be the cause of breaks if someone misinterprets the

14 legal definition. So the CDM is a model distributed

15 hopefully so that people can implement consistently.

16   Now I am going to talk about some of the

17 applications because that was what was promised to be

18 the focus of today's presentation. But those

19 collateral and reporting are just two of the

20 applications which we are working on at the moment. So

21 I just want to mention where they fit in some of the

22 other priorities. And these are sort of, you know,

1   short-term priorities for the first half of this year,

2   really. So we are working on an implementation of the

3   CDM for interest rates clearing processes and how do we

4   move a trade to clearing. And we are working with some

5   of the clearinghouses involved in those markets to work

6   on that. And they will be implementing that part of

7   the model, collateral data and processes, which I am

8   going to go through in more detail. We have developed

9   an equity swap model or equity derivatives model, which

10   we are currently enhancing and that's already been

11   worked on with a company who is working on the

12   implementation of equity swaps on DLT. So that is one

13   sort of example where a company can take our code and

14   implement it on their system.

15   Regs to reporting, which is going to be the

16   demonstration. I am going to run a short video to show

17   you how we have tackled CFTC reporting. And the

18   digitization of ISDA definitions, as alluded to on the

19   previous slides, that is something that we are very

20   keen on working on at ISDA at the moment. And we are

21   looking at, in particular, some of the areas around

22   benchmarks, IBOR transition, fallback mechanisms, and

1 how maybe the CDM code could allow implementation of

2 those fallbacks in a more consistent way, rather than

3 just publishing the .PDF document to tell people how

4 the fallback should work.

5   We are also working -- we do run the CDM as

6 the ISDA CDM, but we are broadening our community and

7 partners by speaking to other trade associations.

8 People involved in other markets who have seen the sort

9 of initial work we have done and pilots we have done

10 are impressed and would like to deploy a similar

11 approach in their markets. So, as I said, we are going

12 to focus on collateral and reporting in the rest of the

13 presentation.

14   So I want to talk about at a very high level

15 the benefits of having a consistent model and where

16 these two examples fit in. So there are three themes

17 that I like to kind of focus on in regards to CDM

18 benefits. So it enables interoperability in removing

19 the burden of setting up connections between the

20 entities we saw in that first slide. Hopefully that is

21 quite clear. If we have one consistent model for the

22 data and another consistent model for the processes,

1 which operate on that data, it should improve

2 interoperability. And it should remove the burden of

3 setting up connections to new systems. And the

4 collateral workflow is possibly an example which I will

5 be able to demonstrate in a moment.

6   Transparency between regulators and market

7 participants, again, the reg-to-reporting example fits

8 into this benefit. And, finally, which I don't want to

9 lose sight of, the ability for the CDM to speed up the

10 development of new solutions for markets that it

11 pertains to for this domain, we can allow providers to

12 focus on technology, rather than asking them to

13 understand the market. And hopefully I can show you in

14 a bit more detail with this slide.

15   So if we think of how the, you know, products

16 are brought to market today, people have to research

17 the business domain. They have to gain subject-matter

18 expertise. They have to design their own proprietary

19 model to solve the problem. They have to implement

20 that model on technology. And then they need to

21 convince the market that the solution is reliable and

22 consistent with market practices.

1   And, then, the next group comes along in

2 green and does the same thing. The outcome are two

3 systems, which may not talk to each other, even if they

4 must do for some purposes. Using something like the

5 CDM and making it available to the market in an open

6 manner so that it can be used means that they just need

7 to learn about the CDM. And then they can take the

8 components that they need to build their system and

9 implement them in building their solution on their

10 technology. So if they have got a really good

11 distributed ledger, if they are really good at privacy

12 or clouds, whatever it may be, they can focus on that

13 and not on the domain expertise, which we can give to

14 them based on the expertise of ISDA's members.

15   And, then, the outcome is that with those

16 systems that use that common domain model, they should

17 be interoperable at the points where they need to be.

18 So by deploying the CDM, we believe new systems will

19 have interoperability, a shorter time to market, and

20 association with a recognized market standard from

21 ISDA. And, based on the subject-matter expertise

22 obviously of our members.

1   Now I want to go into the interoperability

2   and STP with specific relation to collateral. I am

3   going to show you some of the components and some of

4   the code we have worked on for that.

5   So, to think about this in a bit more detail,

6   when a trade is executed on a venue or over the phone

7   or whatever way it may be, the information is agreed at

8   that point. Both sides seem to know what they are

9   talking about and believe that they are agreeing to

10   some terms. The terms tend to be stored, then, and

11   captured in the systems in different ways. And then at

12   each point throughout the lifecycle -- and this is what

13   the left-hand side of the screen is supposed to show,

14   that each event is executed in a different way. So we

15   have the new trade stored and executed in a different

16   way between the bank and the client. The increase is

17   then executed in a different way if they are increasing

18   the position. Margin and collateral processes are

19   implemented differently and processed differently,

20   possibly referencing a different format of where they

21   stored the CSA. One might be on paper, and the other

22   one might be in a .PDF folder somewhere.

1   And, then, finally, the trade comes to

2   maturity, and the maturing of the trade might be done

3   differently. This is what causes breaks and

4   reconciliations that are required or if we can get

5   people code that they can implement in the form of

6   DS-CDM, market participants can implement the same code

7   for each part of the event. They don't need to be

8   using the same system. We are not talking about

9   necessarily a system, but that will be probably a good

10   way to implement it. But we can give them very formal

11   rules as code that they can implement so that each step

12   in the process is done consistently and, moreover, we

13   can use a standard way of representing the trade when

14   it is captured. We can also store the CSA information

15   in a standard way, too.

16   So, looking specifically at the collateral

17   management process and lifecycle, we are looking at the

18   CDM and developing the CDM for a collateral model,

19   let's call it broadly, for the CDM, where we can

20   provide a standard digital reference data form of the

21   CSA, which can be used to store CSA information

22   consistently. We also have ISDA Create, which allows

1 the execution of the collateral documentation and order

2 documentation in time in a consistent manner.

3   Collateral eligibility, how do you identify

4 eligible assets for collateral is something that isn't

5 standardized today. There is an initiative at ISDA,

6 though, which is working on that. And we are at the

7 same time taking the output of the standardization work

8 and putting it into the model and reviewing it

9 digitally in the model so that we could distribute that

10 out as a digital model that people can implement.

11   Connecting different systems in the

12 collateral lifecycle with consistent data model is a

13 prerequisite for any automation. You can't run smart

14 contracts if things aren't consistently described and

15 connected. And that is what the diagram on the right

16 shows for ISDA Create where the CSA document could be

17 executed. It could come out in CDM form, go to the

18 various vendors in the market infrastructure. And they

19 all -- whatever part of the proposal or process they

20 are part of, where they do interact, they will be

21 interacting with consistent data standards.

22   Finally, inconsistent calculations cause

 1 breaks and disputes. Data infractions are often

 2 misinterpreted in implementations and cause breaks that

 3 are settlement breaks that people have to resolve.

 4 That is a cost that we don't believe is necessary in

 5 the same way calculations for - - on CSAs tend not to

 6 be implemented consistently. And there are disputes

 7 and inconsistencies there of settlement which cause

 8 problems. So we are also working on that.

 9   So I am not going to go into too much detail

10 because the diagrams can be a little bit scary, but we

11 have taken the CSA 2016 IM and VM CSAs in the case of

12 New York law, and we have coded them into the CDM. We

13 are working on the 2018s at the moment. I know there

14 are other documents that are currently found on ISDA

15 Create.

16   We can create a standard data model for

17 those, and that is on the right-hand side as basically

18 a screenshot of the graphical navigation of our CDM

19 portal, where we have a model for these documents.

20 Eligible collateral, as I said, is a problem. And this

21 is sort of the nascent work on a collateral eligibility

22 model that could hopefully align custodians and other

1   market participants and vendors to come around to

2   having the same standard model for how they describe

3   these assets because it is really just an instrument

4   identification problem when you get down to it.

5   In the CSAs at the moment, that is a free-

6   format eligible collateral schedule. There is no

7   standardization there. We would like the digital form

8   of these documents to have this module kind of inserted

9   for a standard digital way to describe collateral.

10   Calculation text. This is pretty hot off the

11 press. I think the guys just released it the other

12 day. This describes how you calculate the delivery

13 amount for initial margin from a 2018 IM CSA. There is

14 the legal text on the left. And on the right is the

15 code that will get you the same performance hopefully.

16 It was written with the internal lawyers and developers

17 sitting around the table. I mean, you know, I think it

18 took -- okay. It probably took about a couple of

19 afternoons to get the lawyers to understand what the

20 developers were talking about, but, you know, by the

21 end of it, I think it was a very powerful message that

22 the lawyer involved turned around and said, "I really

1 understand the code now." So that is a positive.

2   But this is the sort of thing that we can

3 deliver with the documentation, a code implementation,

4 which allows consistent implementation of that for the

5 purpose of smart contracts and automation, et cetera.

6   Okay. Putting it all together, looking at

7 what we have, so we could negotiate the CSA on this to

8 create the CDM form of the CSA could come out of ISDA

9 Create. And then we have a model for the calculation,

10 the collateral selection, the posting of the security.

11 These are all components of the CDM that exist today.

12 So if someone was building such a system or multiple

13 parties were building systems across that lifecycle, we

14 could give them the CDM model components so that they

15 could implement them.

16   All right. So that is it on the collateral

17 application. I want to talk about regulation and

18 reporting now. So how do we implement, how does the

19 market implement regulation today? So regulators

20 publish rules. And trade associations such as ISDA

21 work with members to try and interpret the rules and

22 then develop best practices, which can be supplementary

1   to the rules to allow people to implement them

2   consistently. Those tend to take the form of artifacts

3   such as best practice documents or spreadsheets, which

4   we host on ISDA's website or, indeed, the rules

5   themselves, which take the form of being on the Federal

6   Register.

7   Industry participants then read those rules.

8   They read the best practices and, in totality, come

9   together on an implementation that their developers

10 implement. It doesn't always meet the necessary levels

11 of data integrity, of consistent implementation that we

12 would expect from what are often very prescriptive

13 rules. Whatever happens between the best practices and

14 the rule writing and the developer implementing the

15 system, there is too long a chain and there is too much

16 cause, there is too much of different interpretation

17 happening. And what we would like to do is see a much

18 more consistent level of implementation and

19 interpretation of those rules.

20   So how can we do this? Well, we can use a

21 model such as the CDM to represent the rules as code.

22 And we can operate on the data, the transaction data,

1   which is already in the CDM form and then project from

2   the CDM form of that data to the regulatory requirement

3   and maybe the CFTC reporting rule or could be some

4   other type of regulation. So the idea is that the CDM

5   can implement the rules and best practices and allow

6   people in to let them across the industry in a much

7   more consistent way. Reducing that interpretation risk

8   from the developer's point of view by giving them code

9   they can implement and components they can implement in

10 their systems, rather than having them have to read

11 something that a business analyst has put together

12 based on a lot of industry discussion. And hopefully

13 that will improve the data integrity.

14   Now, we did this last summer as part of the

15 digital regs report in the pilot with the Bank of

16 England and FCA. We were approached to see if the CDM

17 would be a potential way to explore digital regs

18 reporting in that pilot. We were successful in

19 applying it to EMIR and MiFID rules, and it was quite

20 successful. The outcome is that I think a lot of our

21 members are very excited about this new way of

22 developing or working on best practices around

1 reporting. And with the idea to come here today, we

2 took some of the CFTC rules and have a demonstration of

3 how those could be implemented in the same way. And we

4 took some trade data from the public tape and developed

5 a prototype of the Part 43 reporting rules. Now, these

6 are based on the reporting rules as they were before

7 the publication last week of the updates. But we will

8 hopefully demonstrate the power of what we can do here.

9 So we define a report so you could maybe

10 think of that top level of text and the bottom level of

11 the table that you find in the annex to the reporting

12 rules. We can define different parties as part of

13 this. So we defined the CFTC based on I think the

14 definition found on the CFTC webpage. We can define

15 the standard, the actual form that the report needs to

16 be generated in, so in this case the FpML SDR message

17 specs. And then we have each field. And each field

18 can then have a logical rule related to it to show you

19 how to fill in that field, so to speak.

20 So we are going to look at one example here,

21 where asset class is a field that needs to be filled

22 out on the Part 43 public report. And we are going to

 1 fill in some rationale here where we could, you know,

 2 note or annotate where ISDA maybe has provided some

 3 supplementary best practice to the actual reporting

 4 rule. We could note I would say what we are doing here

 5 and why we have implemented this logic. In a very

 6 transparent way, as I mentioned, this code exists in

 7 the CDM. The CDM is made available publicly.

 8   And here we have where the system -- and this

 9 is basic implementation where we have the code running

10 against real example trades. So we have taken, we have

11 created a dataset of example trades, which we are

12 creating the reports from. These, the top five reports

13 there, are real data from the public tape that we

14 observed. And we constructed sort of CDM form of those

15 to project out to the report.

16   You can see there by using the tools we have

17 here, we can live-update the reporting rules. So COR

18 is going to change to credit. But you can see how if

19 you wanted to explore certain impacts of new rules or

20 different changes, what they might look like if we had

21 a large dataset with which to test against. Now, this

22 is obviously only very much a prototype.

1   Here is an example we found in the SDR data,

2   trivial perhaps, but the price notations are all

3   measured to -- there is no specification about how many

4   decimal places the price should be reported to. So you

5   can see that people have different numbers of decimal

6   places through just writing a basic rule into filter.

7   Should I say the price notation? We can set the form

8   up to two decimal places. And you can see that can be

9   updated. That is the sort of thing that ISDA could

10   help members implement in real time to try and help the

11   consistent implementation of the reporting rules.

12   So that is the end of the demo. And there is

13   a link to that, which I will share with the committee

14   after. I think we wanted to really just get the point

15   across regarding the direct implementation. We at ISDA

16   and our members believe that there is a potential to

17   approach regulation in a different way and sort of

18   shift the paradigm so that we can work together with

19   regulators and use kind of build test implementations,

20   get lots of data, show up what the application of the

21   rules would look like, and then iterate on that over

22   time to reach a better regulatory outcome. Indeed, at

1 this juncture, with the new CFTC reporting rules, we

2 think there is a potential for an industry project run

3 through ISDA or perhaps with other organizations to try

4 and achieve that. And that is something we will be

5 exploring with our members in regards to the new CFTC

6 reporting rules.

7   Questions?

8   CHAIR GORELICK: Thank you, Ian. Very

9 helpful. It seems like a very sensible approach.

10   I guess I will start with the first question.

11 You are talking about making the code publicly

12 available. Is this a true open-source model or is

13 there some other way that you are going to make it

14 available?

15   MR. SLOYAN: The code is open-source. It is

16 available for download in all those different

17 distributions, different languages as people need. It

18 isn't under Apache 2 license. It is under a different

19 open-source license. And it is obviously -- but it is

20 completely open-source for people to use in their

21 implementations. Indeed, they have been --

22   CHAIR GORELICK: Thank you.

1   Haimera?

2   MR. WORKIE: Thank you.

3   You mentioned earlier that one of the things

4   that was designed to help remediate was the idea that

5   people have potentially different ways of calculating

6   the information. Does the code actually become part of

7   the contract or how is that treated in terms of -- do

8   they just agree to it or is it actually incorporated in

9   the context of the contract?

10   MR. SLOYAN: So I think the CDM will exist as

11   kind of an implementation layer. So those components

12   are not part of the contract per se. I think over

13   time, as the sort of smart contracts topic matures,

14   perhaps it will be by reference to a specific piece of

15   code.

16   But the CDM is intended to help implementers

17   implement in the way they do today. So there are

18   systems built today to do calculations, which are not

19   necessarily -- that code is not part of the contract, a

20   part, you know, of the conformation of the trade. But

21   over time, I think the smart contracts topic and as

22   people look at that and sort of -- is the contract code

1   is something that this code could be incorporated to.

2   MR. WORKIE: Thanks.

3   CHAIR GORELICK: Okay. Thank you very much,

4   Ian. And I think with that, we will take a break for

5   lunch. We are expecting to be back here at 1:30 p.m.

6   Thanks, everybody.

7   (A luncheon recess was taken at 12:38 p.m.)

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

1

2

3

4

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

6   (1:35 p.m.)

7   MS. TENTE: We would like to call the TAC

8   meeting back to order, and I will turn it over to

9   Richard.

10   CHAIR GORELICK: Thank you very much, Meghan.

11   I would now like to turn to our next panel,

12   in which we will hear an overview of the insurance

13   market for crypto custodians and how the insurance

14   market is driving best practices and a discussion on

15   why multi-party computation, or MPC, may be a promising

16   solution to some of the challenges around custody.

17   Our presenters this afternoon are Jim Knox,

18   managing director for technology and communications

19   industry-regional practice leader at Aon; and Itay

20   Malinger, co-founder and CEO of Curv.

21   And, with that, I will turn it over to Jim

22   and Itay.

1   MR. KNOX: Thank you very much for that, and

2   thank you for the opportunity to speak with you today.

3   I am very grateful for that.

4   In case there is a lingering malaise due to

5   food exposure at lunch, I am going to open with some

6   opening statements that might get your attention.

7   It is my belief that insurance is absolutely

8   critical to the digital asset space. It is my further

9   belief that without a robust participation by the

10   insurance companies partnering in the digital asset

11   space, the space will not scale to its full potential

12   without the insurance companies fully embracing this

13   space. I will just open with that.

14   Start off with some slides. Historically,

15   there have been some losses in this space, some

16   unfortunate incidents with stealing and hacking of some

17   significant losses listed here, listing digital assets

18   stolen from exchanges that have been highlighted in the

19   past, some pretty big headlines with the exchanges that

20   have been hacked.

21   The next slide goes into the ICOs, some of

22   the reputed fraud that has been involved with some of

1   the ICOs, a lot of headlines being made here as well.

2   The net effect of all of these headlines,

3   whether it is the fraudulent activity with the ICOs,

4   whether it is with the exchange that had been hacked,

5   and some massive amounts of money stolen from the

6   exchanges in the crypto or digital asset space, the net

7   effect is that it has had a very chilling effect on the

8   insurance industry. It has had an effect on the terms

9   that are being offered to companies in digital asset

10 space, on the amount of limits that is being offered,

11 and the type of insurance that is being offered. So

12 all of this bad news, this negativity has had a

13 chilling effect on the insurance space.

14   Obviously it has not been lost on the

15 regulators. We have comments up here by several

16 regulators, notably Mr. Chairman Giancarlo from the

17 CFTC about how they will strictly enforce fraudulent

18 activity in the space. Insurance companies are aware

19 of this. I am sure they are appreciative of this,

20 these headlines. But the losses still remain out

21 there, and it has had an effect on the insurance

22 companies.

1   So I want to just talk a little bit about

2   anecdotally some of us here with gray hair who have

3   been around for a while, I remember in the late '90s,

4   something called the internet first came out. Back

5   then I was working for a company called Zurich

6   Insurance. I was a young fresh Dino insurance

7   underwriter. At my desk, I was receiving about 20

8   applications a day, sometimes more, from companies that

9   were seeking to make a splash on this thing called the

10 internet.

11   Many of these companies that we were

12 underwriting or at least evaluating for directors' and

13 officers' insurance purposes, it is wild speculation

14 with these companies. There is no clear path to

15 revenue with these early internet companies. They were

16 being successfully wildly funded, though, with no clear

17 path to success, no clear revenue model, no

18 profitability in sight, but they were wildly funded.

19   I would say about two years later, maybe 90

20 percent of the internet companies that we underwrote

21 for, say, directors' and officers' insurance, about 90

22 percent were gone, you know, burning cars on the side

1   of the road. They were just evaporated, disappeared.

2   So what is happening now is, you know, fast

3   track 20-30 years later, some of those young

4   professionals back then who were underwriting those

5   types of risks in the internet space 30 years ago, they

6   are now senior managers at the insurance companies.

7   And they are now listening and the hearing, and they

8   are talking about this new technology called

9   blockchain, somewhat new, in the space. And they have

10   long memories, and they remember what happened back in

11   the day when a lot of these insurance companies took a

12   hit, some severe losses, with the early internet and

13   some of the iterations back then with those companies.

14   So what we have done now, it is becoming more

15   and more of a robust place, the digital asset space,

16   the blockchain space. So this slide here, what it

17   does, it demonstrates. From a perspective of the

18   insurance company, they are looking at several metrics

19   here. So the first top of this chart shows you the

20   typical types of insurances that are going to be

21   offered by insurance company for a company in the

22   digital asset space.

1   So the green, yellow, and red is meant to

2   indicate -- he green is obviously easy to obtain

3   insurance. Yellow is a little challenging. And the

4   right side, the red, is a bit more challenging. So

5   things like surety bonds are quite easy to obtain in

6   the marketplace if you have a need for an MTL license.

7   Cold storage is where you take that -- if I

8   am preaching to the choir, if you know this, indicate -

9   - but cold storage, if you take that digital asset, you

10   download it off the internet, you put it into a hard

11   drive or UBS stick or HSML, it is off the internet. It

12   is very cold.

13   Specie insurance is a very interesting

14   concept. Specie insurance has been around for 100-200

15   years. 100-200 years ago if you had a Monet or a bar

16   of gold and if you stored that, that hard asset, that

17   gold, in a vault, some type of area that was protected,

18   specie insurance is meant to cover the exposure

19   associated with securing that hard asset.

20   When Mt. Gox happened several years ago, we

21   were helping some of the companies in the digital asset

22   space, some of the earlier companies. When the Mt. Gox

1 headlines came out, the insurance industry had a

2 very -- again, the chilling effect on the insurance

3 companies. They started to back away when they saw

4 what happened with Mt. Gox because there is some

5 serious money involved there, some losses.

6   So at Aon, we had to come back to the table.

7 We had to bring the insurance companies back because we

8 had clients who had needs. And we had to think a

9 little outside the box and say, "How do we bring these

10 insurance companies back to the table to offer our

11 clients insurances when you have things like Mt. Gox

12 and there are bad headlines going on?"

13   So not myself. I would like to take credit,

14 but I can't. But somebody at Aon said, "Why don't we

15 use a specie analysis and apply it to digital asset

16 space? Why not apply the same logic? If you are

17 insuring a bar of gold or Monet painting that is being

18 stored somewhere in a secure place, why not apply that

19 logic to a UBS stick that has a bitcoin on it or a hard

20 drive or HSML that has all of these digital assets on

21 them and they are secured safely away off the web?"

22   So we did that. We successfully did that.

1 So now there is an insurance out there called specie

2 insurance, which, frankly, is being used by a lot of

3 the companies now in digital asset space for cold

4 storage. You have cyber insurance. You have

5 technology errors and omission insurance. You have

6 directors' and officers' insurance. The three in the

7 middle there on the yellow on the top, cyber

8 technology, E&O, and D&O, almost all of those

9 insurances are being purchased today by companies in

10 digital asset space.

11   Then you have on the right side, the far

12 right side, crime-hot wallet cover, not an easy

13 insurance cover to obtain. Much, much more due

14 diligence is done on this type of insurance by

15 insurance companies. It is available. You know, we

16 currently do help our clients obtain hot wallet cover.

17   I will tell you that, for some reason, I can

18 speculate why. When it comes to hot-wallet cover

19 insurance, almost primarily the only place you are

20 going to find that insurance is with the London markets

21 right now, not the U.S. markets. They have not fully

22 embraced it.

1   The crime insurance for hot-wallet cover is

2   almost uniquely a London solution right now, London

3   insurance markets. A lot of Lloyd's syndicates are

4   participating in that.

5   If you look at the bottom side of that slide,

6   we are talking about the type of companies out there in

7   the space who are seeking the insurances. If we talk

8   about companies that are using blockchain technology

9   purely, say, for its own intrinsic value, meaning if

10 they are using the blockchain technology for a

11 logistics company or a real estate company, it is much

12 easier to obtain insurance for that type of use.

13   Security tokens, interesting area. This is

14 the CFTC. So I won't get too involved with securities

15 here, but if it is the claim of security, you are

16 acknowledging that we are not going to play games with

17 the regulators. We are going to, you know, call it a

18 security and treat it as such, you know, obtain

19 insurance. Some of your traditional asset managers,

20 advisors obtain insurance. When it starts getting a

21 little bit tricky is the companies that are in the

22 digital asset space are actually touching. They are

1 actually doing day-to-day with the tokens and the

2 assets. When you are talking broker-dealers,

3 custodians, exchanges, minors, the insurance company is

4 a little bit -- they start to get a little bit

5 squeamish because they view more exposure there. You

6 are dealing with these tokens, these assets. You could

7 be tripping regulatory issues. There could be security

8 issues. If they are stolen, these tokens, that starts

9 to get a little bit more challenging with the insurance

10 companies.

11   Far right side, initial coin offerings, it is

12 a dead subject. Some companies now are trying the

13 staff method with offerings and other methods, but it

14 is almost a dead issues as far as your -- an ICO come

15 to look for insurance, you know, "Good luck. God bless

16 you." Not today.

17   Here are some of the issues that the

18 insurance companies are factoring when they are

19 evaluating whether or not to underwrite a company in

20 the digital asset space. Uncertain regulatory

21 environment has an impact on the American and London

22 insurance markets. Perceived reputational risk. You

1   saw it in the headlines that happened earlier.

2   My personal believe is that a lot of the

3   insurance companies, particularly in America, the U.S.

4   insurance companies are on the sidelines right now.

5   They are on the sidelines in the digital asset space

6   because a lot of the senior executive management there

7   are not going to support, put out terms. And if, God

8   forbid there is major loss, a major hack, and it is on

9   their watch, potentially could go back and hurt them.

10   And I personally think that is why a lot of

11 insurance companies -- it is one reason, simplistic

12 reason, but a lot of insurance companies are on the

13 sidelines right now.

14   There are regulatory issues they are very

15 concerned about. Frankly, it is a developing space.

16 But by comparison, it is a fairly new space. Because

17 of that, there is not a lot of claims history. There

18 is loss history developed that the actuarials of these

19 insurance companies can evaluate and make a

20 determination on this risk. So the fact it is somewhat

21 a nascent industry, somewhat has an effect on the

22 insurance companies.

 1   Limited loss history, like I described. The

 2   negative press has a huge effect on the insurance

 3   industry. And, again, people are very hesitant to put

 4   the name out for risk if, God forbid, there is going to

 5   be a loss.

 6   Some of the coverages to consider. We talked

 7   about this briefly. Most of your insurance offerings

 8   out there for companies in digital asset space are

 9   directors' and officers' insurance. You have cyber.

10   You have technology errors and omissions, which covers

11   the issues regarding the technology platform that a

12   company is using; investment advisors; crime insurance.

13   All of these different types of offerings are out there

14   for the markets.

15   As far as the actual markets who offer the

16   insurances, this gives you an idea of what we are

17   facing. The D&O insurance marketplace, if you look at

18   the primary, which means on the right side on top, it

19   says, "Primary." That is the first insurance company

20   that will take that first layer of insurance. And they

21   have what we call the burn layer, if you want. There

22   is a claim that comes in. So they are the ones that

1   are on the ground from dollar one if a claim comes in.

2   So you see Lloyd's there, which is, again,

3   Lloyd's of London mark, which is very big in the area,

4   very supportive. You have some other markets as well.

5   What is interesting is in that first tranche there, you

6   don't see the big names in the insurance space, again

7   because all of the bad news, the negative press,

8   regulatory uncertainty has had a chilling effect on the

9   insurance market.

10   So in the digital asset space as far as D&O

11   and then it is crime. As far as crime, interestingly,

12   the top right quadrant there, Lloyd's, is the only

13   marketplace right now for crime insurance for hot

14   wallet coverage, there are some American markets that

15   may attach a very, very high level if the company is

16   buying $100-$200 million worth of hot wallet insurance.

17   But you don't see a lot of purchases that size.

18   E&O market, very similar. Again, you see

19   Lloyd's as the primary player. You have Munich Re and

20   some others. Then you have some others down below.

21   Someone made a comment to me a while ago. I

22   do believe it is very true. I like to think that the

 1 insurance industry is driving best practices in the

 2 digital asset space, you know. And why? For the

 3 following reasons: that if you do not have your house

 4 in order as a digital asset company, you will not get

 5 insurance. And in order to get the insurance, you have

 6 to have very, very, very good, robust compliance

 7 procedures in-house. If you are dealing with the

 8 regulators, you have to let the insurance companies

 9 know where you are with your regulators, how are you

10 doing with them, is your timeline good to meet all of

11 the requirements with them. You must have very, very

12 good KYC/AML in-house procedures. If you don't have

13 that, you will not get insurance.

14   And there is a host of items here on this

15 slide that shows you just how deeply the insurance

16 companies are going to do a dive into your company, the

17 diligence, and ask you exactly what is going on with

18 your company, what are your best practices, what is

19 going on to get that insurance.

20   So, with that, I will leave it at that, but

21 thank you very much for your time. Thank you very

22 much.

1   MR. MALINGER: All right. Good afternoon. I

2 am Itay, Itay Malinger. I am the co-founder and CEO of

3 Curv. We are a digital asset security company, a tech

4 company based in New York.

5   I am going to touch on some of the points

6 that you heard from Jim around digital asset security.

7 So when insurers are trying to evaluate the security

8 posture of their customers that want to buy insurance,

9 we will talk a bit about the evolution of security for

10 digital assets and the challenges that they pose,

11 specifically the challenge of securing private keys. I

12 assume you all know that private keys are those secrets

13 that enable to sign transactions on a blockchain. And

14 they pose a very significant challenge of a tradeoff

15 between security and liquidity. And solutions today

16 are very difficult to get insurance for but also

17 impractical to scale.

18   We will then present -- it is going to be a

19 bit technical, but we will present some teasers around

20 the latest and greatest in cryptography to enable to

21 address those challenges, so multi-party computation,

22 zero-knowledge proofs, and an example of a protocol

1 called Diffie-Hellman. And then we will circle back

2 and talk about what this means for custody and for

3 digital asset security.

4   So, as we mentioned, private keys are a

5 single point of failure as long as you talk about

6 digital asset security. And since it is easier to get

7 insurance for cold storage compared to hot wallets, as

8 was just mentioned, the reason is that it is perceived

9 to be actually more secure specifically from

10 adversarial attacks. But when you think about what are

11 the attack vectors around digital assets, it can be, of

12 course, the first thing that comes into mind is an

13 adversarial cyber attack -- right? -- hackers getting

14 into a hot wallet and stealing the funds. But it can

15 also be an insider threat, of course, the people that

16 you trust the most to have access to a cold storage

17 vault in that case.

18   Once they are within that cold storage

19 facility and have gone beyond all of the authentication

20 mechanisms to that cold storage vault, they have full

21 access to the entire liquidity of your company. So do

22 you really trust those people to get in? And how can

1 you construct a way to better protect from those

2 insiders?

3   And, finally, because the private key is the

4 holder of the identity on the

5 blockchain -- right? -- the private key is the way to

6 generate your identity on the blockchain so that you

7 can receive assets, losing a private key means losing

8 the ability to make transactions. And you have seen

9 that as well.

10   So there are many cases that you have heard

11 about, such as cases in which people lost their keys.

12 A loss of keys means the keys are there forever. They

13 were not stolen. There is no hacker who got the

14 assets. There was no employee who stole the assets.

15 And, yet, mathematically, it will not be possible to

16 retrieve those assets in the near future.

17   So, really quickly, I will go over the

18 existing solutions. I think these are terms that most

19 of you have heard in the past, but you will see this

20 tradeoff between the more liquid solutions that enable

21 you to withdraw funds quickly versus the more secure

22 solutions that enable you to keep the assets more

1 secure, especially from adversarial threats. Right?

2   So, of course, a wallet is the infrastructure

3 to secure their keys. So it can be either software-

4 based or hardware-based. The hardware are HSMs if you

5 heard about that term. It can be a consumer-based

6 piece of hardware or more enterprise-grade, but, of

7 course, the software-based solutions since they are

8 based on software, they can be more flexible to address

9 many consumers trying to withdraw funds.

10   Another tradeoff is between hot wallets and

11 cold wallets. When we say, "hot," we mean wallets in

12 which the private keys are connected to an internet-

13 connected machine. And cold wallets are wallets in

14 which those keys are disconnected from the internet,

15 and you can see this is state-of-the-art today. Right?

16 Take a World War II bunker. Take a piece of private

17 key, and keep it within that bunker. There are

18 actually vendors who are offering that. And it is good

19 practice, again, mainly against adversarial cyber

20 attacks.

21   Another element is usually when we talk about

22 private keys and public keys, an address or a wallet or

1   a target destination can have a single-sig address.

2   But for some blockchains, specifically bitcoin, there

3   are blockchains that support multi-sig address. So

4   think of it as, instead of having just one key, you can

5   have two separate keys, just like in some banks, when

6   you go to a vault in the bank, there is the clerk that

7   has one key, and the owner of the asset that has the

8   other key. And both need to open the wallet.

9   And, finally, one more technique that is

10 called sharding, or Shamir's Secret Sharing if you have

11 heard. It is the ability to take a key and split it

12 into separate locations. Every time you want to sign a

13 transaction, you need to bring those pieces back

14 together, sign the transaction, and then delete the

15 pieces that you brought together.

16   So, as you can see, on the right side, we

17 have more complex constructs. Some of them are

18 literally physical to secure the blockchain. So you

19 have this great construct, very state-of-the-art

20 blockchain, which is very connected and decentralized,

21 but, effectively, the security requirements are causing

22 solution providers. Right? Most exchanges will have

1 98 percent of their assets in cold storage. Right? So

2 eventually you are having a very centralized set of

3 service providers, who are holding their assets in a

4 very disconnected environment.

5   And the question is, can we solve this

6 tradeoff between security and liquidity? And, now,

7 there is a way to solve that. And, actually, the

8 answer is, of course, yes.

9   So if we look at the way the blockchain is

10 designed, what is a blockchain, it is a set of

11 protocols that enable players or participants in the

12 network to maintain one ledger that everyone knows and

13 everyone agrees upon, right? And the way to do

14 that -- and what is powering the blockchain is actually

15 math, right?

16   So three simple mathematical functions that

17 are being used over the blockchain are the ability to

18 create a public key. Right? I said the private key is

19 a secret known to the holder of the asset, but their

20 identity is their public address, right? So deriving a

21 public address from a private address is a mathematical

22 function, actually a very simple one, just taking some

 1 number to the power of the private key. And that is a

 2 public address. So that is one mathematical function.

 3   And another mathematical function would be

 4 the function that is used to sign a transaction,

 5 basically to say, "I am who I say I am. This is the

 6 transaction that I want to make. And this is the

 7 mathematical proof that I want to make this

 8 transaction." Okay? So signing is just another

 9 mathematical function.

10   And, finally, the ability to validate that

11 the person who said who he is -- right? -- is actually

12 behind this. The ability to verify that a transaction

13 is authentic is also a mathematical function.

14   So, effectively, all of the blockchain is

15 powered by those mathematical functions. And, yet, the

16 private keys are kept in cold storage vaults of World

17 War II, right? So MPC and zero-knowledge proofs are an

18 attempt and a successful one that is on the mainstage

19 today to take math itself to protect the private key

20 itself. Okay? And the way to do that is effectively

21 to eliminate the private key and to create identities

22 in which the secret material is distributed across

1   many, many players.

2   So this is the point at which we are going to

3   do a bit of math, but I think it is going to be more

4   clear once we are done. So let's take a very simple

5   example of a multi-party computation protocol, which

6   is -- let's say we want to calculate we have a circle

7   here, and we want to calculate the average salary of

8   the people around this circle. Okay? So we could have

9   brought some trusted third party, right? And we don't

10   want to share our salaries to one another or to anyone,

11   right? We could have brought some trusted party. And

12   each of us would go to that party and tell our salary

13   to that party. That party will then go and calculate

14   the average. They know all of the inputs. Right? And

15   that is the way to do it with the equivalent of private

16   keys. Right?

17   The issue is, what happens if this party is

18   malicious? What happens if this party is compromised,

19   right? Can we collectively calculate the average

20   salary without bringing any trusted third party into

21   the protocol? And the answer is yes. Okay? Very

22   simple example. I will go first.

1   We will do a protocol. I will take my

2   salary. I am not going to tell you what it is. I am

3   going to add some random number that only I know.

4   Okay? I am going to think of that random number. And

5   I am going to add those two together. I am going to

6   send it to you. And you will receive a number that you

7   don't know what my salary was because there is some

8   randomness there. And so you have no way of knowing

9   what was my original salary unless you know my secret.

10 You will add your own salary and will send it to the

11 next person and so on and so on. So each of you will

12 add your own salary. At the end, I am going to receive

13 the sum of all of your salaries from Jim. And I am

14 going to subtract the random number. Only I know that

15 random number. I have the sum. I am going to divide

16 it by the number of people. And we got the average

17 salary. No one in this process has learned anything

18 about each other's salary. And, yet, we were able to

19 calculate the average salary.

20   So this is a very simplistic example, of

21 course, but it was proven back in the '80s that you can

22 take any mathematical function, a sum, a

1 multiplication, or any function whatsoever, and

2 cryptographically do a multi-party calculation in which

3 those secrets remain private to the different parties.

4 Not only that, let's say that some of us were trying to

5 trick people, the other part of the room. It will also

6 be resistant to malicious adversaries who are a part of

7 that process.

8   So another construct is called zero-knowledge

9 proofs. And that is another -- again, in the MPC, it

10 was a protocol, right? Each one of us did some

11 calculation. And we sent some information over the

12 network or to one another. Here we are talking about

13 another set of protocols that the goal in this, in

14 zero-knowledge proofs, is to prove that I know a secret

15 without revealing the secret to the other party. Okay?

16 But I want to prove to the other party that I know that

17 secret.

18   So a very simple example, let's say that I am

19 Bob, and I have two balls. One is green, and one is

20 red. And I have another party, Alice, that wants to

21 prove to me that those balls are different without

22 telling me, without telling me, Bob, which ball is

1   green and which ball is red. Okay?

2   So I have one green ball and one red ball. I

3   am going to put them behind my back. I am going to

4   present one ball. Right? I am going to take it back.

5   And then with a probability of 50 percent, I am going

6   to switch the balls and present the other ball. Right?

7   And Alice will have to say whether or not I changed the

8   balls. Right? So if I do that enough

9   times -- right? -- after a few times, basically I am

10 going to know whether or not I have the same color or

11 not. I am going to be able to prove, Alice is going to

12 be able to prove to me that I have, indeed, different

13 balls without telling me that it was red or a green

14 one.

15   So the third example -- and here we get a bit

16 to kind of sixth grade math, but it is the -- here we

17 show how we can create a public key that does not have

18 a private key. Okay? This is a very simplistic

19 example, but we will try to do that. Right?

20   So what we want to do is we want to create,

21 we want to calculate the public key that corresponds to

22 the sum of two randomly generated numbers by two

 1 people. So here we have Alice and Bob. Each of them

 2 will think of their own secret. Okay? Each of them

 3 has their own secret. Alice has thought of the number

 4 12, but she does not tell that to Bob. And Bob thought

 5 of the number 10. He will not tell that to Alice.

 6 Right? The "private key" will be 22. We will just sum

 7 those numbers. And we will call that the private key,

 8 but we will never calculate that private key. We only

 9 want to calculate the public key. Right? And,

10 basically, the ability to calculate a public key is to

11 take a generator number, in this case the number

12 4 -- right? -- and to take it to the power of the

13 private key.

14   So you are going to have to believe me, but

15 4^{22} is the number 25. Right? But are we able to

16 calculate the number 25 without calculating the number

17 22? And the answer is yes, and it is pretty simple.

18 Alice will take her number and calculate her public

19 address. That will be the number 20. She will send

20 the result to Bob.

21   Bob will take his own public key, will

22 calculate the private -- will take his own private key,

1   the number 10. We will calculate the number 23, which

2   is 4^{10}. And then they will send the results they have

3   to one another. Right?

4   So now after the exchange of the results

5   phase, both of them will have 20 and 23, which is both

6   what they calculated and the result of their

7   counterparty. And the multiplication of 20 and

8   23 -- you have to believe me. It is 25. Because we

9   are operating in cryptography, we always operate under

10 a specific prime modulate, right? So you do 20 times

11 23, and you divide it by 29. And what is left, the

12 modulate is 25. You can try this at home. And,

13 basically, both parties got the same result, which is

14 the number 25. But at no point in time did we have the

15 number 22. If you did, you would have seen red. But

16 there is no red here above the line.

17   And, basically, this is a way to calculate a

18 public address with no private key. The private key is

19 distributed between Alice and Bob. And for advanced

20 students, if Bob is trying to trick Alice, there is

21 actually a way for him to do that. And zero-knowledge

22 proof can come to the rescue for Alice to ask Bob to

1 prove that it was actually a random number that he used

2 in order to choose the number.

3   So what this means is that we are able to

4 make mathematical constructs in a distributed way.

5 Right? So we just saw that we can collaboratively

6 calculate a public key without a private key. And

7 cryptography has gotten to a point in which we can do

8 that also for digital signatures and for the validation

9 and for calculating cash. So calculating cryptographic

10 functions in a distributed way, again, back in the

11 '80s, it was proven that it was feasible. The issue is

12 that in the past years, it had become also feasibly

13 within the timeframe that we would be able to forgive.

14 Right? So it would take about a second to do this but

15 will not take 30 months to do one calculation. Right?

16 So we got to that point in which those protocols are

17 feasible. And we are talking about advances in the

18 recent years in cryptography.

19   So now once we are able to create the

20 identity on the blockchain with several parties, now

21 comes the question of, how do we distribute the secrets

22 between the different parties? So that is kind of a

163

1 business decision. It can be between -- let's say I am

2 an exchange. Remember that I had employees who were

3 able to get into a room to be able to move assets

4 around. Instead, I can give each and every one of

5 those employees a different secret. And together

6 through MPC, each of them, their assets -- their data

7 is not valuable at all. But collectively, they are

8 able to move the assets or if I am a custodian, I can

9 hold part of the secret and give the other part of the

10 secret to my customer, the funds who are my customers

11 or if I am serving consumers, I can have these

12 constructs of distributing the key material between

13 parties in a way that there is no point in time, no

14 point in history in which a private key will exist,

15 either in a hardware wallet or in a software wallet.

16   So, effectively, the solution is that this is

17 very secure, right? There is no single point of

18 failure here. It is connected. All the parties are

19 connected to one another. And you get the ability to

20 be very liquid and very flexible to the business

21 requirements that you need.

22   And one more bonus is that it is agnostic to

1   the blockchain, which is very important. Right? You

2   have many blockchains today, but do you really need a

3   different keyed mechanism for each and every one of

4   them or you can have something that is completely off

5   the chain that can help you resolve the security issues

6   of all the blockchains that you manage? And we see a

7   proliferation. A blockchain is each of them with their

8   own business value, but from a security perspective,

9   this should be kept separate.

10   Thank you.

11   MR. KNOX: Any follow-up questions from the

12   audience at all?

13   CHAIR GORELICK: Let me start with one quick

14   question for Itay. Itay, why is multi-party

15   computation preferable just to a multi-sig wallet?

16   MR. MALINGER: Yes. So the two main reasons

17   would be one is that in multi-sig, you do have two

18   keys. Right? And those keys are constant over time.

19   In multi-party computation, what you can do is you can

20   change those secrets that I mentioned, change those

21   secrets, every time, every hour, every day, every time

22   you make a transaction. So those secrets are not

1 constant constructs. So that is a huge security

2 benefit because, for example, if an adversary gets to

3 one point of the network and they get to the other

4 point after six months, they will actually have no

5 value.

6   The other benefit is what I mentioned last,

7 the blockchain agnosticism of the asset. Right? You

8 have the same infrastructure that can apply to bitcoin,

9 Ethereum, or whatever, instead of having separate

10 support by the various blockchains. And there are

11 blockchains we don't even have multi-sig, right?

12 Specifically, Ethereum does not have a native multi-sig

13 solution. So you can have that also to support non-

14 multi-sig blockchains.

15   CHAIR GORELICK: Okay. Great. Thank you.

16   Mayur?

17   MR. KAPANI: That was a very good

18 presentation. Thank you.

19   One quick question. The actual math for

20 doing MPC or in terms of the logic, are there multiple

21 ways of doing this or is this still evolving or is that

22 a standard way? It is kind of people are converging

1 based on the quality of the math in terms of it being

2 able to be hacked? What do you think is the state of

3 the union?

4   MR. MALINGER: Yes. So there are multiple

5 ways to do this, various protocols trying to optimize

6 on different parameters, just like you have many

7 different signature schemes in

8 cryptography -- right? -- not just issued BSA or a

9 lifted Curv. Some are using other ways. Some are

10 faster than the others. Some are better for many

11 parties versus better for two parties. And this is an

12 evolving space. It got to a point today in which there

13 are I think three to four like main protocols for MPC,

14 specifically for the crypto use case, which is digital

15 signatures, that got it to ballpark in the second

16 today. When you compare it to the time that it takes

17 for bitcoin transactions, this is pretty good. And I

18 assume that this will get better now as we move

19 forward.

20   MR. KAPANI: Thank you.

21   CHAIR GORELICK: Thank you.

22   Haimera?

1   MR. WORKIE: So my question is really more

2   the intersection between what you two discussed. How

3   much does the insurance companies look at the key

4   management systems that are actually being used? Is

5   there like a baseline that is attached to that? Do

6   they give credits if it is more robust or how is that

7   taken into account?

8   MR. KNOX: Sure. Thank you for the question.

9   Are you talking specifically about the security

10 measures regarding the --

11   MR. WORKIE: Yes.

12   MR. KNOX: So, to answer your question, yes,

13 they do take a careful look at that. To give you an

14 idea of just how interested they are in the whole

15 process, we actually had Curv speak with 60 insurance

16 underwriters around the world about 2 months ago to

17 explain the technology to them because they are very

18 aware of multi-sig insuring. They have a clear

19 understanding of that. But they heard rumblings that

20 MPC technology was coming, but they didn't know what it

21 was. So we at Aon actually thought it prudent to put

22 an MPC provider in front of the insurance writers so

1 they got this technology, they understood it because

2 they are going to have to evaluate it.

3   So the response directly to your question is

4 they do take a very deep dive in these security

5 measures.

6   MR. WORKIE: And a question, I guess a follow

7 up question about the difference between the public

8 markets, the public blockchains, and private blockchain

9 systems. Obviously, in addition to the key management

10 systems, there are also issues around kind of the

11 infrastructure of how the blockchain system is set up

12 and how that gets utilized and where there is ability

13 within any given blockchain system to do nefarious

14 things on the system. How is that taken into account

15 in terms of looking at public versus private? And how

16 is that considered?

17   MR. KNOX: Sure. So several factors are

18 going to be evaluated by the insurance underwriters,

19 the insurance companies, the use of that blockchain and

20 what is it being used for when it is public versus

21 private? Who has access to that blockchain? Who is

22 integrated into it? What are the values? If there is

1   a blockchain that is being utilized, what are the

2   values, say, of if there is tokens, some type of assets

3   being dealt with on that blockchain? What are the

4   values of that?

5   So there are several factors they are going

6   to look at, but, most importantly, they are going to

7   look at who is involved with that blockchain, who are

8   the parties involved, what are they doing with it.

9   MR. WORKIE: Thank you.

10   CHAIR GORELICK: Okay. I understand we have

11 a question from Chris Hehmeyer on the phone.

12   MR. HEHMEYER: Hey, everyone. I am sorry I

13 am not there. It is pretty wimpy of Chicago to be

14 canceling flights with two inches of snow this morning,

15 but that is what they did to me. So I am sorry I am

16 not there.

17   Itay, I have a question for you. Given the

18 computational heaviness of an MPC solution, how much

19 capacity is there? Can it provide the liquidity that

20 you talked about? Does it have a lot of capacity or

21 can it get bogged down with a lot of activity?

22   MR. MALINGER: Yes. So the capacity is

1   pretty unlimited. I mentioned that it is ballpark of a

2   few hundred milliseconds per signature, but the

3   advantage is that this is software, right? So you can

4   do as many of those in parallel as you need. And with

5   that, we are just setting it up, even in the cloud,

6   right? You can set up as many of those in parallel.

7   So, effectively, the capacity is pretty unlimited. It

8   is very loosely coupled with the computation that you

9   have. And it is even getting better, and it is any

10 case orders of magnitude better than what you get from

11 the blockchain itself. So it is still like however the

12 blockchain will improve, you can assume that the MPC

13 protocol will improve as well. And they will always be

14 quicker than the blockchain itself.

15   MR. HEHMEYER: Thank you.

16   CHAIR GORELICK: Thank you.

17   Yesha?

18   MS. YADAV: Thank you so much. Terrific

19 presentation.

20   So I have a question I think mainly for James

21 just to try and -- some very basic questions. So I

22 understand insurance to be regulated at the state

1   level. And so in that context, how much input have you

2   had from state regulations in terms of how they see

3   this landscape and how they see their own rulemaking in

4   relation to insurance developing in response to the

5   risks that you are outlining in this presentation?

6   And, second of all, in terms of the insurance

7   companies themselves and the state regulators that

8   might be working on this, do they see the reserve

9   requirements for insurance companies changing given the

10 potential volatility of the underlying assets if you

11 are looking at crypto, bitcoin, the price volatility

12 that attaches to it, the technological fragilities and

13 so on and so forth that you outlined? Are the reserve

14 requirements likely to change, shift upwards,

15 particularly given the lack of data and so on and so

16 forth? And to what extent is that likely to affect the

17 ability for companies to actually want to be in this

18 space?

19   MR. KNOX: Sure.

20   MS. YADAV: And then finally -- I'm so sorry.

21 And, finally, I just wanted to ask, you know, normally

22 when we think about insurance, the insurance companies

1   are able to diversify and then control their exposure

2   because their diversifying met multiple geographies and

3   risks and so on and so forth. Is that diversification

4   potential available in this space or is there some kind

5   of correlated risk exposure that attaches in this

6   market more so than others?

7   MR. KNOX: Okay. Thank you for that. I will

8   start in the order that you posited the questions.

9   Regulators are extremely aware of this space

10 on a state level. Without mentioning names, I can tell

11 you that one of my larger digital asset clients was

12 proactively contacted by New York State regulators

13 after a press release went out about an activity that

14 they were engaged in. So the regulators are very aware

15 of this space on a state level. They are watching it

16 very carefully. They will proactively reach out to

17 companies within their domain and ask them questions if

18 they feel it is proper and follow along that.

19   Second question I think on reserve

20 requirements, that is a really interesting question. I

21 personally do not see the reserve requirements being

22 changed right now by the insurance companies, but I do

1   see them being changed in the following situation. Our

2   sales, Aon, and possibly others are evaluating the

3   possibility of having insurance companies issue

4   insurance policies in denominations of digital assets.

5   In other words, not offering a $10 million policy but

6   offering a $10 million bitcoin or some type of token

7   policy. Right? If that happens, yes, then I do see

8   the requirements for reserves being changed in that

9   situation.

10   And my apologies. Your last question was

11 diversification and?

12   MS. YADAV: (away from microphone)

13   MR. KNOX: Right. Another good question. I

14 think diversification is huge for the insurance

15 companies. And I don't know if diversification is the

16 metric, but, as I said to you earlier on in the

17 presentation, a lot of the insurance companies right

18 now, particularly in the U.S., are evaluating the space

19 very carefully without diving full in and offering

20 insurance products.

21   I think that diversification of a portfolio

22 is always very important. So, obviously, they will

1 diversify but, frankly, right now for the insurance

2 space in the U.S., there is only a handful of insurance

3 companies that will offer insurance products for the

4 digital asset space, the exposures. So yes, they will

5 obviously diversify when needed, but it is not a ton of

6 activity right now from the insurance companies in the

7 U.S. in this space.

8   CHAIR GORELICK: Thank you.

9   Tim?

10   MR. McHENRY: Yes. Thank you.

11   So, given its complexity, how would I as a

12 customer know that the MPC protocol is being properly

13 applied? Is there some sort of a third party

14 authentication that can be done or a cryptographic

15 audit or anything like that?

16   MR. MALINGER: Yes. So the same validation

17 mechanism that applied to any cryptography --

18 cryptographic libraries, specifically because of

19 encryption or digital signatures, right? These are

20 being validated by cryptographic review companies. So

21 there are companies who are, first of all, offering

22 commercial MPC protocols, right? And those vendors,

1 Curv included, are being reviewed by third party

2 validators, both by academic professors and by

3 cryptographers at large. And there is not just a

4 review. You can also do some other kind of attack

5 simulations on those protocols, like band testing, et

6 cetera. All the best practices that you have for

7 encryption, you can apply to MPC and to any

8 cryptographic protocol.

9   CHAIR GORELICK: And Chris?

10   MR. CHATTAWAY: A question for James. Can

11 you give us some perspective on the size of the market,

12 like notional underwritten number of claims that were

13 filed, you know, notion of those claims?

14   MR. KNOX: Sure.

15   MR. CHATTAWAY: Just for some perspective.

16   MR. KNOX: That is a great question. So

17 early on, I showed you some of the headline hacks that

18 happened in this space with the exchanges. To our

19 knowledge -- and there is a lot of those companies that

20 were hacked and some significant losses. Not one of

21 those companies was insured.

22   The interesting thing is in the digital asset

1   space, there has not been a lot of claims yet. There

2   has been some very -- there were some small claims.

3   There has not been heavy losses.

4   The interesting thing is that we have

5   actually had insurance companies, some large insurance

6   companies who were leading the space several years ago.

7   And one day, they decided because the headlines were so

8   bad with some of the severe hacks and losses, they

9   walked away from the space completely without paying

10 one penny of loss.

11   So, to respond to your question, there has

12 not been a lot of significant loss in the insurance

13 space, interestingly. Maybe it is a good job by the

14 insurance underwriters that they did not underwrite

15 those exchanges that were hacked.

16   And I think did you want to know a little bit

17 about capacity in the marketplace?

18   MR. CHATTAWAY: Yes, like are they charging

19 enough premiums, then, to like compensate? Like it

20 feels like there should be some tradeoff or some

21 efficient frontier here where like if there is a great

22 demand for this service, that people are stepping away

1   from it, that other market participants would provide

2   it at some price.

3   MR. KNOX: Sure. So the market is always

4   going to find its --

5   MR. CHATTAWAY: Equilibrium, yes.

6   MR. KNOX: Yes. So the issue becomes -- we

7   will talk about real quickly just the different types

8   of insurance. So you sell cold specie insurance,

9   right? It is low-exposure. You have a bitcoin in your

10 assets offline, right? You can get a lot of insurance

11 for a lot of capacity, pretty reasonable pricing.

12   When you start to go to the other end of the

13 spectrum, we are talking hot wallet

14 coverage -- right? -- the highest exposure for digital

15 assets from an insurer's perspective. There is

16 capacity out there. It is limited, and it is very

17 expensive. So, you know, we have successfully helped

18 clients with their hot wallet coverage. If I was going

19 to evaluate, I would say, right at this time, it is

20 just the price is not good for us right now.

21   MS. TENTE: All right. Thank you. I think

22 we will take a five-minute break now before the next

1 presentation.

2   MR. KNOX: Thank you all very much.

3   (Recess taken.)

4   CHAIR GORELICK: Okay. Good afternoon,

5 everyone. I would now like to turn to the final panel

6 on our agenda, in which we will hear an overview and

7 updates from several entities looking to create useful

8 corporate governance regimes in the digital asset and

9 cryptocurrency marketplace.

10   Our panelists today include Jeff Bandman, who

11 is a board member of Global Digital Finance; Yusuf

12 Hussain, who is the president of Virtual Commodities

13 Association; and Brad Vopni, who is a founding board

14 member of the Association for Digital Asset Markets.

15   And, with that, I will turn it over to the

16 panel.

17   MR. BANDMAN: Good afternoon. Thank you very

18 much for having me. Jeff Bandman, board member,

19 cofounder and lead for regulatory affairs for Global

20 Digital Finance. Thank the Technology Advisory

21 Committee for inviting us and fellow panelists here.

22 Today, as a former CFTC official, it is a particular

1 thrill for me to be here among so many friends and

2 former colleagues. And every day is a good day at the

3 CFTC.

4   (Laughter.)

5   MR. BANDMAN: So I decided to do that. And,

6 really, you know, this panel and all the work has been

7 a real tribute to the CFTC's forward thinking and

8 leadership in digital assets. And, really, a

9 commitment of the resources and energy in this space,

10 you know, does set a global standard for regulation in

11 this area around the world.

12   So I will start by just introducing Global

13 Digital Finance, or GDF, who we are. And in the course

14 of this presentation, I am going to talk about how we

15 came about and then how we are working on setting

16 global standards and self-regulation in this space and

17 what the role of the regulators can be.

18   So we are a global international policy

19 organization headquartered in the U.K., but our

20 membership is global. You know, we think of ourselves

21 in the global landscape as sort of akin to a standard-

22 setting body. We have a global footprint in

1 membership. You know, our focal point, our codes of

2 conduct for crypto asset, which I will describe are

3 internationally community-based. In addition, we do a

4 lot of global regulator and policy-maker outreach and

5 also try to be a resource and, you know, comment on

6 things like consultations and promote those kinds of

7 things. We do work internationally, so regulators,

8 governments, international bodies, foundations,

9 subject-matter experts, as well as the industry itself.

10   So the context for, you know, how did GDF

11 come about -- and, really, the organization was kind of

12 incubated in late 2017. And the work commenced in

13 early 2018. At the time, you know, there was a sense

14 of real urgency around it. I think some of the

15 concerns at that time were well-expressed by letter to

16 the G20 from the finance ministers and central bank

17 governors of France and Germany. You know, there was

18 all of this exuberance. There were a lot of behaviors

19 in the market. And so while there was promise for this

20 new technology, you know, it seemed like there also

21 needed to be kind of a sense of standards. And it

22 would be, you know, you could say, "Well, we don't

1 think what is happening is necessarily right." Well,

2 but in reference to what? And so there really needed

3 to be the industry to show it could come together and

4 do these things. And so some of the things that were

5 articulated at the time, the need for a common

6 understanding on the nature of tokens; the taxonomy; a

7 common vocabulary, which was actually the first project

8 of GDF in 2018; the implications of the exposure of

9 market participants to tokens in terms of market

10 integrity; protection for vulnerable investors; and

11 finally, AML and KYC concerns. So those were a

12 catalyst to us. And so, as a result, we did the work

13 to develop a taxonomy and to start to develop codes of

14 conduct in this area, which is still kind of a core

15 part of our mission.

16   So a bit about kind of who GDF is. And then

17 we will turn our focus to the work. So here is a list

18 of our -- the slide is showing our patron members,

19 advisory council, working members, and partners. You

20 see it is a global group. You see a lot of our

21 guidance and steering comes from the patron board and

22 advisory council, who are global firms. We are a

1 member- and community-driven organization. But also as

2 the kind of list of partners, there shows we partner

3 with different organizations, other not-for-profit

4 governance organizations around the world because we

5 think collaboration is very critical. And these are

6 global markets. And so it is important for people to

7 work together globally as well as locally.

8   Our extended GDF community and those who

9 participate in our summits and drafting of codes

10 include an even broader mosaic of firms. And we also

11 have very extensive engagement with the regulatory

12 community, who participate in our summits as observers,

13 who provide bilateral feedback on our codes of conduct,

14 who we engage with sometimes on deep dives in the

15 various subject-matter areas.

16   So community-led standards. What do we mean

17 by that? And why is that important? So, as I said at

18 the outset, when this work started in late 2017, early

19 2018, you know, we saw the need for a set of rules and

20 standards to be there, but who appointed us? It wasn't

21 as if we came down from Olympus and suddenly had the

22 wisdom to know what was right in this area. It was

1   important to convene the industry as a community and

2   have community-developed standards. And so that was

3   the nature of the work that we did.

4   We found that the regulatory perimeter in

5   2018 and still, frankly, the case today is different in

6   different jurisdictions. Here in the U.S., many

7   digital assets fall under the CFTC or the SEC for

8   different purposes than the IRS or FinCEN for others.

9   But in terms of the market, you know, in the U.K., you

10 might have a single regulator, same in Singapore. In

11 Europe, many digital assets fall outside the oversight

12 of -- they don't qualify as financial instruments or

13 commodities. So we felt this is a global market.

14 There needed to be a set of global standards.

15   So the work, the way the codes of conduct are

16 developed are by working groups. They are done,

17 drafted. And then once they are developed, they are

18 subject to kind of public and notice in comment period,

19 similar to what from my own and other regulators'

20 experienced working at the CFTC. So in 2018, the

21 first, the taxonomy in the first set of codes that we

22 did, we attracted about 650 comments from about 150

1   commenters around the world. Fortunately, somebody

2   other than me had the job of collating those. But the

3   important thing was really to have community-driven

4   things. And then we think that really -- in terms of

5   adherence to those for people who participated in

6   creating them, that is a very important element.

7   So these are -- this slide lists -- on the

8   left, those are the codes that have been ratified. We

9   have a number that are in development. And then we are

10   starting to work on the next ones.

11   Why have we structured it this way? Well,

12   when the work started, you know, we looked around for

13   models of codes of conduct in other industries, whether

14   in peer-to-peer finance. Something that we thought

15   very highly of was the FX code, but the FX code, even

16   after all of the concerns with FX prices, took three

17   years to develop. And we felt, "We don't really have

18   three years. We need to get this work started now."

19   And so we started a modular approach where part 1 was

20   the overarching principles. And then we have added

21   additional modules kind of in a priority order based on

22   what the community and the industry and the regulators

1 tell us are the most urgent topics. And the work has

2 grown. So, for example, our AML group that is done

3 published a number of these and has published.

4   You know, we also have been very engaged with

5 the with the FATF process around the travel rule. And

6 that was about 85 global members. Our custody code of

7 conduct that was just approved at our summit this

8 morning to go to the public consultation phase, again,

9 that group has over 80 participants as well. So there

10 is very broad-based work that goes into those. And all

11 of those are available on our website, a lot of public

12 and transparency.

13   How do GDF codes relate to law and

14 regulation? You know, I think in one sense, they fill

15 gaps. There are many evolving areas. They also try to

16 be a single set of global rules that others can live

17 on. They can serve as models for law and regulation.

18 They can be adapted or they can be worked with by

19 groups. Like my colleagues on the panel, VCA and ADAM,

20 they can be adapted or applied in specific

21 jurisdictions. They don't supersede applicable law,

22 but they are a complement to law. And in many cases,

1   there are regulatory gaps.

2   So now that we have a code of conduct, how is

3   that applied and implemented? So we have a self-

4   attestation registration. People at the CFTC will be

5   familiar with the concept of self-certification. And

6   this is how we started with self-certification. I

7   think over time, there is interest in moving to kind of

8   an external certification or audit process. But today,

9   you know, members or anybody without being a GDF member

10   can signal their adherence, elect to adhere to the

11   code. About half of our members have already publicly

12   attested to that. And others are in the process of

13   reviewing, and we hope doing so. So that is growing.

14   We have started studying kind of a phase 2 of

15   this, which would be external, having a third party

16   audit or verification, but, again, with an interest

17   toward we need to get better standards in the industry,

18   starting with a self-certification model. And then,

19   again, this is a global process, and we will work our

20   way towards external certification.

21   Here these are just some of the contents of

22   the code, just to give an idea of things that we cover,

1   some of the overarching principles, you know, very

2   fundamental topics: ethics; treatment of customers and

3   customer assets; and then as we have gone into the specific

4   code modules, principles for token-trading platforms. You

5   know, a lot of these things might say they are common sense,

6   but we have really gotten into the weeds within the

7   organization, debated those, and submitted those for public

8   comment. So that has been a very rigorous process.

9   And we also have principles for funds and fund

10 managers, token comparisons and rating websites,

11 stablecoins. The stablecoin one, obviously that has

12 become a huge topic internationally with the rise of

13 global stablecoins. That group actually started its

14 work with a stock take. Like they thought it was kind

15 of premature to propose principles. First, they needed

16 to get the lay of the land, which, again, is something

17 that is very common in regulatory things. And,

18 similarly, our custody group that just published

19 something today, you know, they started with a stock

20 take. And we also have a tax working group that is in

21 the midst of a stock take now before it gets to those.

22   Today is actually the second anniversary of

23 when we have had our first meeting. It was our eighth

 1   summit. We had about 200 people around the world in 10

 2   global locations from Bogata to Johannesburg. The Asia

 3   sessions normally meet in person, but, for health

 4   reasons, they met virtually. And so we have been very

 5   excited about that.

 6   The points I would like to kind of wrap up

 7   with are, you know, first of all, you know, the

 8   regulators, like the CFTC and others, how can they be

 9   involved? And then sort of what is the progress to

10   date? And where do we see the challenges ahead?

11   So GDF itself has been very proactive from

12   inception of reaching out and engaging with regulators.

13   You know, at our very first meeting, we had observers

14   from the SEC, the FCA, the Bank of England, Her

15   Majesty's Treasury. And that has grown to include

16   observers from the CFTC, the FSB, you know, regulators

17   around the world. I showed you the other. So we have

18   had that kind of engagement.

19   We also have had a lot of feedback, typically

20   bilaterally, rather than at the meetings, around when

21   they see things in our code. Are there

22   inconsistencies? Have we thought about particular

1 language? It is a lot of kind of issue spotting,

2 things that we may not have thought of ourselves. And

3 so those get kind of integrated into the process of

4 improving the codes before they are finalized. So that

5 is a very important role of the regulators.

6   Progress and challenges ahead. So at the end

7 of last year, we surveyed our membership to get an idea

8 of what their concerns were. Some of the biggest

9 regulatory challenges that they see: inconsistent and

10 unaligned cross-border regulatory guidance, lack of

11 clarity. There is sometimes consistency on the

12 regulatory perimeter.

13   Also, some inconsistencies are caused by the

14 fact that some market actors are regulated, and others

15 are not. And so you can get potentially either a

16 forgiveness-permission dichotomy or personal challenges

17 if some people are playing by one set of rules and

18 others are playing by another. So the fact that where

19 regulators can create a uniform set of rules and a

20 level playing field, that is something that is very

21 important to our members.

22   Also, things like boxing platform

1 interoperability, custodial insurance. It was great to

2 hear the previous panel on that. That is a big

3 priority for the industry. And the readiness of

4 financial institutions and access to banking is an

5 issue internationally.

6   In terms of progress, I think we are very

7 heartened by seeing the development of these codes and

8 people not just getting together in rooms and

9 conference calls and drafting these but putting their

10 hands up and saying, "Yes, we agree to live by these

11 standards." I think that is very important. The fact

12 that we see that there has been broad international

13 consensus on the importance of having these high

14 standards I think is really encouraging to us. And we

15 felt at the time we couldn't wait for regulation to

16 come, that the industry needed to show that it could

17 adopt some of these best practices.

18   We are very encouraged. We think there has

19 been good response to our model, which is very

20 participatory in an industry which has been sort of

21 driven by decentralized technology that we have a kind

22 of distributed model for kind of driving the content

1 and participatory of what the rules are.

2   So, again, thank you very much for having us,

3 certainly happy to answer questions at the end of the

4 session after my colleagues have gone. You know,

5 again, we thank the CFTC for its interest and

6 engagement.

7   MR. HUSSAIN: Thank you. Thank you,

8 commissioners, members of the TAC, for the opportunity

9 to present on the industry's approach to building

10 healthy, safe markets through self-regulations. Thank

11 you.

12   So when regulation is done right, it can pave

13 the way to healthy and sustainable markets, unlock the

14 promise and innovation of crypto for the better.

15 Regulation is the pathway to building trust and broad

16 market adoption. You can't point to a thriving market

17 that isn't either principles-based, rules-based, or

18 governed by some level of regulatory oversight.

19   We recognize the importance of state and

20 Federal-level focus on market integrity and investor

21 protection, but we also do believe that the industry

22 has an important role to play in these self-regulatory

1 efforts within the United States.

2   Today I will discuss the role of industry,

3 examples of paths to self-regulation, coupled with an

4 evolving regulatory landscape, and recommendations for

5 how we get there, including why the VCA is the

6 appropriate vehicle to meet such goals.

7   A little background on the founding members

8 of the Virtual Commodity Association. Gemini Trust

9 Company and bitFlyer are the original founding members

10 of the VCA. Gemini is a regulated New York Trust-

11 licensed crypto exchange and custodian founded in and

12 operating since 2014, the first crypto exchange and

13 custodian to obtain a SOC 2 Type 2 report, providing

14 additional levels of transparency into the security and

15 availability of our infrastructure. Additionally, we

16 recently announced the launch of our captive insurance

17 company to provide additional subject-matter expertise

18 and additional capacity to the somewhat limited

19 capacity available in insurance markets today.

20   bitFlyer is a globally regulated

21 cryptocurrency exchange with operations in Japan, the

22 U.S., and the E.U. They are one of the first

1 recipients of the New York Bitlicense. bitFlyer is not

2 only a founding member of the VCA but also a founding

3 member of the world's first cryptocurrency SRO, the

4 Japan Virtual Currency Exchange Association.

5   A little bit about the VCA. The VCA was

6 established in September 2018 with the ultimate goal of

7 being designated an SRO, a self-regulatory

8 organization. To be very clear here, there is no

9 designation of the VCA as an SRO today. We are looking

10 for paths forward to become an SRO. Being an SRO means

11 a very specific thing. And we will get into that a

12 little bit later in the slides. We don't take this

13 goal lightly. We understand that it is a multi-phased

14 approach that begins with basic organizational capacity

15 building.

16   The launch of the VCA was directly responsive

17 to concerns and public statements made by government

18 officials and regulatory officials by senior officials

19 at the CFTC and the SEC as well as the view of the

20 industry that the industry should take steps to enhance

21 standards, including those around market integrity and

22 transparency.

1   We believe that the CFTC has an important

2   role to play by enhancing investor protection and

3   market integrity within key markets that underpin

4   emerging futures and derivatives-trading activity.

5   Adding a layer of oversight in the form of

6   self-regulation is important for investor protection,

7   as we have seen in traditional securities and

8   derivatives markets and with well-respected and

9   successful SROs, such as FINRA and the NFA.

10   In terms of our structure and organization,

11   you will see a combination of crypto industry subject-

12   matter experts as well as traditional financial

13   industry subject-matter experts. In the past year, a

14   lot of focus on organizational capacity building. In

15   2019, we were able to establish 6 committees focusing

16   on concerns highlighted by government officials and

17   regulatory authorities, including one on BSA/AML; a

18   second one on custody and security; a third on

19   insurance, which was discussed earlier today; fourth on

20   tax; a fifth on market integrity, focusing on

21   information sharing, consolidated audit trails, and

22   cross-market surveillance; and, finally, a committee

1 focused on examination and enforcement, being able to

2 build out an enforcing regulatory framework. We

3 believe the last two committees are of utmost

4 importance. Not to diminish the priorities or the

5 importance of the other committees, but examination and

6 enforcement are capabilities that we are looking to

7 build out that are in alignment with international

8 standards defining what a self-regulatory organization

9 does.

10   As noted, the goal is to establish the VCA as

11 an industry-sponsored self-regulatory organization for

12 the U.S. spot virtual currency industry. I do want to

13 highlight that the road to growing the VCA has not been

14 an easy one. In addition to the natural organizational

15 challenges of a young nascent industry, we found that

16 absent explicit regulatory support or engagement, it

17 can be difficult to drive a voluntary adoption and

18 enforcement.

19   In order to succeed, the VCA will need to

20 bring together a diverse array of market participants

21 subject to an objective governing framework that places

22 the overall health and integrity of our markets before

1   the interests of any particular set of actors.

2   We do believe progress is attainable. As we

3   do so, we look at domestic role models, such as FINRA

4   and the NFA; as well as international examples that can

5   inform our journey.

6   For instance, bitFlyer, as mentioned earlier,

7   is a founding member of the VCA as well as a founding

8   member of the JVCEA, which is the world's first crypto

9   SRO. The notion of self-regulation in Japan was

10 catalyzed by a - - by the hack of a Japanese exchange,

11 Mt. Gox, in 2014. Likeminded exchanges gathered

12 together in a grassroots movement to form the JVCEA.

13   The action was further catalyzed with one of

14 the largest hacks in the history of crypto, Japanese

15 exchange Coincheck, at 500 million, $500 million. That

16 catalyzed the Japanese FSA to designate and formally

17 approve the JVCEA as a crypto SRO in October of 2018.

18   Through Japan's mandate of the JVCEA, the

19 JVCEA has been able to overcome the challenges of

20 voluntary adoption in a young industry and now consists

21 of 27 members, including 19 cryptocurrency exchanges.

22   Currently the JVCEA has formulated 12

1 categories of self-regulatory rules, including, but not

2 limited to, token listings, margin trading, financial

3 management, anti-money laundering, and enforcement.

4   With bitFlyer's membership in VCA and the

5 JVCEA, we have been able to establish synergies not

6 only between likeminded exchanges but also likeminded

7 self-regulatory initiatives across the globe. We

8 believe that collaboration between the VCA and the

9 JVCEA is especially important in an industry that is

10 truly global and operates 24/7. While global SRO

11 examples are certainly informative, we agree with

12 Chairman Tarbert that the U.S. should be a leader in

13 this space.

14   We should look to Japan as a model for self-

15 regulation. However, U.S. regulators should not wait

16 for a hack of a U.S. exchange to prompt delegation of

17 an SRO. In parallel, the VCA continues to build out

18 its capabilities and self-policing measures. Creating

19 a U.S. virtual currency SRO is a two-way street that

20 requires collaboration between government and industry.

21   On the industry side, we continue to focus on

22 capacity building and bridge building. In terms of

1 capacity building, as I mentioned earlier, it means

2 something very specific to be an SRO. A report from

3 IOSCO in 2000 identifies the elements for an effective

4 SRO, which include rulemaking, dispute resolution,

5 surveillance, and enforcement. The IOSCO report also

6 emphasizes that self-regulation is an effective method

7 of regulation as SROs are familiar with the

8 increasingly complex nature of their respective

9 industries. SROs are deemed to have specific knowledge

10 and ability to effectively implement regulatory

11 programs.

12   The NFA is an example of an SRO that has been

13 delegated authority by the CFTC in 1976. Leo Melamed,

14 chairman of the CME, formed a committee comprised of

15 industry leaders to engage Congress on supporting

16 legislation for the creation of the NFA, legislation

17 that gives the CFTC the authority to authorize an SRO

18 when it is in the public's interest and when an SRO can

19 remove impediments to and perfect the mechanisms of

20 free and open futures trading. Six years later, in

21 1982, the creation of the NFA gave the futures industry

22 the regulatory framework on which its markets could

1 continue to grow and succeed.

2   The Commodities Exchange Act and related CFTC

3 regulations set out a number of requirements for an

4 RFA, a registered futures association, like the NFA,

5 requirements which the VCA is also in alignment with.

6   Following on the IOSCO SRO principles, the

7 case study of the NFA; global examples, like the JVCEA;

8 and existing CFTC rules and regulations, it is our goal

9 to build up the VCA to serve a similar crucial self-

10 regulatory function for the spot virtual currency

11 markets in the United States.

12   In terms of bridge building, we must also

13 work across our industry. Just like traditional

14 finance, traditional financial industry, there is no

15 shortage of thought leaders and associations. The same

16 applies within the crypto industry. There are thought

17 leaders and associations that focus on being think

18 tanks, lobbying associations. There are standard-

19 setting bodies like those beside me, Global Digital

20 Finance and ADAM. And then there are those like the

21 VCA that are looking to obtain SRO designation. We are

22 not competitors. We are collaborators in this place,

1 in this space. And we look forward to continuing to

2 collaborate with our industry as peers.

3   Two of the committees that I would like to

4 focus on and highlighted in the IOSCO report as being

5 fundamental to having an effective SRO include

6 examination/enforcement, and market surveillance. The

7 examination/enforcement is a key pillar of an SRO. As

8 in traditional finance, there are best practices and

9 standards set by global standard-setting bodies, like

10 ISO or FATF, that require localization by regulatory

11 authorities. In a similar fashion, more than setting

12 standards, the VCA will continue to collaborate with

13 the various crypto associations for purposes of

14 leveraging and localizing those best practices and

15 standards to inform rulemaking. Those rules will then

16 be adopted, examined, and enforced.

17   As crypto markets are globally distributed

18 with institutional and retail investors having direct

19 access, no longer gated by traditional intermediaries,

20 being able to trade crypto in multiple venues 24/7

21 requires a cross-market surveillance approach, not any

22 one single market surveillance approach.

1   Just as over the years traditional financial

2   markets have become increasingly distributed with

3   multiple venues to trade on, SROs have taken steps to

4   adjust their approach to market surveillance. For

5   example, the conversations that we had earlier today

6   around the FIA's initiatives around consolidating audit

7   trails, additionally FINRA's consolidated audit trail

8   initiatives.

9   VCA members are making progress towards

10 building a technical platform to ingest data feeds from

11 member exchanges for purposes of cross-market

12 surveillance.

13   The creation of an SRO is a two-way street

14 which requires collaboration between government and the

15 industry. Government and regulators play an important

16 role in motivating industry self-regulatory efforts by

17 speaking about them and encouraging such developments.

18 This can catalyze action. The action that we are

19 looking to catalyze is the designation and delegation

20 of authority to an SRO. We have had a number of

21 interactions with the CFTC trying to figure out how we

22 can make this happen. We have engaged our special

1 advisor, Sullivan and Cromwell, to perform an analysis

2 to understand what authority does the CFTC have within

3 current rules, within current regulations, to designate

4 an SRO?

5   Our analysis looks hopeful. We would like to

6 further the analysis with the CFTC. But at initial

7 blush, it looks like the section 17 of the Commodities

8 Exchange Act does indeed provide the CFTC broad

9 authority to designate and register an SRO. According

10 to our analysis, there is no statutory rule-based

11 reason that this authority could not extend to a self-

12 regulatory organization offering its services in the

13 spot virtual currency markets where those virtual

14 currencies are commodities as defined by the

15 Commodities Exchange Act.

16   Given the CFTC's oversight over virtual

17 currency-based futures and derivatives, we do believe

18 that it is in the public's, the market's, and the

19 agency's interest to designate an SRO to surveil and

20 enforce overly and rules-based trading in a market

21 underlined and used for the pricing of the futures

22 traded on CFTC-registered entities.

1   Finally, while we believe this analysis

2   indicates a potential path forward, as mentioned

3   before, we would like to continue our dialogue with the

4   CFTC and key stakeholders to further the analysis.

5   Additionally, we would like to note that state

6   licensing regimes may benefit from a federally

7   authorized SRO, filling in any gaps that may result in

8   state-level and Federal-level regulation.

9   I would like to thank the Commission and the

10   TAC for the opportunity to present on the industry's

11   path to designating and delegating authority to an SRO.

12   Thank you.

13   MR. VOPNI: Thanks, Yusuf. Thank you, Jeff.

14   Thank you to CFTC and the TAC. Thanks so much for

15   having me. I appreciate the opportunity to talk about

16   the ADAM.

17   My name is Brad Vopni. I head up digital

18   asset trading at Hudson River Trading, a global multi-

19   asset proprietary trading firm. And I am here as a

20   representative and a founding board member of the ADAM,

21   which is the Association for Digital Assets Markets.

22   So what is ADAM? ADAM is a private, self-

1   governing, broad-based association of firms seeking to

2   build a safer, stronger, and more efficient digital

3   assets marketplace. The development of digital assets,

4   including cryptocurrencies, digital commodities,

5   digital securities, and the underpinning technologies

6   we believe has a tremendous potential and is rapidly

7   and ever evolving.

8   In the Summer of 2018, a number of firms

9   convened to explore what could be done to significantly

10 reduce issues for both existing and future investors in

11 the digital assets markets in order to give them a

12 higher degree of comfort and security as they looked to

13 transact in this nascent asset class. Most of the

14 individuals in the room were experienced financial

15 services professionals, having worked in the equity

16 commodity and FX markets and exchanges, brokers-dealers

17 were actively involved in some fashion or another in

18 the digital assets markets and had experienced

19 firsthand the idiosyncratic nature of the digital

20 assets markets and were sanguine about the asset class

21 but knew more could be done to build credibility and

22 improve conduct in the markets. Within a few months,

1 ADAM was created, formally launching as a nonprofit on

2 October 24th, 2018.

3   Membership in ADAM is open to organizations

4 involved in or that seek to become involved in the

5 markets for digital assets, including trading venues or

6 exchanges or marketplaces, custodians, investors, asset

7 managers, traders, lenders, liquidity providers, and

8 brokers.

9   ADAM has a relatively simple mission: to

10 foster fair and orderly digital assets markets, where

11 participants can transact with confidence, certainly

12 easier said than done, but when determining what ADAM

13 should do, we established four guiding principles,

14 which are, one, provide clear standards for efficient

15 trading, customer, clearing, and settlement of digital

16 assets; two, encourage professionalism and ethical

17 conduct by market participants; three, increase

18 transparency and provide information to the public

19 about digital assets markets; and, four, seek to

20 protect market participants from fraud and

21 manipulation.

22   Now, equally as important in establishing

1   what ADAM was intended to do, we were also very mindful

2   of what ADAM isn't. ADAM is not intended to be an

3   advocacy group. ADAM is not intended to be a

4   replacement for regulation. Simply put, ADAM exists to

5   enable industry to pave the way toward fair and orderly

6   markets by complementing existing laws and regulation,

7   basically to bridge the gap between the status quo and

8   future regulation of the digital assets marketplace.

9   So, historically, as some of us have

10 mentioned before, market-driven efforts to establish

11 industry standards led to effective self-regulation,

12 both in securities and the commodities markets.

13 Subsequently, through authority granted by Congress,

14 FINRA, previously NASD/NASDAQ, was established as the

15 SRO to oversee our securities markets. And NFA was

16 established as the SRO to oversee our commodities

17 markets.

18   The ADAM membership is composed of industry

19 experts who have combined hundreds of years experience

20 and expertise in the traditional equities and

21 commodities and various other markets and who are now

22 active participants in the digital assets markets in

1   both the United States and abroad.

2   There are 10 founding members of ADAM. And

3   they represent a large market share across key areas

4   within digital assets markets. Those members are

5   BitOoda, BTIG, Cumberland, Galaxy Digital, Genesis

6   Global Trading, GSR, Hudson River Trading, Paxos,

7   Symbiont, and XBTO. All of these firms committed to

8   two years of participation in ADAM and all have

9   representation on the board.

10   And while we were fortunate enough to attract

11 a distinguished list of firms at the start, the group

12 was thoughtful regarding the types of market

13 participants that ADAM should involve. What that means

14 in practice meant understanding how firms arrived at

15 the roles that they played within the markets, mostly

16 due to how the digital assets markets has evolved.

17   So while many service providers in other

18 asset classes exist entirely independent of one

19 another, we have to appreciate that many firms in the

20 digital assets markets, especially marketplaces, often

21 perform the function of numerous other firms in other

22 asset classes. Marketplaces themselves can often

1 operate as the exchange, the clearinghouse, the

2 custodian, the broker, and sometimes even the dealer.

3 And while we believe that over the long-term, industry

4 will ultimately dictate how some of those services

5 should be offered, either within the four walls of

6 those organizations or potentially segregated like they

7 are in other assert classes, ADAM understood that it

8 needed to find the appropriate balance between

9 appreciating how things actually operate with an eye

10 towards how they might in the future. Striking that

11 balance helped drive our mission and ultimately our

12 purpose.

13   So what have we done? In collaboration with

14 industry and legal experts as well as academics, ADAM

15 has developed a code of conduct that will set standards

16 for professional conduct and efficient industry self-

17 governance for digital asset markets. And I will go to

18 the code in a little bit, but our goal is that through

19 the introduction of and adherence to the code of

20 conduct, others in the marketplace will be ADAM members

21 as trusted players and create best practices and

22 establish higher industry standards.

1   We formally announced the code and our new

2 members at the consensus event in November of last

3 year. We hosted a launch party the evening prior to

4 consensus and had over 50 high-quality firms, who came

5 to learn more about ADAM. Two of our founding members

6 participated in a panel at consensus to discuss the

7 mission of ADAM and went into what the code is intended

8 and not intended to do and ultimately published a draft

9 of the code itself.

10   Membership has also been a key focus for us.

11 And even while managing to be somewhat low-key and pen

12 to paper as we drafted the code, we managed to increase

13 our membership by 50 percent, adding a number of well-

14 regarded firms who share the same vision around

15 establishing best practices and creating higher

16 industry standards.

17   So alongside the announcement of the code was

18 the announcement of the few new members who had chosen

19 to join ADAM. Those members are BitGo, Anchorage,

20 BlockFi, CMT Digital, and Tagomi.

21   So before getting into any specifics

22 regarding the code, it is important to appreciate what

 1 we believe this milestone ultimately meant. One, it

 2 signals that members are committed to professional

 3 standards of conduct, standards that institutional

 4 investors are familiar with from other markets and

 5 would require if they are to enter these markets in any

 6 meaningful way. Two, they help improve the standards

 7 of conduct in the industry. Where regulatory gaps are

 8 general and uncertainty exists, this can ultimately act

 9 as a backstop by setting minimum reasonable standards

10 of conduct; and, three, provides an opportunity for

11 industry to step up and provide leadership in defining

12 what those best practices should be.

13   So, as indicated, the code of conduct is

14 really designed to promote integrity, fairness, and

15 efficiency. Intended to inform and complement, rather

16 than replace existing regulation, the code is drafted

17 to inform participants on best practices and is part of

18 a long-term effort to define and promote ethical

19 behavior and conduct by all digital asset markets'

20 participants.

21   The code is really divided into a number of

22 principles, which guide and define appropriate

1 professional standards in the following areas:

2 governance, compliance, risk management, market ethics,

3 conflicts of interest, transparency and fairness,

4 market integrity, custody, information security and

5 business continuity, and anti-money laundering, and

6 countering the finance of terrorism.

7   Complying with the letter and spirit of the

8 code should be well within the reach of firms who

9 understand basic standards of professional conduct and

10 have a commitment to sound governance and risk

11 management.

12   That said, we do believe that there is

13 tremendous value in coming together as an industry to

14 commit to these standards. And because it is

15 principles-based, the code is intended to be flexible

16 enough to address issues that will inevitably arise

17 given the nascent technology and asset class. And we

18 expect these best practices to evolve over time and be

19 reflected in the code.

20   ADAM's code is to provide industry-

21 led, -developed, and -maintained best practices and

22 standards to the digital asset space so it is better

 1 able to grow and attract new participants, who expect

 2 and demand some form of clear regulation, whether

 3 industry- or government-led, and should ultimately

 4 raise the level of professional conduct in digital

 5 assets markets.

 6   Looking forward, what does 2020 and beyond

 7 hold for ADAM? First, at the end of next month,

 8 members will be signing the code. Those are the 10

 9 founding members and the 5 new members. Second, ADAM

10 is going to continue to focus on growth. We have

11 embarked on an executive director search and are

12 looking to bring a seasoned, sharp, respected

13 individual to help us lead the next phase of ADAM. We

14 continue to recruit new members, being ever mindful of

15 reputation, credibility, function, and geography. ADAM

16 is not exclusively a U.S.-focused organization. But

17 given how historically U.S.-based institutional firms

18 have often been the tip of the product in asset class

19 sphere, we appreciate that if we can assist in making

20 institutional-grade participants in the U.S. feel as

21 though they are dealing with professionals, then it

22 will be useful in other jurisdictions. And the

1 borderless nature of digital assets is ultimately one

2 of its most exciting and intimidating features

3   Governance. We will expand our board of

4 advisors. We have been very fortunate enough to have

5 worked in a variety of capacities with a number of

6 academic, legal, and industry experts and will be

7 looking to create an advisory board to aid our

8 executive director and the board of directors in its

9 further push to legitimize the markets.

10   And finally, generally looking to leverage

11 the ADAM platform to raise awareness among digital

12 assets market participants and engagement, ADAM can be

13 a resource to market participants, to regulators, and

14 other stakeholders. We are early on in the stages of

15 exploring how we might do that, but some early ideas

16 include submitting comment letters on regulatory and

17 policy initiatives, engaging with regulators on matters

18 beyond the code of conduct, being a source of

19 information about industry trends and practices, and

20 possibly expanding the role of ADAM in defining what

21 industry best practices should be, perhaps issuing

22 model policies or FAQs or case studies to clarify how

1 the code should be applied in various situations. All

2 of this is quite speculative at this point but

3 identifies a few areas that we are exploring

4 internally.

5   So we are incredibly proud of where ADAM has

6 arrived. And the code is an incredibly meaningful

7 milestone in what we anticipate to be a long road ahead

8 to give investors the same confidence in dealing with

9 digital assets that our other, more established markets

10 afford. And while we are very mindful that ADAM

11 doesn't have all of the answers today, what it does

12 have is an ever-growing list of high-quality firms in

13 the digital assets markets that share a common vision

14 of an industry-led initiative to continue to promote

15 fairness, decency, and ethical behavior doing the hard

16 work to build credibility, helping sort out the rules

17 of the road, and improving the conduct in the digital

18 asset markets.

19   That being said, I am happy to answer any

20 questions. And thank you for your time.

21   CHAIR GORELICK: Thank you to the panelists.

22   So I will start with Charlie.

1   MR. COOPER: Thank you. Thank you for all of

2   the presentations. And, Brad, I am cognizant of the

3   fact that you don't have all of the answers. I am

4   still going to ask questions.

5   I am actually thinking that what might help

6   up front is a bit of a definitional question. And the

7   reason I say that is, Yusuf, in your presentation, you

8   talked about cryptocurrencies. Jeff, in yours, you

9   talked about crypto and digital assets. And, Brad, you

10   talked about digital assets potentially more broadly.

11   The reason I think that matters is if we are talking

12   about the idea of a self-regulatory organization that

13   looks at cryptocurrencies, that is one conversation.

14   And it is interesting because we could make the

15   argument there is nothing currently overseeing them,

16   and we wouldn't make the argument there is nothing

17   overseeing them. But, Brad, if you are talking about

18   broader digital markets that can refer to digital

19   shares of stock or digital bonds or digital futures,

20   that is a different SRO because we could also make the

21   argument then that all of those assets, the underlying,

22   are already regulated. They already have SROs. So we

1 don't need this.

2   So I guess, what are we talking about here or

3 are all three of you actually talking about different

4 things?

5   MR. HUSSAIN: I will make a quick start. The

6 usage of the term "virtual currency" was intentionally

7 used just to use the same terminology and parlance

8 familiar with the CFTC in the commodities space. The

9 VCA is looking at specifically U.S.-based spot

10 cryptocurrency market self-regulation.

11   MR. BANDMAN: Yes. Thanks for the question,

12 Charlie. And, also, I was remiss in not recognizing R3

13 and DTCC as GDF members. And thanks for your

14 engagement and support.

15   So you are very right to make that

16 distinction. So I would say that GDF, our initial

17 focus was crypto assets. And we used that term

18 starting in 2018 because that was the term that the FSB

19 and a lot of the regulators were using. You know, we

20 know FATF calls them virtual assets. I think Chairman

21 Tarbert calls them digital assets. So there is a lot

22 of terminology there.

1   So our initial focus and where we thought the

2   most urgency in developing the code of conduct was for

3   crypto assets. And that was our initial focus.

4   The name of the organization is Global

5   Digital Finance. And I would say aspirationally over

6   time, you know, if we can play a role in helping to

7   support truly global digital finance, I think that is

8   in our roadmap but not what we are most urgently

9   working on.

10   I think one of the new working groups that

11   our members want to start is one on sustainable finance

12   and how that ties into digital finance. So I think

13   that will maybe be the first step in that direction.

14   And we maybe also be starting a group around digital

15   identity, but, you know, our initial work has been

16   focused on crypto assets. And that is where we got

17   started.

18   MR. VOPNI: And for the lawyers in the room,

19   I will read exactly sort of what we indicated in the

20   code. But I think it is a fair question because you

21   are absolutely right in that a number of digitized

22   securities or other digital assets already have

1 governance and rules around those. And so when we

2 spent a lot of time thinking about what a digital asset

3 is -- and, again, this is sort of why the -- it is a

4 principles-based code and why we sort of anticipate it

5 to be a living, breathing document is that, you know,

6 we at ADAM believe that currently a digital asset is a

7 cryptographically derived digital instrument available

8 in a public, private, or commissioned blockchain or

9 other form of distributed ledger. There are some other

10 words, too.

11   And then sort of from an asset class

12 perspective, any option futures contract swap or other

13 instrument or index, the value of which is derived,

14 wholly or principally, from the value of the underlying

15 insurance meeting the description in clause 1. So it

16 is specifically designed as a wrapper for what we

17 believe the definition of cryptocurrency would be if

18 that answers your question.

19   MR. COOPER: Thank you.

20   CHAIR GORELICK: Tom?

21   MR. CHIPPAS: Thank you. Thank all three of

22 you. No doubt it has been quite a bit of work. And it

1   is very obvious from the presentations the

2   thoughtfulness that you have all put into it. And I

3   appreciate that. And I am sure everyone here does as

4   well.

5   Charlie asked my first question. So thank

6   you, Charlie. Appreciate that. So, with that

7   stipulated already, I guess I would ask just a broad

8   initial question. Then I may have a follow-up or two.

9   Today, we have digital commodities, bitcoin, for

10 example, that trade. And, historically, we have

11 commodities like gold that trade. And we have

12 derivatives on these things as well, too.

13   Can you give me an example of a spot

14 commodity SRO that perhaps you have looked at for

15 inspiration or has governed any sort of spot commodity

16 trading, at least in the United States, that you can

17 think of?

18   MR. BANDMAN: Yes. So, I mean, SRO, I think,

19 you know, in terms of something that has legal

20 authority, delegated, statutory legal delegated

21 authority, you know, I think that my colleagues already

22 made the observation that I think in the U.S., that

1   there is not, to our knowledge, a specific example of

2   that. But there is obviously the Japanese one.

3   One of the models that we looked to was the

4   FX code of conduct. So there may not be an FX SRO, but

5   the introduction of a code of conduct and then people

6   who adhere to that is an important step in promoting

7   market integrity and higher standards.

8   MR. HUSSAIN: To be clear, we are not

9   advocating for a non-crypto spot commodity SRO. There

10   isn't one that exists that I am aware of. However,

11   crypto is a unique asset class that has similarities to

12   other asset classes, like derivatives, like futures.

13   Additionally, we are looking to be responsive to the

14   CFTC and other regulators and government officials'

15   concerns around market manipulation, especially as the

16   futures and derivatives product continues to grow for

17   cryptocurrencies. It would be important to ensure that

18   the underlying, the underpinning markets are also

19   appropriately surveilled.

20   So it is a unique asset class. There aren't

21   any non-crypto commodity SROs that I am aware of. But

22   there are similarities and there are differences.

1   MR. VOPNI: Tom, the answer to your first

2   question is no, I am not aware of any. I think when

3   I -- ADAM was very mindful. I know the title of the

4   panel involves the letters SRO, but we were very

5   mindful in sort of using that term as sort of a guiding

6   light for how we think about things, but we also sort

7   of recognize that an SRO status is generally earned.

8   We are not entirely sure exactly who would be decreeing

9   necessarily an SRO title amongst or upon whatever body

10   that may be in the future. So I think from ADAM's

11   point of view, we wanted to be a rather broad-based

12   sort of self-governing organization looking at items

13   like the global FX code, many of us having gone through

14   sort of the equities markets in the late '80s, early

15   '90s, and sort of what became of NASD and then FINRA

16   and others and using those as sort of guideposts for us

17   as we think about, you know, how this market is going

18   to evolve over the next 5, 10, 20 years.

19   MR. CHIPPAS: So, with that stated, what I

20   just posit as a general question is, is crypto really

21   that different? So if a token is just called a token

22   when it is actually a security, then in the United

1 States, I think we know who should regulate that and

2 where it should go. If it is a spot commodity, then we

3 have the Commodity Exchange Act and we have decades of

4 history of how spot commodity markets have worked and

5 how derivative markets have worked.

6   And, certainly, you know, speaking selfishly

7 for a moment, ErisX operates a DCM and a DCO.

8 Everything listed, for example, in the VCA presentation

9 with the exception maybe of the information sharing,

10 our responsibilities that we have as a DCM operator, we

11 already have the authority and obligation to do many of

12 these things.

13   So I guess I would just ask, how

14 fundamentally different is crypto as a commodity than

15 other things today? It is a tiny, tiny commodity

16 market in comparison to many, many others. And FX I

17 think, Jeff, is a great example, where if there are

18 specific things that need to be addressed, they could

19 be addressed maybe with something less invasive,

20 expensive, and time-consuming than a completely new set

21 of obligations, some of which already exist in the

22 derivative markets. And the CFTC already has the

1 authority to get involved in underlying spot commodity

2 markets under various conditions.

3   So has there been any real analysis away from

4 headlines and not planned to review only of headlines?

5 How different is it? I know there would be some unique

6 aspects, but ultimately if it is spot commodity under

7 derivative, how different is it?

8   MR. HUSSAIN: Sure. Non-crypto spot

9 commodities physically distributed, typically

10 wholesale, that is a broad statement, typically

11 wholesale. Ease of access is different compared to

12 crypto, to the spot market crypto, the spot crypto

13 currency market, there is access by retail investors,

14 institutional investors that are no longer gated by

15 intermediaries and completely agree that for the

16 futures and derivatives market, there already are

17 existing self-regulatory initiatives and efforts,

18 regulations and rules around the futures and

19 derivatives market. What we are trying to do is fill

20 in a gap for the crypto spot currency markets in the

21 U.S.

22   MR. BANDMAN: Just to add to that, so I think

1 some of the differences are, you know, these markets

2 are global, right? The instruments are frictionless or

3 may be frictionless, digital. They may be

4 characterized by the sort of instantaneous settlement.

5 And I think there are other assets that have those

6 attributes. But I think also, taking an international

7 global perspective, which has been our outlook on this,

8 you know, the regulatory treatment of these things is

9 different in different jurisdictions. And our outlook

10 has been that there were a lot of gaps in regulation.

11 And particularly for people who are participating in

12 this market, either locally or internationally, we

13 thought there needed to be some sort of reference point

14 for what the behaviors should be.

15   I take your point very much that where there

16 is already an existing supervisory framework, you know,

17 like there is already excellent supervision of

18 derivatives markets in the U.S. and securities markets

19 in the U.S. So we don't need to reinvent the wheel,

20 but there are also kind of gaps. Looking at it

21 internationally, there are a lot of places. And

22 regulation is still catching with sort of the

1 definition of is a commodity -- can it be a tangible

2 interest? In some jurisdictions, it can't. That may

3 evolve with these things.

4   You know, you sort of kind of brought up the

5 point about cost-benefit analysis. For us, that is one

6 reason for starting out with kind of a self-

7 certification model that is kind of wider and probably

8 less expensive for participants than kind of the

9 supervisory model. So that is another observation I

10 would make.

11   MR. VOPNI: Tom, what I might also add is

12 that I think your fundamental question is actually sort

13 of why ADAM exists. And while I don't think for many

14 of the digital assets that we are referencing there is

15 a fundamental difference, I think that the issue that

16 there is uncertainty still means that in absence of

17 clear definition of what those are, who sort of

18 ultimately is responsible for surveilling, regulating

19 those assets, that participants need to come together

20 to try to create a rules of the road that make sense

21 until that time and place, where it is much clearer for

22 all participants.

1   MR. CHIPPAS: My final comment would be I

2   keep going back to gold as a great reference. I heard

3   anecdotally that eBay is the second largest spot gold

4   market in the world. That is fully retail,

5   unregulated, consumer-driven. So I will just continue

6   to point out that I think we have a lot of analogous

7   commodities we can look at today that, as much as I

8   love crypto and all things that go with it, I am

9   obviously dedicating my time and career to it,

10   sometimes we might be better served thinking that there

11   is a lot more in common than different. And finding

12   simpler solutions would be the only comment I make.

13   Again, congratulations to all of you. There

14   is a lot of hard work and foundation building you are

15   all doing, and I appreciate the effort.

16   CHAIR GORELICK: Thank you.

17   Commissioner Berkovitz?

18   COMMISSIONER BERKOVITZ: Thank you.

19   Just, Yusuf, when you talk about an SRO, are

20   you contemplating like the SROs that we have, the CME,

21   ICE, NFA, that there would actually be not only just

22   surveillance but enforcement authority, that persons

1 who trade on the member exchanges would sign basically

2 membership agreements where they would consent to the

3 jurisdiction of the platform? And that would include

4 potentially enforcement actions, which could include

5 civil monetary penalties.

6   And then, secondarily, if the answer is to

7 that yes, is that something that Jeff and Brad in your

8 codes of conduct, that a number of these entities

9 believe an SRO should do because otherwise if just a

10 couple of them say, "Okay. We are really going to have

11 an effective SRO based on the futures of securities

12 models," where there is actually surveillance plus

13 enforcement authority but you are the only ones that do

14 it, there are others that don't, market participants

15 will gravitate towards the lesser regulatory or the

16 lesser potentially burdensome "Why am I going to

17 subject myself to penalties on this exchange if I don't

18 have to have them on another exchange?"

19   So if you could just -- what type of actual

20 membership agreements do you contemplate? And would

21 this include potential enforcement authority? And

22 then, more globally, is this something that you are

1 striving to have a baseline for everybody to sign up

2 and agree to?

3   MR. HUSSAIN: What you defined and what you

4 just went through is the definition of an SRO per the

5 IOSCO report, per what a registered futures

6 association's responsibilities are. That is the

7 intent. That is what we are looking to build towards.

8 That is what the response to the calls to action by the

9 regulators and government officials is intended to do.

10   Once again, for the U.S. cryptocurrency spot

11 markets, we do agree that it is not a level playing

12 field right now. So it doesn't make sense to live in a

13 world where there are certain venues that are not

14 regulated in a similar fashion. So as other

15 jurisdictions further formalize their self-regulatory

16 organizations, as Japan did, as others continue to do,

17 we would want to ensure that there are appropriate

18 synergies between these different self-regulatory

19 authorities.

20   And, once again, we are not looking to

21 replace any sort of existing regulatory authority.

22 What we are looking to do is serve as an extension in

1 this specific case, an extension to the CFTC to provide

2 sensible, thoughtful regulation to the cryptocurrency

3 markets.

4   MR. BANDMAN: The other part of the question,

5 you know, you sort of asked, well, if there is this

6 SRO, will people move towards the less regulated part

7 or the more regulated part? I mean, part of that is

8 dependent on, you know, is the scope of its authority,

9 is sort of compliance with that voluntary or not?

10   I think that in terms of adoption in this

11 area, retail but also institutional adoption, people do

12 trust well-regulated markets. I think if -- like I

13 hadn't heard until we were discussing before the panel

14 that there was a theory that the CFTC might be able to

15 authorize the VCA in this context for the spot market.

16 But if it did and if it had that authority, you know, I

17 think a lot of the market would actually -- you know,

18 maybe not everybody -- there might be actors who didn't

19 wish that for cost or principle or other reasons, but,

20 you know, I think that a lot of market participants and

21 especially those who have yet to adopt in this area

22 would be encouraged by the fact because -- right -- and

1   if they were an SRO, not only would they be acting

2   under delegated authority, but the CFTC would be

3   supervising them. Right?

4   I think in other jurisdictions, I think

5   having a voluntary code of conduct that fills in gaps

6   and regulation, there would still be a lot of demand

7   for that because in the absence of clear legal

8   authority or regulation, then self-regulation and

9   having codes and principles is the best alternative

10 available.

11   MR. VOPNI: I think that Jeff summed that

12 rather well. Maybe just to add to that, I think that

13 it is not perfectly clear to me how it would work if a

14 single entity -- right? -- was sort of operating as an

15 SRO and what that meant given sort of the -- not even

16 sort of decentralized but just the global nature of

17 digital assets. And so yes, is it voluntary or is it

18 required to be sort of a meaningful outcome or

19 determinant for participants in the space?

20   You know, speaking specifically about ADAM,

21 we -- our members need to sort of self-certify and

22 comply with the code, both initially in a month and

1 then also on a yearly basis. We are sort of putting

2 governance around what it would like to develop a

3 formal process to identify and evaluate instances of

4 noncompliance and determine appropriate disciplinary

5 acts them. That is challenging to do in a self-

6 governing organization, let alone enforcement and what

7 that would look like for a self-regulatory

8 organization.

9   So we are going to focus on that for ADAM in

10 the near term and let others sort of worry and opine

11 and think about what that would look like for an SRO.

12   CHAIR GORELICK: Thank you.

13   We have time for one more question, and I

14 think we will go to John.

15   MR. LOTHIAN: I am a winner. Thank you.

16   My question, you alluded to it a little bit

17 earlier. My question has to do with structure a little

18 bit because if you look at the SROs that we have, they

19 are mostly organizations that are full of

20 intermediaries. And the cash crypto market is one that

21 has a lot of direct retail members, as opposed to an

22 intermediary, a broker, prime dealer, you know, or

1   prime broker, whatever, kind of a thing. What is the

2   role of this organization relative to the retail crowd?

3   MR. HUSSAIN: So the approach for the VCA has

4   been working with the markets, the exchanges, where

5   institutional and retail investors can operate, execute

6   trades on directly, with or without an intermediary.

7   We believe that these rules and regulations move closer

8   to the core, the core being the marketplace. That way,

9   we capture not only those individuals and institutional

10 investigators that proxy trades through intermediaries

11 but also those that are directly accessing the

12 exchange, which is the case for the retail investors.

13   MR. BANDMAN: So in our case, kind of retail

14 investors would typically be the ones who might be

15 protected by the code or might elect to do business

16 with those who have signified that they are adopting by

17 these principles. The way our organizational structure

18 works also, the retail participants can also

19 participate in the composition and drafting of the

20 codes or comment on them as well. At this time, we

21 don't have a specific retail governance methodology.

22   MR. VOPNI: Two comments. One, I would say

1 that ADAM is intentionally broad-based, specifically

2 because of the sort of nuanced nature of the digital

3 asset landscape, sort of again, you know, alluding to a

4 number of marketplaces wearing numerous hats that would

5 be generally decoupled in other asset classes.

6   And so we are -- and I guess the second point

7 is part of the principles are or one of the governing

8 elements of the principles or of the code is that it is

9 sort of based on, your adherence to the code is based

10 on your size, is based on your role, and is sort of

11 appropriate for an organization depending on what hat

12 or hats you wear. So the way sort of a principal

13 trading firm that generally operates on a proprietary

14 basis that doesn't have clients or counterparties or

15 deal with people on a bilateral basis, you know, their

16 adherence to the code may be more concentrated and less

17 onerous than somebody who runs a number of businesses

18 and what they would have to do to self-certify and

19 identify conflicts of interest and other elements.

20   So, you know, I think that is one of the

21 reasons or sort of one of the primary reasons that ADAM

22 is broad-based is because there are a lot of

1 participants that perform a number of functions within

2 the space.

3   And I think the second comment is that we

4 sort of look at this in sort of a rising tide, sort of

5 floats all boats. And this is one of these asset

6 classes. And I don't have a lot of context for -- or

7 we can't come up with context for another where retail

8 has been the tip of the spear for adoption. And so in

9 order for institutions and institutional-grade

10 participants to sort of come in, they are going to

11 require clarity, reasonable practices, best practices,

12 and things that don't necessarily exist or are

13 uncertain for them. And those will sort of be just the

14 general table setting for them to feel more

15 comfortable, sort of regardless of the regulatory

16 structure of it.

17   CHAIR GORELICK: Thank you to our panelists.

18   So I think at this point as the last matter

19 for the day, the TAC is going to vote on a

20 recommendation from the Cybersecurity Subcommittee.

21 The recommendation was emailed around to the Technology

22 Advisory Committee last week. And there are also

1 copies of the memo in everyone's folder for today.

2   This is also a recommendation that has been

3 well-signaled by the subcommittee. This was first

4 presented two meetings ago. It was re-presented at the

5 last meeting. And today is the day, finally, that they

6 are asking for a vote to approve these recommendations.

7   So the Cybersecurity Subcommittee is

8 recommending that the full Technology Advisory

9 Committee make a recommendation to the CFTC that it

10 join with other noted organizations in making a

11 statement of support for the FSSCC cyber profile

12 similar to the following, and I will quote, "Regulatory

13 harmonization regarding cybersecurity requirements is a

14 worthy objective saving resources for both regulators,

15 such as the CFTC and financial institutions, by

16 allowing increased focus on the most important risks

17 and necessary investments to mitigate those risks.

18   "The FSSCC cybersecurity profile is a

19 customization of the NIST cybersecurity framework that

20 financial institutions can use for internal or external

21 cyber risk management assessment and regulatory

22 organizations can use as a catalog of best practices

1   and requirements to support both informed and efficient

2   risk-based compliance-related examinations and the

3   development of future cyber regulation."

4   As I mentioned, TAC members were provided

5   with the materials for the vote in advance of today's

6   meeting. In addition, the Cybersecurity Subcommittee

7   presented on the background to these recommendations at

8   the last two TAC meetings.

9   Before I open the vote, I would like to open

10 the floor for a discussion on the recommendation from

11 the Cybersecurity Subcommittee.

12   MR. McHENRY: Thank you, Mr. Chairman.

13   As you said, for the last two meetings, we

14 presented information on the cybersecurity profile,

15 which was developed through a coordinated effort with

16 the Financial Services Sector Coordinating Council.

17 This was done in response to an industry-wide need for

18 consolidated and reconciled catalog view of various

19 cybersecurity regulatory standards. So since its

20 release, the profile has garnered broad support among a

21 variety of financial sector participants, industry

22 associations, and agencies. The Cybersecurity

1   Subcommittee believes that this is because the profile

2   summary framework can provide great utility and

3   efficiency to firms as well as the regulators that

4   oversee them.

5   So as the profile continues to attract

6   significant attention, it would obviously benefit a

7   great deal from support from the CFTC, as outlined in

8   your materials. Therefore, the Cybersecurity

9   Subcommittee recommends that the TAC move forward with

10 its own recommendation that the CFTC make a statement

11 in support of the cybersecurity profile, as suggested

12 in the materials.

13   CHAIR GORELICK: Thank you.

14   Is there anyone else who would like to make a

15 statement or ask any questions at this time?

16   (No response.)

17   CHAIR GORELICK: Okay. With that, I will now

18 move that the Technology Advisory Committee adopt the

19 recommendation from the Cybersecurity Subcommittee on

20 making a recommendation to the CFTC that it join with

21 other noted organizations in making a statement of

22 support for the FSSCC cyber profile. Is there a second

1 for that motion?

2   MR. LOTHIAN: Second.

3   CHAIR GORELICK: Okay. I am happy to

4 entertain the motion as well. Is there a motion?

5   MR. LOTHIAN: I so move.

6   CHAIR GORELICK: So moved. Is there a

7 second?

8   MR. TABB: (Indicating.)

9   CHAIR GORELICK: Okay. We have a couple of

10 seconds here. Okay. With that, I will now call for

11 the vote on the motion. All of those in favor of

12 approving the subcommittee recommendation, please say

13 aye.

14   (Chorus of ayes.)

15   CHAIR GORELICK: All those opposed, please

16 say nay.

17   (No response.)

18   CHAIR GORELICK: Are there any abstentions?

19   (No response.)

20   CHAIR GORELICK: Okay. The motion carries.

21 Congratulations to the subcommittee.

22   And, with that, I think we can turn it over

1 to the commissioners for closing remarks. Thank you

2 very much.

3   COMMISSIONER QUINTENZ: Well, thank you,

4 everybody, for joining us today. I know it takes a lot

5 of time to participate in these in an effort to travel

6 and to be with us and to think about engaging

7 productively. I was very pleased. I hope you all felt

8 the presentations we heard were informative,

9 enlightening, and represented a great deal of

10 leadership in some transformative areas of finance that

11 we will all be dealing with I think going forward in

12 the future.

13   So let me thank all of our panelists. Let me

14 thank all of you, our full members. Let me thank all

15 of the subcommittee members that aren't represented on

16 the full panel for their participation. And, as

17 always, thank you, Richard, and thank you, Meghan, for

18 going above and beyond, especially the last couple of

19 weeks with all of the other work that has been going

20 on. So thank you.

21   COMMISSIONER BEHNAM: I will just echo

22 Commissioner Quintenz's comments. Thanks to the

1 committee, a huge effort I think leading up to today, a

2 lot of great questions, a lot of great panels, which I

3 think raised a lot of questions for me from a legal

4 perspective and authority perspective in sort of how we

5 should move forward on these really important issues.

6 And a special thanks or Richard and Meghan, of course,

7 for your work and look forward to seeing all of you

8 again soon. Thanks.

9   COMMISSIONER BERKOVITZ: I would also like to

10 thank everybody and thank the committee and thank my

11 colleagues here, Commissioner Quintenz and Meghan and

12 Richard.

13   Today's meeting of the Technology Advisory

14 Committee shows why we need a technology advisory

15 committee. Really, technology is integral from

16 everything, the ISDA program to basically put into code

17 the ISDA agreements, which will have tremendous

18 benefits for market participants and for the CFTC, to

19 the presentation on multi-party confirmations, to the

20 presentation on stablecoins and the banking system

21 really shows the extent to which our markets, really

22 dominated by technology and a whole host of issues that

1 we really benefit by all of the expertise of the

2 presenters and you around the table bringing to this

3 agency. And we really need meetings like this and a

4 committee like this to help us stay informed on these

5 issues and so we can formulate appropriate regulatory

6 responses and intelligently consider your well-thought-

7 out recommendations. So I thank everybody for coming

8 to Washington and participating in the meeting. Thank

9 you.

10   MS. TENTE: All right. Thank you, everybody.

11 The meeting is now adjourned.

12   (Whereupon, at 3:43 p.m., the meeting was

13 adjourned.)

14

15

16

17

18

19

20

21

22