EXHIBIT B

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

----------X

SECURITIES AND EXCHANGE COMMISSION,

Plaintiff,

against

Civil Action No. 20-cv-1 (AT)(SN)

RIPPLE LABS, INC., BRADLEY GARLINGHOUSE and CHRISTIAN A. LARSEN,

Defendants.

----------X

** HIGHLY CONFIDENTIAL **

VIDEOTAPED DEPOSITION OF [redacted] Ph.D.

New York, New York

Friday, December 17, 2021

Reported by

JEFFREY BENZ, CRR, RMR

JOB NO. 203725

December 17, 2021

8:21 a.m.

Videotaped Deposition of [redacted] Ph.D., held at the offices of the U.S. Securities and Exchange Commission, 200 Vesey Street, New York, New York, before Jeffrey Benz, a Certified Realtime Reporter, Registered Merit Reporter and Notary Public of the State of New York.

A P P E A R A N C E S:

U.S. SECURITIES AND EXCHANGE COMMISSION
Attorneys for Plaintiff
200 Vesey Street
New York, New York 10281
BY: MARK SYLVESTER, ESQ.
JON DANIELS, ESQ.
LADAN STEWART, ESQ. (Remotely)
DAPHNA WAXMAN, ESQ.

A P P E A R A N C E S: (Ctd.)

DEBEVOISE & PLIMPTON LLP
Attorneys for Defendant Ripple Labs, Inc.
919 Third Avenue
New York, New York 10022
LISA ZORNBERG, ESQ.
ASHLEY HAHN, ESQ. (Remotely)
BENJAMIN LEB, ESQ. (Remotely)
SCOTT CARAVELLO, ESQ. (Remotely)
CHRISTOPHER FORD, ESQ.

-and-

KELLOGG, HANSEN, TODD, FIGEL & FREDERICK
1615 M Street, N.W.
Washington, D.C. 20036
BY: COLLIN WHITE, ESQ.

A P P E A R A N C E S: (Ctd.)

PAUL, WEISS, RIFKIND, WHARTON & GARRISON LLP
Attorneys for Defendant Christian Larsen
1285 Avenue of the Americas
New York, New York 10019
BY: CARLY LAGROTTERIA, ESQ.
MEREDITH DEARBORN, ESQ. (Remotely)

CLEARY GOTTLIEB STEEN & HAMILTON LLP
Attorneys for Defendant Bradley Garlinghouse
One Liberty Plaza
New York, New York 10006
BY: SAMUEL LEVANDER, ESQ.

ALSO PRESENT:
CHRISTOPHER JOHNSON, Videographer
DAVID SCHWARTZ, Ripple Labs, Inc. (Remotely)
DEBORAH McCRIMMON, Ripple Labs, Inc. (Remotely)
STELLA UVAYDOVA, S.E.C. (Remotely)
KYLE E. CHERMAK, Debevoise & Plimpton (Remotely)

[redacted] - Highly Confidential

THE VIDEOGRAPHER: We are now on the record. This is the start of media labeled number 1 of the video-recorded deposition of [redacted] in the matter of Securities and Exchange Commission versus Ripple Labs, Incorporated, et al., in the United States District Court for the Southern District of New York. Civil Action Number 20-CV-10832 (AT)(SN).

This deposition is being held at U.S. SEC, 200 Vesey Street, Suite 400, New York, New York. Today is Friday, December 17, 2021. And the time on the video monitor is approximately 8:21 a.m. My name is Chris Johnson. I am the legal video specialist from TSG Reporting, Incorporated, headquartered -- excuse me.

The court reporter today is Jeff Benz, in association with TSG Reporting.

Will all counsel present please introduce yourself and the parties you represent.

MS. ZORNBERG: Good morning. I'm Lisa Zornberg from Debevoise & Plimpton together

with Chris Ford, who is also in the room. We represent Defendant Ripple Labs, Inc., in this case.

I would also just let you know that we have through Webex participating today two employees of Ripple: David Schwartz, who is the chief technology officer, and Deborah McCrimmon, who is the vice president for litigation.

THE WITNESS: Good morning.

MR. SYLVESTER: I'm Mark Sylvester. I am an attorney for the plaintiff, the Securities and Exchange Commission. I'm here with my colleagues Jon Daniels and Daphna Waxman.

MR. LEVANDER: Samuel Levander of Cleary Gottlieb, on behalf of the defendant Brad Garlinghouse.

MS. LAGROTTERIA: Carly Lagrotteria. I'm from Paul, Weiss.

THE VIDEOGRAPHER: Will the court reporter please swear in the witness and then we may proceed.

[redacted] - Highly Confidential

[redacted] Ph.D.,

called as a witness, having been first duly sworn by Jeffrey Benz, a Notary Public within and for the State of New York, was examined and testified as follows:

EXAMINATION BY MS. ZORNBERG:

Q. Good morning.

A. Good morning.

Q. Dr. [redacted] for purposes of today's deposition, I'm going to refer to Defendant Ripple Labs as Ripple. Okay?

A. Very good, yes.

Q. Yes? Okay. Are you taking any medication or suffering from any medical or physical condition, that would prevent you from testifying truthfully and completely today?

A. No.

Q. Okay. Please state your full name for the record.

A. [redacted]

Q. Where do you live?

A. I live in [redacted].

Q. How old are you?

[redacted] - Highly Confidential

A. 44.

Q. Have you ever been deposed before?

A. No.

Q. Okay. You understand that your testimony is under oath. Correct?

A. Yes.

Q. And it's being taken down by the stenographer and by the videographer in this lawsuit. You understand that --

A. Yes.

Q. -- correct?

A. Yes. I do.

MR. SYLVESTER: Just let her finish the question before you answer.

THE WITNESS: Okay.

MS. ZORNBERG: Just a couple of ground rules. Because the court reporter is taking down all of the testimony, it's important that you verbalize all answers. So a nod of the head is not sufficient. You have to be verbal.

Another ground rule that your counsel just pointed out -- or not -- counsel for the SEC just pointed out, please let me

finish my questions before you start to give an answer so that we get a clean record and we're not talking over one another.

Sound good?

A. Yes.

Q. Okay.

We'll take regular breaks. If you need a break at any point, just let me know and we'll be accommodating.

The only thing I may ask is that you answer a pending question before we take a break.

Okay?

A. Yes.

Q. Okay. Is English your first language?

A. No.

Q. What is your first language?

A. [redacted].

Q. Are you fluent in English?

A. I consider myself fluent in English, yes.

Q. Do you write papers in English?

A. I do.

[redacted] - Highly Confidential

Q. Have you taught classes in English?

A. Yes, I did.

Q. Okay. If for whatever reason you don't understand a question, that I've asked, please let me know you don't understand the question. I'll be happy to repeat it or rephrase it.

Have you ever lived in the United States, Dr. [redacted]

A. [redacted]

Q. Have you ever given testimony under oath in any type case?

A. I did in [redacted].

Q. What type of case?

A. [redacted]

[redacted] - Highly Confidential

Q. [redacted]

[redacted]

Q. I'm sorry for that experience.

Have you ever served as an expert witness in any type of case before?

A. You mean the court case, such as this one, the legal proceeding?

Q. Yes, in a legal proceeding.

A. No, I did not. No.

Q. Okay. So this case is the first time that you're serving as an expert in any type of legal case.

A. Yes, it is.

Q. When was your first contact with the SEC about this case?

A. My first contact with the SEC in this case was in the summer, so June this year.

Q. Your first contact from the SEC was June 2021?

A. 2021. June 2021.

Q. How did that contact come about? I'm not asking you to tell me your conversations with SEC lawyers, but how did -- without revealing those conversations, how did the

[redacted] - Highly Confidential

contact come about?

A. [redacted] people from [redacted] reached out to me, so they found me. I think it was a cold email first. Would I be interested in -- I think the email said, I believe, I -- the email said the -- the -- like, they would like me to be an expert on some -- on some court case related to the blockchain.

Then I had a discussion with [redacted] with maybe one hour, initial, where they didn't reveal which case this was.

And, after that, I had a call with SEC, which was also -- so we were all talking early June. I could not give you exact dates, but we are talking early June.

Q. When was -- when was the cold email from [redacted] that initial email from [redacted]

A. Let's say it was, again, early June or very late May, I would put more probability -- I don't know. I cannot vouch for it. My take is very early June. We're talking 1st to 4th of June maybe. I'm not sure.

Q. Was that your first contact with [redacted]

[redacted] - Highly Confidential

A. Yes.

Q. What is [redacted]

A. I believe it's -- so it's a litigation firm that, to my understanding, helps SEC with certain case.

Q. Is your engagement in this case the first time you've ever interacted with [redacted]

A. Yes, it is.

Q. Who at [redacted] did you speak with prior to your engagement in this case?

A. I spoke to [redacted]. I'm not sure I pronounce his name correct. I spoke to [redacted] and [redacted]. I believe that is it.

Q. Can you give the last name one more time?

A. [redacted].

Q. [redacted]?

A. Yes.

Q. Okay. Thank you.

A. [redacted] and [redacted], I think, is the last name.

Q. Can you describe your communications with [redacted] about this case.

[redacted] - Highly Confidential

A. [redacted] reached out to me. And, again, if I recall correctly, to the best of my recollection, he was trying to understand if I would like to be an expert in a certain litigation in a court case. Since it related to blockchain, I'm interested. But I'm not necessarily interested in just picking up anything, so -- you know.

Then he suggested that -- he asked me few questions about, how would you -- how would you think about going classifying certain blockchain system as decentralized and centralized? So we discussed that topic.

And I told him, basically, what's my approach, how I think about it. So we talked about it real time, so I didn't -- he was asking questions; I was giving him answers.

And, yeah. I guess this was the reason they carried on with me.

Q. That was -- that was your initial one-hour call, was with [redacted]

A. There might be [redacted] on that call and [redacted] but, yeah. So the first -- I -- I distinctly remember communicating -- like

[redacted] - Highly Confidential

discussing this decentralization/centralization with [redacted].

Q. How did you discuss the issue with decentralization with [redacted] In other words, was it a phone call, a video conference, an email, some other messaging communications?

A. It was a video call or Webex, I believe.

Q. And did you email with him as well about the subject of decentralization?

A. I don't recall I did.

Q. Is it possible you did?

A. I doubt. It might be possible since I don't recall for sure. So let's leave it to possibility, I doubt.

Q. Have you communicated with [redacted] by any means other than -- in writing, by any means other than email?

A. In writing an email or sending an email? No?

THE COURT REPORTER: I'm sorry. Say that again, please.

A. I'm just repeating the question. Sorry. So -- have you communicated in writing?

[redacted] - Highly Confidential

I'm repeating the question.

Q. Yes.

A. In any other means other than email?

No. Could I be missing something? Like -- we didn't text. We didn't write letters, so no.

Q. Okay. So -- did [redacted] tell you what he was looking for?

MR. SYLVESTER: Objection.

Q. You can answer.

A. I can answer. Okay.

No. No.

Q. Other than this case, have you worked with the SEC in any capacity?

A. No.

Q. Prior to -- do you have a written retention agreement in this matter with the SEC?

A. I have a written agreement with [redacted] And with SEC, I -- I signed some documents which are nondisclosure documents and -- and certain documents. I think, for example, things like my rate and these things, they are all signed with [redacted]

Q. Okay. Do you know --

[redacted] - Highly Confidential

A. I don't know if this answers your question.

Q. Do you know the date of your retention agreement with [redacted]

A. It was -- it must be, again, in June. I don't know the date.

Q. Okay. Prior to your engagement in this case, had you heard of Ripple Labs, Inc.?

A. I did. Yes.

Q. How?

A. I followed the blockchain space since 2009, so basically since the inception of bitcoin. And Ripple was definitely prominent blockchain network, which on top of that was trying to put in work, consensus protocols that are different than those used by bitcoin, which I happened to be researching since 2003. So again, much before -- like considerably before bitcoin was accepted -- incepted.

So I did research on these protocols in my Ph.D. thesis. Since I did it and Ripple was essentially trying to come up with a similar, let's say the protocol which falls into -- into this category, then it obviously

[redacted] - Highly Confidential

drew my attention.

And then I was paying attention to the protocol discussing at that time with my colleague and collaborator, [redacted].

And then we discussed, like, look at this protocol; this is similar to what we did. But it doesn't seem that -- you know, there seems to be something not correct with this protocol. And then we actually started looking into that.

And then I understood that Ripple -- I think at some point Ripple was in the name of the network. Before it was called XRP Ledger, there were different names. And Ripple was in the name of the network. And then the name of the Ripple was associated to this organization, this -- this protocol, as --

Q. So when -- approximately when did you start talking to your collaborator, [redacted], about the protocol for the XRP Ledger?

A. We started intensively -- we might have mentioned it before the date I will give you, but we started looking -- actually, he

[redacted] - Highly Confidential

started looking into more details, and I was following on the high level -- I can explain in more technical details what's the high level -- in 2015.

Q. Okay. So --

A. I heard about -- sorry. Just to the complement the answer, I heard about Ripple even before, as you're -- as I'm following the --

Q. Yeah.

A. Yeah.

Q. So let me just clarify. You heard about Ripple prior to 2015, correct?

A. Yes.

Q. The person you've described as your collaborator, [redacted], started looking at the protocol for the XRP Ledger, around 2015?

A. So 2015 I moved back to [redacted], as you can see in my CV. Right? So this is the moment when I was collaborating with [redacted] nonstop. So I was collaborating with [redacted] since 2008 to 2010 when I was in [redacted]. And then I went to [redacted] to be assistant professor. But we continued collaboration. So we might have mentioned it before, but, intensively, we

[redacted] - Highly Confidential

started looking into it in 2015.

Q. You just said that you and [redacted] intensively started looking at the XRP Ledger protocol in 2015.

A. Uh-huh.

Q. But a few minutes ago, you said that [redacted] started looking at it first, and you were following his work at a high level.

Can you clarify?

A. Yes. It's the first thing. So when I say "we," I mean as a team, because we looked -- but he was leading the analysis of the -- let's say within the team, he was leading the analysis of the XRP Ledger.

I was following it on a high level. I can explain. For -- yeah. If you wish.

Q. What does it mean that you and [redacted] were the team?

A. We co-authored many scientific papers together. We would discuss protocol -- when we designed a new protocol, we would discuss protocol details together, each and every one of us trying to find, you know, shortcomings in others' work. And this is what, you know, the

[redacted] - Highly Confidential

whole scientific community is doing. We're just at a faster pace of iteration, talking to each other.

We're exchanging ideas, collaborating on -- on building protocols, collaborating on analysis of the protocols and so on.

Q. Okay.

And so just to make sure I understand your testimony, [redacted] started looking into the details of the XRP Ledger protocol in 2015?

A. To my understanding, yes. He might have started earlier. But at least in 2015.

Q. Was that as part of his work at [redacted] or as a separate interest of his?

MR. SYLVESTER: Objection.

Q. You can answer.

A. Uh-huh. As part of -- so we had -- we had very much freedom in what we choose to work for [redacted]. It was never -- as researchers of the standing that we were just, just like how -- how [redacted] approached blockchain. They let us suggest what are we going to work on.

So, yes, it was part of [redacted]. But it came -- you can say that it came bottom

[redacted] - Highly Confidential

up, grassroots, during -- because of his interest, because he thought it is relevant.

Q. So can you please describe what work you personally have done, or did, relating to the XRP Ledger protocol, while at [redacted].

A. So I looked at the -- the -- the original white paper. And basically, original white paper, which is co-authored by David Schwartz, had reasoned about the quorums, which are the sizes of the faulty nodes, Byzantine faulty nodes that are tolerated by the protocol. And these were rather nonstandard.

Since the protocol was underspecified, I didn't dive much into the details. But it seemed that this is not a correct protocol, so it's not doing what it promises to do. So I was reading and I was gathering this understanding.

Q. So let me pause you there.

A. Yes.

Q. In what year was this?

A. This is year 2015.

Q. Okay. Can you just state again, what -- what was it that you, based on reading the white paper by David Schwartz, did you think

was not correct?

A. It was not correct that it can basically tolerate -- it can provide a guarantee that it does.

Q. Which guarantees did you felt, based on reading the white paper, the XRP Ledger protocol could not provide?

A. It -- that it couldn't provide safety and liveness because of the way quorums are sized, essentially, in the protocol.

Q. What does it mean for a quorum to be sized?

A. Because of its assumption in the number of quorums and the assumption of the number of correct nodes, the number of faulty nodes. So that defines the quorums. So the adversarial assumption is how many -- which percentage of nodes can be Byzantine or not. So basically the -- how the protocol was constructed, it was intuitive, according to my prior experience of designing this protocol, that something is wrong here.

Q. Did you write any papers between 2015 and 2020 relating to your evaluation of the

[redacted] - Highly Confidential

XRP Ledger protocol?

A. So we write -- so [redacted] we wrote one paper, which is called [redacted] where, basically, the things with Ripple protocols were mentioned. So --

Q. Other than that paper you've mentioned, [redacted] --

A. Yes.

Q. -- did you write -- in which you -- you said that the XRP Ledger protocol is mentioned in there. Correct?

A. Yes.

Q. Did you -- did that paper, [redacted] express or contain analysis of safety and liveness concerns that you're talking about here today?

A. I believe -- I believe we mentioned it. But it was not analyzed in the details, for example, at the level I'm giving in the -- in my expert report.

Q. Other than the paper [redacted] have you written any papers to date addressing the XRP Ledger protocol?

[redacted] - Highly Confidential

A. No, I did not.

Q. So the answer is, no?

A. No.

Q. Within [redacted], did you prepare any written analysis, during the time that you were at [redacted], on the XRP Ledger protocol?

A. No, I did not.

Q. Do you know anyone who works for Ripple?

A. You mean like personally?

Q. Yes.

A. I do not, no.

Q. Have you ever met Chris Larsen?

A. No, I did not.

Q. Have you ever met Jed McCaleb?

A. No, I did not.

Q. Have you met David Schwartz?

A. No, I did not.

Q. Have you ever communicated with David Schwartz in any way?

A. No, I did not.

Q. Back in 2015 when you've described that you started looking at the XRP Ledge

protocol, did you ever consider reaching out to David Schwartz to discuss your concerns about the protocol?

A. No, I did not.

Q. Why not?

A. You know, we were focusing -- it's in our interest to look at other protocols. At that time we were trying to build -- we were busy building our own systems. And it's not my job to help others, necessarily. I didn't have a -- you know, even this -- the attack was not specific or anything. And it's not my job to reach out to people and help them out.

Q. What do you mean -- just said the attack was not specific or anything.

A. So --

Q. What do you mean by that?

A. Yeah. So, for example, the attack that I'm describing in my report, I didn't have that level of understanding of Ripple protocol that I gained later on, where I actually took to analyze it in details, took the task of analyzing it in details.

Q. When was it that you analyzed the

[redacted] - Highly Confidential

protocol at the level of detail that you're describing is contained in your report?

A. After I -- after I was retained by [redacted] and I started working for SEC, so we're talking after June this year.

Q. Would it be fair to say that the concerns that you noted in 2015 about the XRP Ledger protocol were at a high level?

MR. SYLVESTER: Objection.

Q. You can answer.

A. We can say that, yes.

Q. And it was not until after -- sometime in or after June 2021 that you looked at those issues in detail. Correct?

A. Yes.

Q. Have you ever met Brad Garlinghouse?

A. No.

Q. Have you ever spoken to anyone at Ripple, to your knowledge?

A. No.

Q. Did you read any of the deposition transcripts taken in this case?

A. I did.

Q. Which ones?

A. David Schwartz.

Q. How many transcripts of David Schwartz's testimony did you read?

A. I'm not sure I get the question. How many?

Q. Do you know if there's one or more than one deposition or -- let me rephrase. Do you know if there's one or more than one transcript of David Schwartz giving testimony related to this case?

A. To my understanding, there is one.

Q. Okay. So you read one transcript?

A. One.

Q. Did you read the entire transcript?

A. I did.

Q. All right. Do you recall the date of the transcript that you read?

A. The transcript. I think it was in May. Don't hold my -- you know. I think it was May, May this year.

Q. Dr. [redacted] do you know anyone from the Ethereum Foundation?

A. No.

So let me put it this way: I never

met physically anyone.

So, no, if this is like your definition of "no," no, we never met physically or something.

Q. Have you ever -- have you ever met in any way, physically or through other means of communication, Vitalik Buterin?

A. No, I did not.

Q. Have you ever met in any way Gavin Wood?

A. No, I did not.

Q. Do you know who he is?

A. I know.

Q. Who is he?

A. He's the -- one of the original founders of Ethereum.

Q. Okay.

A. And currently, he is mostly involved in the Polkadot project, so he's putting his attention there.

Q. What is the relationship between Ethereum Foundation and Ether, if you know?

A. I would need more details to answer this question. So Ether -- yeah, I would need

more details to answer this question. So normally Ether is the token which is the native token of Ethereum network. And Ethereum Foundation is linked to the development of Ethereum network, so that's it.

Q. Do you know what Ethereum Foundation does?

A. To my understanding, it funds the development of the Ethereum network. It might be doing other things that I'm not aware.

Q. Do you know what the Ethereum Foundation's ecosystem support program is?

A. I do not.

Q. Does the existence of a foundation that's dedicated to supporting the Ethereum network mean that Ethereum is a centralized system?

MR. SYLVESTER: Objection.

Q. You can answer.

A. No, it does not. So it's -- I give definitions in my report. I give precise definitions, about the basic or minimal condition for a system to be considered decentralized. I can repeat it for you if you

wish.

And the existence of Ethereum Foundation is related to governance aspect that I discussed my report. It should be looked at as such, through this lens.

Q. Is it your view that simply the existence of a foundation that is dedicated to supporting development on a particular blockchain network, does that automatically mean that network is centralized?

A. It does not. So I could imagine several -- so imaginary networks, several people who are interested in development of a blockchain network, they come up with their own foundations. So you could have ten foundations for one blockchain network.

And, yeah, we call it centralized because these foundations exist, so normally these -- these would be people who distribute their wealth, let's say, in those tokens, to fund the development of the network.

Q. That does not render the network centralized.

MR. SYLVESTER: Objection.

[redacted] - Highly Confidential

A. So that -- that meaning what? Can you repeat? "That does not render" -- so "that" is what?

Q. I'm just trying to clarify my own understanding of what you're saying. Does the mere existence of one or more foundations, dedicated to supporting a blockchain network, mean that network is centralized?

A. You got my brain racked. So does the -- I'm repeating the question. Does the existence of several foundations mean that the blockchain network is centralized?

I guess the answer is no.

So. Yeah.

Q. In the case of Ethereum, besides the Ethereum Foundation, are you aware of other foundations that -- that exist in order to support Ethereum?

MR. SYLVESTER: Objection.

A. To support Ethereum development, to support --

Q. Yes.

A. To support --

I'm not aware of any.

Q. Okay. Do you know anyone from ConsenSys?

A. No, I do not.

Q. Have you ever met Joe Lubin?

A. No.

Q. Do you know what ConsenSys does?

A. ConsenSys, to my understanding, it takes the Ethereum public blockchain network and tries to adopt it in a way that it can be used in so-called permission blockchain networks, in blockchain for businesses, as we call it in [redacted]

And I know about the existence of ConsenSys because they were, like, competitors to [redacted] once we worked in [redacted] the permission blockchain space, because they were trying to build their technology on the Ethereum stack. That's what I know about ConsenSys.

Q. Okay. Do you know anyone from the Bitcoin Foundation.

A. No.

Q. Have you ever met Gavin Andresen?

A. "Andresen."

No.

Q. Andresen.

Have you ever met someone named Craig Wraight?

A. No, I did not.

Q. Do you believe that he invented bitcoin?

A. No, I do not.

Q. Why not?

A. There is a simple proof. If you invented bitcoin and you claim you did it, there is an, arguably, high probability that you mined as an early player in the bitcoin network one the first bitcoin blocks.

So if you want to prove, it's very easy. So you could use the cryptographic keys that are associated with that block to sign basically any message. So you give the Craig Wraight challenge: Sign me this message. And if he does it, you can verify that this was signed with the keys that belonged to one of the first blocks.

That's a very simple test. And he never was able to produce such a test -- to basically produce such a signature.

Q. Do you know what services the Bitcoin

Foundation provides to bitcoin?

MR. SYLVESTER: Objection.

A. I do not.

Q. Do you know anyone from the XRP Ledger Foundation?

A. No, I do not.

Q. Do you know anyone who runs an XRP Ledger validator?

A. No. Well, I know institutions that were reported in my report that's run XRP Ledger validators.

As for persons, if they're private persons, if you ask me that, or somebody maintaining this node, I don't know these people personally.

Q. Outside of the information on validators included in your report, do you know anyone who runs an XRP Ledger validator?

A. No.

Q. Do you know Peter Adriaens?

A. No, I do not.

Q. Have you ever heard him speak?

A. No.

Q. Have you read any of his reports in

this case?

A. I did.

Q. What reports of Peter Adriaens have you read?

A. I read the rebuttal to my report. And I read his original report.

Q. What other expert reports, if any, in this litigation, have you read?

A. I read [redacted] rebuttal on agent's report. We can classify it as expert's report, right?

Q. Yes.

A. And that would be it.

Q. You say you read [redacted] rebuttal report?

A. Yes.

Q. Are there any U.S. universities that you have worked closely with, Dr. [redacted]

A. If you define "closely" for me, closely.

Q. Well, what -- what U.S. universities have you worked with in any substantive way?

A. Let's put it this way, so -- did I ever co-author a paper with somebody. That's an

interesting question, actually.

So I know many researchers -- let me put it this way. I know many researchers from conferences from different U.S. universities, including Cornell, UT Austin, Brown University, et cetera.

Did me -- did I ever -- this is an interesting question. Did I ever co-author, for example, a paper? I don't know, I would need to check.

Q. Fine.

Have you ever heard of MIT's Digital Currency Initiative?

A. I think I heard.

Q. Okay. Have you ever interacted with MIT's Digital Currency Initiative?

A. No, I didn't.

Q. Have you had any interactions with Neha Narula?

A. No. I think we were attending maybe a few workshops or conferences, so I know the name. I believe she might know mine, but we never -- I don't think we even talked. No.

Q. Do you know whether Ms. Narula has a

good reputation in the scientific community?

MR. SYLVESTER: Objection.

A. You need to define "a good reputation."

Q. Do you -- do you know -- do you know anything about her reputation in the scientific community?

You know, is she -- is she well regarded? If you know?

A. I don't know.

Q. Okay.

Have you ever met or spoken with Gary Gensler?

A. No, I did not.

Q. Dr. [redacted] do you know what this lawsuit is about?

A. I could state it in my words, and then you tell me if I know or don't know. Can I --

Q. Go ahead.

A. So, what I believe is that SEC is complaining that -- maybe the answer is I don't know. But since I started talking, then I should just finish. But --

MR. SYLVESTER: Only say what you

[redacted] - Highly Confidential

know.

THE WITNESS: Yes, so what I know.

A. So the SE-- the Ripple and the defendants were selling certain products, including, perhaps, the XRP token, as unregistered securities.

Q. Do you know what, if any, allegations the SEC has made in this case relating to decentralization?

A. I don't -- I don't know.

Q. Okay.

A. No.

Q. Have you read any of the court filings in this case?

A. I read the complaint.

Q. Okay. When did you review the complaint?

A. Very early in the process, so we would be talking again June this year.

Q. Why is that not listed in your report as materials that you considered in the case?

A. It didn't influence my expert opinion.

Q. Do you understand that you were required in this case to identify all materials

[redacted] - Highly Confidential

that you considered, whether or not you ultimately relied on them?

A. What does it mean to consider? If I just read them?

Q. Yes.

MR. SYLVESTER: Objection.

A. I was -- so I was -- if this is correct, what you're saying, I was not aware of this. And what I listed is what impacted my expert opinion --

Q. So you --

A. -- which this complaint did not.

Q. I'm sorry, did you finish your answer?

A. Which this complaint did not. Yes.

Q. So your report only listed materials that you relied on, not that you considered?

MR. SYLVESTER: Objection. Misstates his testimony.

A. Again, can you please define "considered" for me.

Q. Well, I would -- I would -- that is actually a term -- that's a term that is required of all experts. The rule says to -- you have to identify materials you considered.

[redacted] - Highly Confidential

For purposes of today, I'll ask it this way. Are there materials that you read, and thought about, and looked through, in -- during your work on this case, that you did not cite in your report?

A. There are many scientific papers that -- for example, that I didn't cite in my report. Because, for certain concepts, they are very well accepted. So there would be hundreds of papers that refer to this concept, and I didn't make each and every -- for example, if I talk about resilience of distributed and decentralized algorithms, I know literally hundreds of papers, which, you know, they were in my head as someone with 18 years' experience on this topic. Which you can call I considered. Which are not referenced there.

But this is like, you know.

Q. Yeah.

A. Can I reference all the papers that -- on the topic that I know about?

Would it be useful?

Q. Well, your report ultimately lists 22 references.

[redacted] - Highly Confidential

How many scientific papers beyond the 22 did you look at during the timeframe from June 2021 through the -- you know, through October 4, 2021, when you -- when you issued your report in this case?

MR. SYLVESTER: Objection. Limited only to his preparation of the report. Correct?

You asked how many papers he looked at in that timeframe. I just want to limit the question to preparing the report.

MS. ZORNBERG: That's fine.

A. So, it depends again on the definition of "consideration." So, if I'm writing my report, I'm relying on 18 years of experience.

So, even if I didn't read the paper in the timeframe you're referring to, I might be considering it because it's part of my understanding of the topic. So that's where the definition of "considering" versus "read" is unclear to me.

How many papers? So there were more papers that I read than those that I cite. But I give -- so, yeah. So there -- there are more

[redacted] - Highly Confidential

papers. How many more, I cannot say precisely.

Q. So you read more papers in your work on this case than just the ones you cite in your report --

MR. SYLVESTER: Objection.

Q. -- correct?

A. So I -- in the timeframe between -- that you're referring to, I read more papers that relate to this topic that -- you know, than what I cite in my report. Yes.

Q. Outside of attorneys with the SEC, with whom have you discussed your work on this case?

A. With no one. I think my contract allows me to mention the case to my wife, which I did.

No one else.

Q. Well, you talked about it with [redacted] [redacted] correct?

A. Sorry. Can you -- okay, can you repeat the question --

Q. Yeah. Other than SEC --

A. -- because I didn't --

Q. Other than SEC attorneys, I asked --

[redacted] - Highly Confidential

A. Other than SEC attorneys, yes.

Q. -- who -- with whom did you discuss your work on this case.

A. Okay. Very good.

Q. You said your wife.

A. Very good, very good. So with the [redacted] -- with the members of the [redacted]

Q. Did you discuss your work on this case with anyone at [redacted]?

A. No, I did not.

Q. Did you discuss your work on this case with [redacted]?

A. No, I did not.

Q. What did you do to prepare for today's deposition?

A. I read Adriaens' rebuttal, Professor Adriaens' rebuttal. I tried to prepare for, essentially, dismissing the points that he makes in his rebuttal.

Q. What -- and can you describe what that means? What did you to do to prepare to dismiss points in Professor Adriaens' rebuttal?

A. Yes. So Professor Adriaens' rebuttal states, for example, if he cites a paper, he

would take certain sentence out of the context. For example -- can I gave an example? May I give an example.

Q. Go ahead.

A. So I base my basic definition of decentralized systems on the paper by Troncoso and three other authors from 2017. So this is the paper that systemizes 15 years of research in decentralization, and comes up with a definition of decentralized systems.

At that paper, so example, what Adriaens did, is that -- there is a motivation in 2017 paper which says it is not well understood how decentralization is defined. But that's the motivation of that paper.

And then it continues, it actually says, This is the motivation of our work; hence, we systemized -- systematized 15 years of research and then we give this definition.

So Adriaens would take the definition, you know -- definition. Take the sentence. There is no definition. Even Troncoso admits that there is no definition, no -- that's the motivation of their work, and they actually

[redacted] - Highly Confidential

propose the definition.

So things like that. And then you go, point by point, and -- yeah.

Q. Okay. Who did you meet with from the SEC in preparing for the deposition? Just names, not communications.

A. Yes. I met Mark Sylvester.

Q. And did you review any documents in preparing for today's deposition that were not cited in your own report of October 2021?

A. No, I did not. My report itself was cited in my report. I reviewed my report.

Q. Okay. Let's turn to another subject.

What digital assets, if any, do you yourself currently own or have you owned in the past?

A. [redacted] I have owned in the past other -- other digital assets.

Q. Okay. So -- so today, sitting here today, the only digital asset you own is [redacted]

A. Yes. I have interest in [redacted] as well, since part of my compensation is in [redacted]

[redacted] - Highly Confidential

Q. How much [redacted] do you currently own?

A. [redacted]

Q. [redacted]

A. Yes.

With my wife. So it's not my personal owning, so it's like a -- you know, I'm married and things --

Q. How did you acquire that [redacted]

A. All [redacted] were acquired by purchasing from my -- so, purchasing on the -- today registereds exchanges, so mostly from [redacted] so I would take my salary by coins from [redacted]

Q. When did you first purchase [redacted]

A. 2017.

Q. What's the current value of your [redacted] holdings?

A. [redacted]

Q. Why did you start purchasing [redacted] in 2017?

A. That's an interesting question. So, I would say working in this space -- and this is the blockchain space, et cetera -- so I was starting slowly by experimenting. It's more

[redacted] - Highly Confidential

like do we have skin in the game about the whole space that you are working on. This was the first motivation.

And then I invested a bit more when my understanding of [redacted] changed and what it actually could do.

Q. And when was that?

A. So that understanding was -- changing in the understanding was in 2020.

In the meantime I also -- so we also invested. [redacted] So we bought in the -- between 2017 and 2020, but my understanding of [redacted] the way -- so not from technical side, it changed in 2020.

Q. Did you invest substantially more money in [redacted] starting in 2020?

A. In 2020 substantially more -- I would say more, yes.

Q. Have your ever acquired [redacted] by mining?

A. No.

Q. Have you ever been compensated in [redacted]

[redacted] - Highly Confidential

A. No, I did not.

Q. Where do you store your [redacted]

A. [redacted]

Q. Have you ever -- have you ever sold [redacted]

A. I did.

Q. When?

A. I did several times. You can say I sold when I -- if I buy a different token, so you sell [redacted] to buy that token. So this was in 2017. And my last sale of [redacted] was in early 2021.

But not for -- so basically for other tokens, at that point I called it a day, and soon after that I moved my holdings back to [redacted] with -- [redacted].

Q. When you sold [redacted] in 2017, did you sell at a profit?

A. I sold it to buy other coins. So if you measure profit in U.S. dollars and -- so -- or U.S. dollars or any other fiat currency, then the answer is no because I never did it.

Q. Okay. What -- and what coins did you

[redacted] - Highly Confidential

use [redacted] to buy in 2017?

A. So, I was buying directly [redacted] -- so for fiat money, I was buying [redacted] at 2000-- in 2017. And probably I bought some minor coins.

So I think there was [redacted] as a project that's working on data storage. Some other coins I cannot -- you know, I don't have an exact recollection, but these were minor -- these were minor amounts.

So nothing --

Q. Okay.

A. -- nothing substantially.

Q. So just so we have a clear -- just to clarify, other than [redacted] what other digital assets or tokens have you purchased?

A. I purchased [redacted] and I purchased [redacted] on very small amounts at some point. Very early in 2017.

And few others. Maybe [redacted] I recently purchased [redacted] because my son asked me to buy him some [redacted] I guess after [redacted]

THE COURT REPORTER: After what?

[redacted] - Highly Confidential

THE WITNESS: [redacted] or something like that. When [redacted] became popular --

MS. ZORNBERG: Did you get that?

[redacted]

A. My son -- my son wanted me to buy him some [redacted] And I think --

Q. Okay.

A. -- yeah.

Q. So other than [redacted] and [redacted] sitting here today, can you think of other digital assets or tokens you've purchased?

A. There could be others, minors, for very min-- for like smaller fraction. I don't remember exactly which one.

I would definitely not say that the -- that the list ends there but honestly not because I'm trying to withhold, because I don't remember.

Q. Okay. Have you ever --

A. At some point -- at some points for -- what I know, what I can recall, I invested in the ICO of [redacted]

[redacted] - Highly Confidential

Q. [redacted]

A. Yes. And so basically, I think -- I remember I sent half a [redacted] to [redacted] ICO and recovered less than that. So no profits, even a loss in [redacted] which is typical when you do these things, yeah.

Q. Would you say that among all digital assets, you've purchased more [redacted] than anything else?

A. We can say that. I probably -- at the beginning, there was -- yeah, more [redacted] than [redacted] for sure at the beginning. I don't hold any [redacted] today.

Q. You hold no [redacted] now?

A. No.

Q. Okay. Let's just first finish up on [redacted] Then I'll turn to [redacted]

Have you ever used [redacted] to purchase a product?

A. No, I did not.

Q. Have you ever used [redacted] to purchase a service?

A. No, I did not.

Q. So, can you just describe how much

[redacted] - Highly Confidential

[redacted] you -- you've owned at any point and, you know, when you purchased and when you sold?

A. I don't remember exactly. I think at some point I had like 100 [redacted]

But I'm not sure. So everything -- that all is conflated now to my [redacted] holdings. So...

Q. Why did you -- did -- was it your testimony that you transferred your holdings in [redacted] to purchase [redacted]

A. At some point, yes.

Q. When was this?

A. Last time, end of 2020, beginning of 2021.

Q. Have you ever used [redacted] to purchase a product?

A. No, I did not.

Q. Have you ever purchased XRP?

A. No, I did not.

Q. Have you ever held XRP, no?

A. I did not.

Q. Do you own any NFTs?

A. No, I do not.

Q. Have you ever used [redacted] to purchase a

[redacted] - Highly Confidential

service?

A. I did not.

Q. Okay. All right.

Outside of your work on this case, can you describe your personal or professional use of the bitcoin blockchain.

MR. SYLVESTER: Objection.

A. Personal or professional use of bitcoin blockchain?

I didn't get the question, sorry.

Q. Have you ever used the bitcoin blockchain for personal use?

MR. SYLVESTER: Objection.

A. I still don't understand the question. Like how would you define "personal use"? [redacted]

Q. So let me -- let me rephrase the question.

[redacted] how, if at all, have you used the bitcoin blockchain?

A. I did not.

Q. Have you ever run a bitcoin node?

A. I did.

Q. You did run a bitcoin node.

A. Yes.

Q. When did you do that?

A. I started two months ago.

Q. For what purpose?

A. For purpose of further decentralization of the network, to contribute with the small node to further decentralization of the network.

Q. Have you ever run a node on a blockchain system other than bitcoin?

A. No, I did not.

Q. Have you ever run a bitcoin miner?

A. No, I did not.

Q. So the node that you started to run two months ago can participate in validation but does not mine?

A. Yes.

Q. Have you ever submitted a bitcoin improvement proposal?

A. No, I did not.

[redacted] - Highly Confidential

Q. Have you conducted research projects specifically using the bitcoin network?

A. Currently, we are doing a similar project. It's not exclusively using bitcoin network, but it's using the bitcoin network.

Q. What project is that?

A. This is the project of anchoring the membership of proof of stake, like blockchains, into bitcoin.

Proof-of-stake blockchains have an attack surface when they reconfigure membership. This is actually similar to accept the ledger. And when you change the membership, this is the pain point of these protocols.

So if you put concisely the membership of the network into the bitcoin blockchain, you get more security out of the whole system together.

Q. Is that a project you're doing for [redacted]?

A. You can say I'm doing it -- I started it in [redacted] I continued while I'm working with [redacted]. I wouldn't use the word "for." I would say the [redacted] knows, of course,

and supports that I'm doing this project, and yes, I would put it this way.

Q. And just -- would it be fair to say that your -- your project involves using a development on the -- hold on.

Say it one more time.

A. Yes.

Q. Explain how does -- how does the project relate Ethereum to the -- to the bitcoin network?

MR. SYLVESTER: Objection.

A. Ah, so I didn't say Ethereum.

Q. Okay. So tell me --

A. I was talking about proof-of-stake family of protocols. And also, Byzantine full tolerance protocols. They -- they are very similar, so proof of stake and Byzantine full tolerance protocols, they are -- they are very close to each other.

Their pain point is the -- so if you have a static membership -- static membership meaning membership doesn't change -- then you can run Byzantine Full-Tolerant protocols, and that works. This is like how we understand

them, that would work.

It would come with a big assumption. It's usually you have a threshold of the number of Byzantine nodes that such a protocol can tolerate. And that's static, that's fixed in time.

So if you start modifying the membership, you are starting playing with the -- with the -- essentially which nodes.

For example, to give you -- give you an example. In proof-of-stake protocols, what's dangerous is that current power of the network is relate to the stake of the validators.

And we have a snapshot in time in which, you and me, we have the power in the network, but then, we are transferring this stake to others. But we are keeping the cryptographic keys from this point in time.

So basically, once we don't have the stake in the network, we can essentially invent another history that would be valid because we were valid validators at some point, and if we present two alternative histories to the client, the client couldn't tell which one to believe

because they're both legitimate.

Now, what you -- what the client could say is this one that evolved first, is the right one, but how do you know which one is the first.

Q. So how is your project trying to solve for what you've described?

A. Great question. Thank you so much.

So it would, from time to time, as -- for example, this first -- as we are transferring tokens to others.

When the system sees that there is a lot of difference between the membership -- membership or the stakeholders at certain snapshot of time, and the other, it would go and checkpoint this information of the new members and the new stakeholders to the bitcoin blockchain, which doesn't suffer from this because of the way consensus protocol works in bitcoin. We can just checkpoint this information into bitcoin.

And basically, then, in order to mount the attack that I just described, you would need to mount the attack on bitcoin as well, to forge that network, in order for that work on your

network.

So you're actually gaining more security from the -- in a proof-of-stake blockchain or Byzantine fault-tolerant protocol from the proof-of-work protocol. You're getting the security from there.

Q. So your proposal would have proof-of-stake networks rely on bitcoin network for certain aspects of security?

A. Yes.

Q. Okay. Are you -- is it your view that a BFT protocol works well only if membership is static?

MR. SYLVESTER: Objection.

A. Depends on the definition of the protocol. So it's much better understood how it works, and the security properties are much more easier to guarantee and prove if the membership is static.

Q. So sit -- so sitting here today, are you saying that BFT protocols will only work well if membership is static?

A. No.

MR. SYLVESTER: Objection. Misstates

his testimony.

THE WITNESS: Yes.

Q. Okay. So you're not --

A. I'm not saying that.

Q. Okay. Have you ever run an Ethereum node?

A. I did not.

Q. Have you ever run an Ethereum miner?

A. No, I did not.

Q. Have you ever proposed changes to the Ethereum consensus protocol?

A. I did not.

Q. Have you done any research projects -- putting aside the proof-of-stake project that you've just described you're currently working on, have you done any research projects specifically relating to Ethereum?

A. The predecessor of that project was trying to do the same what I described, checkpointing into bitcoin network, checkpoint into Ethereum proof-of-work network, because so long as you have a proof-of-work protocol, you can do this thing.

And we had one protocol, one --

basically the predecessor to the work of checkpoint into bitcoin that I'm describing, that we did as a -- while I was still in IBM, actually. We did -- we checkpoint into Ethereum assuming Ethereum runs on proof of work. So it's important which class of protocol checkpoints into which. You cannot checkpoint --

Q. Right.

A. -- proof of stake into proof of stake that doesn't make sense, but you can checkpoint proof of stake to proof of work.

Q. So have all of your checkpoint research projects involved creating an extra checkpoint on a proof-of-work network?

A. Yes, they did.

Q. Okay. Outside of your work on this case, have you ever used the XRP Ledger?

A. I did not.

Q. Well, including your work on this case, even during your work on this case, did you use the XRP Ledger?

A. No, I did not.

Q. Why not?

[redacted] - Highly Confidential

A. I didn't. So while I was analyzing the -- mostly the internals of the consensus protocol, I was inspecting the code, as I mentioned. And I was expecting -- inspecting the papers which were endorsed by Ripple employees.

To -- for me to gain the understanding of how the protocol works, I gained it without running the node.

Q. Okay. So have you ever run a node on the XRP Ledger?

A. No, I did not.

Q. Have you ever run a validator on the XRP Ledger?

A. No, I did not.

Q. Have you ever proposed changes to Ripple D?

A. No, I did not.

Q. Have you ever conducted research projects relating to the XRP Ledger?

A. Apart from the paper that we discussed, if you call that, that would be a yes. Or otherwise, no.

Q. And the paper that we discussed,

[redacted] - Highly Confidential

you're referring to the 2017 --

A. '17 paper, yes.

Q. -- paper.

Okay.

A. Yes.

Q. Have you -- while at [redacted] did any of your work projects involve the XRP Ledger?

A. No, they did not, apart from -- yeah.

Q. Are you aware that the XRP Ledger contains a decentralized exchange?

A. I think I heard about something that would go along these lines. I'm very about calling things decentralized, as you may imagine, without looking more deeply into that.

Q. So you -- you don't really know?

A. If you -- if you tell me, Do I know if it runs on decentralized exchange, I say yes, then I might be admitting that it's decentralized, so this is not what I'm doing.

So I heard, I have -- I have understanding that some people run something which they call decentralized exchange on the Ripple -- on the XRP Ledger.

Q. Have you ever used it?

[redacted] - Highly Confidential

A. No.

Q. Do you know what the Interledger Protocol is?

A. Not -- no.

Q. Okay.

All right. We're going to mark -- or show you what's been premarked, actually --

MR. SYLVESTER: Louise, we're at about an hour. Should we take a break before you mark?

MS. ZORNBERG: If -- if Dr. [redacted] wants to take a break, we can break. Otherwise I want to -- I'd -- I'd push through, but if this a convenient time.

THE WITNESS: Yeah, let's -- let's take a break, yeah.

MS. ZORNBERG: Ten minutes? How --

THE WITNESS: Ten minutes.

THE VIDEOGRAPHER: The time is 9:24 a.m. We're going off the record.

(Recess from 9:24 to 9:39.)

THE VIDEOGRAPHER: It is 9:39 a.m. We are back on the record.

Q. All right. Dr. [redacted] I'm showing

[redacted] - Highly Confidential

you what's been marked as Exhibit [redacted] 1.

(Expert Report of [redacted]

Ph.D., was marked [redacted] Exhibit 1 for identification, as of this date.)

Q. Is this a copy of your expert report in this case?

(Witness reviewing document.)

A. Yes, it is.

Q. Okay. And on page 28, is that your signature?

A. Yes, it is.

Q. Does this report contain all of the opinions that you're expressing in this case?

A. This report contains all the -- yes.

Q. I'm asking, because if -- if there are any --

A. Yes, if there -- yeah, so what I wrote in my paper, maybe. But my report, if there are any additional -- so provided with all the information I got until that date.

If there are new developments, I reserve the right to supplement my report.

Q. Well, are there additional opinions that you're offering in this case that are not

[redacted] - Highly Confidential

contained in your report? As you sit here today.

A. Yes. If -- as of my -- so in particular, my report is related to a snapshot, as I've explained on the -- on the software.

If the software changes, there could be additional opinions.

Q. Okay. Sitting here today, Dr. [redacted] are you -- are there additional opinions, as you sit here today, that you're offering in this case?

A. I know there are other changes, to the software, which might change certain things that I wrote in this report.

And they actually happened after the report was submitted.

So I know about that. But I'm not -- I'm reserving the right. So in some cases, it would take me more time to form this depth of the opinion. So I wouldn't necessarily offer them today. I -- in some cases, I would require more time to, for example, analyze the software changes in depth, to adapt my report to the new reality, right? So you always need to -- when

you have already decentralized system, you're actually taking a snapshot in time.

Q. What changes in the software for the XRP Ledger have been made since October 4, 2021, that you're referring to?

A. To my understanding and what I checked is that there are two validator list sites instead of one. So Ripple 1.7.3, there are -- there was one validator list site, which was important for the things I wrote in the paper, in the report. And that was controlled at the URL vl.ripple.com.

So there was another one added to the configuration, default configuration filed, plus recently there is update that's called Negative UNL. That was in the software since 2020, but it was not active. So in a sense, it didn't influence the operation of --

Q. Okay.

A. -- the software.

But it was, to my understanding, activated on 23rd of November, so just recently.

Q. All right. Let's take those two for a minute. You said that since your report in this

[redacted] - Highly Confidential

case, you've seen that the -- the rippled code now contains two validator list sites.

Correct?

A. Yes.

Q. Does that change in the rippled code affect any of the opinions you previously expect -- expressed in your report?

A. We would not go in -- you would need to go in details to see. There are certain sentences that I say. For example, I'm pretty sure I say at some point that only -- that the only validator list sites listed in the configuration file is Ripple. That's obviously need to be amended.

In general and on a high level, does it influence -- because in the report, I'm accepting the Troncoso definition that a system is decentralized if no single authority is fully trusted by all. That change doesn't impact the fact that XRP Ledger, according to that definition, cannot be classified as decentralized. So it doesn't impact the main finding of the report.

Q. What -- what opinions in your report

[redacted] - Highly Confidential

have changed based on the change in the software listing to validator lists?

MR. SYLVESTER: Objection.

A. I would need to spend more time, so basically, I'm offering at that -- at this moment, I'm offering my opinion on the current report. I would need more time to -- in details, so I don't want to tell you certain things now online and then not be sure that these are all the implications. So basically, that -- so if I say it affects Sentence A, I need to just process and be sure that it affects Sentence A; but I also need to be sure that if -- you know, if I don't say it affects Sentence B, that this is actually the case; it may be affecting Sentence B, and I need more time to go through that.

Q. You're not prepared to do that today?

A. I'm not prepared to do that today in details. I can discuss certain high-level things. Yes.

Q. At a high level --

A. Yes.

Q. -- how do you think it could affect

your opinions in this case that the rippled software lists two validator sites?

A. It will -- just let me refer to my report.

(Witness reviewing document.)

A. For example, I see one thing that is not necessarily so. I see one item that would not need to be done by Ripple anymore.

Q. What are you referring to? What page?

A. Page 25, item 1. But this is an example. I would -- you know, before we go into details, I would just give an example. So I gave you an example of my opinion that doesn't change, which is the qualification of the XRP Ledger on the Troncoso definition it would remain centralized. I'm giving you an example of what changes.

Q. Okay. And --

A. And then for exhaustiveness of this, we would need -- I would need more time to make sure, you know, that this is one that I notice, aha, this would change. So we can discuss that.

Page 25 -- sorry.

Page 25 at the top of the page.

[redacted] - Highly Confidential

Q. Okay.

A. So --

Q. So let's just -- let's just be clear for the record. Page 25 at the top of the page contains your answer to the question, E2, quote, To what extent have Ripple's efforts been needed to support the proper functioning of the XRP Ledger, closed quote?

Right?

A. Yes.

Q. Okay. So you're saying that the change, you've noticed recently of there being two validator lists in the rippled code, could impact your answer to that question.

MR. SYLVESTER: Objection.

A. Yes. So it could impact my answer to that question, assuming that the protocol changed. So in my -- for the specifics of my report, which are discussed and I'm getting -- if I fix my opinion to my report, my report sticks -- my opinion with rippled 1.7.3. So it wouldn't change this. If you say, Would I change my opinion? And this refers to 1.7.3, the answer is, no, it wouldn't change.

[redacted] - Highly Confidential

If new elements are presented as of October 4, and this happened after October 4, if I would be in a hypothetical case where I would be assuming the new version of the code and writing this report as of Ripple 1.8.1, this would change.

MS. ZORNBERG: Okay. Let's show Exhibit 13.

Q. And while we're getting that exhibit, I would like to direct your attention to the bottom of page 20 of your report.

In the last -- in the last paragraph, of your report, you reference the validators example text file. Correct?

A. Sorry. Can you repeat? I was --

Q. Yeah. Page 20 of your report.

A. Yes.

Q. The very -- it's the very last sentence on the page that ends on the top of page 21. In that part of your report, you reference the validator example .text file. Correct?

A. Yes.

Q. Okay. So please take a look at what's

[redacted] - Highly Confidential

been marked as Exhibit [redacted] 13.

(Document was marked [redacted] Exhibit 13 for identification, as of this date.)

A. Yes.

Q. Do you recognize this document?

And I'm basically asking, is this the document -- is this the -- what you've cited, at the very last line of your report, on page 20? The cite.

A. It is not. So --

Q. Why is it not?

A. So just a second.

(Witness reviewing document.)

Q. Dr. [redacted] doesn't the -- the actual citation at the last line of your report, page 20, match exactly to --

A. Yes.

Q. -- the GitHub site at the top of Exhibit 13?

A. It does. I see where the error is. Okay.

Q. Okay. What is the error that you're seeing?

A. The error is that this is the cite --

so the link that I put, so I'm always referring to the code that was in the release, 1.7.3.

And this was on the develop branch. So basically, the link that I'm giving, by error, is referring to the development branch, which is not in the release branch. So you can see by the URL mentioned the develop.

Q. Okay.

A. So the development, yes, in the development branch, the second validator list site was mentioned for a long time, but this doesn't affect the release.

Q. Okay. So you're saying there's an error in your report in including that citation?

MR. SYLVESTER: Objection.

A. Yes. So there is -- what I meant here is to refer to the release branch. And I think -- so not I think.

I basically say that in page 19, Item 3, I'm referring to rippled software on its release branch.

And then I'm probably by omission giving the -- the development branch, which you can see the URL denoted as develop.

[redacted] - Highly Confidential

Q. If you turn your attention to lines 57 and 58 --

A. Yes.

Q. -- of Exhibit 13.

Would you agree that those lines of code identify one validator list for vl.ripple.com and one for vl.xrplf.org?

A. They do.

Q. What do you understand that to mean?

A. So this is -- basically, this was in the development branch but not in the release of 1.7.3.

This was propagated to the release. This is the change that we discussed after my report which propagated to the release branch of 1.8.1, if I'm correct. This means that a server which periodically refreshes the dUNL, instead of going only to vl.ripple.com and no other site as a release 1.7.3, would now first go to the vl.ripple.com. And then if this doesn't work, it would go to xrplf.org.

Q. How long was -- did this commit exist in the code?

MR. SYLVESTER: Objection.

[redacted] - Highly Confidential

A. I'm not sure. If we look at the document that you gave me, it says, Latest commit on May 10. Need to observe that this is the commit to the development branch.

Q. Okay. And you -- you considered this before you wrote your report, correct?

A. I saw this before I -- before I wrote my report.

Q. Okay.

A. I was focusing on the release branch as I pointed out on page 19, Item 3.

Q. All right. Let me just show you briefly, Exhibit 13A.

And that would be Exhibit [redacted] 13A.

(History Page was marked [redacted] Exhibit 13A for identification, as of this date.)

Q. I'll represent to you that Exhibit 13A is what -- is the page you get if you click on the link in Exhibit 13, that says, History.

So this is the page that shows up as history.

Did you ever review Exhibit 13A in your work on this case?

A. This is -- so as you presented it

here, I did not have this list. This is mostly related to the development branch again.

Q. Okay.

A. And I focused my findings on the rippled release Version 1.7.3, as pointed out on page 19, item 3.

Q. And the history, in Exhibit 13A, do you agree it shows that a commit was made on July 27, 2021, to add the XRP Ledger Foundation to the validator list sites?

A. This is the commit, yes, that affected the development branch --

Q. Did you --

A. -- which means at that point -- which means at that point if somebody downloads the releases code, it gets -- it is not affected by this change.

Q. Did you consider this commit at any time before July 27, 2021?

A. If you asked me did I saw that the development branch has two validator sites, it does. I did.

I took a snapshot of the release talking about with one validator list site.

[redacted] - Highly Confidential

Q. So --

A. Yes.

Q. So Dr. [redacted] if you were aware of this code change in development before you wrote your report in this case, why did you not -- what -- did you consider it -- did you consider it in writing your report in this case?

MR. SYLVESTER: Objection.

A. I -- well, if -- what I read, I considered, you can say I had it in mind. So you can say I, you know, considered it in the sense of consideration that we discussed before.

When you talk about decentralization of a certain blockchain, you need to fix the code.

This is a development branch. Things can come, go, and back from the development branch.

So for that purpose I'm focusing on the release branch. Now we can -- I mean, so this propagating to if I were writing the report now, I would need to consider this change and include it in my report because now, only now, after I submitted my report, it's in the

release.

Q. And what would happen if a validator used this configuration in Exhibit 13, for its Unique Node List?

A. I think we discussed it. So if this means that it go would to vl.ripple.com and fetch the -- try to fetch the UNL from there, if this doesn't work, it would go to the vl.xrplf.org and try to fetch the UNL from there.

Q. Would the validator recognize the nodes on both lists as trusted?

A. It would -- so from the perspective of the node, it would continue its operation, regardless of where it fetches the UNL from.

Q. So is that yes?

A. Can you repeat the question?

Q. Yeah. Would a validator using the configuration code in Exhibit 13 recognize the nodes on both UNL lists as trusted?

A. I wouldn't say so trusted -- it would continue operation of the protocol, regardless of the place it fetched the UNL from.

Whether they are trusted or not, I

[redacted] - Highly Confidential

mean, if the -- so if the node would trust the UNLs that it gets from the validator list sites, the answer would be yes.

Q. Can a server run the development branch?

A. You can install the development branch, sure, run it in production yes, you can.

Q. Okay. And is it your understanding that the UNL at Ripple and the XRPL Foundation URLs -- hold on. Let me rephrase.

Do you know one way or another if the UNLs at the Ripple's published UNL and the XRPL Foundation's URL are identical?

A. I do not know for sure.

Q. Okay. All right.

Were there drafts of your final report, prior to this final version in Exhibit 1?

A. There were.

Q. Did you show those drafts to anyone?

A. I showed them to [redacted]

Q. Do you know who [redacted] showed them to?

A. I suspect that they showed them to the

[redacted] - Highly Confidential

SEC.

Q. Who at [redacted] reviewed your draft?

A. [redacted] [redacted] mostly. At some point [redacted] I don't remember last name. I'm not sure [redacted] reviewed it, but I don't think I got any comments from [redacted]

Q. And did [redacted] and the others at [redacted] aside from [redacted], provide comments?

A. Sorry. Can you repeat? Did [redacted]

Q. Did anyone at [redacted] or the SEC provide comments on your draft report?

A. So --

MR. SYLVESTER: Objection. With respect to the SEC, any SEC comments, I just instruct you not to get into the substance of any communications between any SEC attorney and yourself.

A. So SEC and [redacted] yeah, they provided comments on my draft, yes.

Q. Okay. You identify two changes, in the software, rippled, since your report was issued, that might change your opinions.

The first we've just talked about, the two validator lists. You also mentioned a

Negative UNL update.

A. Yes.

Q. What is that?

A. To my understanding, which is -- so that's a substantial protocol change which doesn't affect dUNLs. So when you reason about decentralization of the system of the dUNL, this Negative UNL doesn't really impact that aspect of centralization.

Now, Negative UNL, to my understanding, but I would definitely need time to dive into more details of that, to my mid-level understanding, is that what it does is it takes this dUNL and doesn't treat it as a fixed line, assuming that you get always the same UNL from the validator list site.

Now, this not a static configuration, but this can change basically -- now, I'm getting into the territory where I need more time to inspect, but based on how nodes behave on the network, you can exclude them from the UNL.

Q. How might that change in the rippled code affect the opinions you've given in

this case?

A. For that I would need more time to opine.

Q. Sitting here today, you're not prepared to say one way or another if it affects your opinions --

A. I can say it does not impact the main. So it doesn't make XRP Ledger suddenly pass the Troncoso definition because it doesn't have -- so neither of the two changes that I can say make XRP Ledger pass the Troncoso definition because we still need to trust a single authority. We can go into details why.

There might be other parts of the paper. Notably I would need to understand, you know, does it impact my Appendix B attack or some other point in the paper? But for that I would not offer any other opinion before I have time to opine on that.

It's a very -- it's a substantial change. It's an interesting one. It's an interesting one. But -- and I would actually like to have more time to look at it, but I didn't.

[redacted] - Highly Confidential

Q. Has the SEC given you the assignment -- any assignments beyond the issuance of the report you've already done in this case?

A. No.

Q. So you've not been asked -- sitting here today you've not been asked by the SEC to offer a supplemental opinion?

A. No.

Q. So why don't you tell us, what is your view as to -- going back to the two validator list sites that you've acknowledged are now in the rippled code, why does that not change your opinion that -- that there is still a single trusted -- hold on. Let me rephrase.

You've said that the two validator lists sites do not affect your opinion on how the Troncoso definition applies to the XRP Ledger. Please explain why.

A. Assume vl.ripple.com is the first validator list site. Let's assume that it doesn't disappear; it continues publishing the list. It just serves -- the different list is the attack that I'm describing for the untrusted

[redacted] - Highly Confidential

validator list site. It just serves a different dUNL -- continues serving different dUNLs to different nodes.

It can break safety line as properties of the system, regardless of the adding of the second one. You can add third and fourth and fifth, and it doesn't really matter.

In the way they are added, like one by one, one after the other.

Q. So your view is that it doesn't matter how many UNL validator lists are referenced in the rippled code, no matter what? Even if there are a hundred, it's still a centralized system?

A. Why? Because if you default to first, as the software goes and defaults first to first, and that one is working, it can serve different UNL to different nodes, hence by actually invalidating, so making the UNL overlap nonexisting.

And as we know from the analysis which I confirmed through my inspection of the code, this overlap is required. And you would need to trust the first validator site on the list, that it doesn't serve a different UNL.

[redacted] - Highly Confidential

And then if that one doesn't work, you're defaulting to the second one. You need to trust that one. So let's assume vl.ripple.com doesn't exist anymore. Everybody goes to vl.xrplf.org and now everybody needs to trust vl.xrplf.org that it's not -- that it doesn't serve different UNLs for different people.

So somehow, what this contributes to the protocol, is it improves in some sense availability if validators list sites are not trying to cheat others. It would help you that.

But it still assumes that validator list sites do not cheat to validator nodes.

Q. What is the basis for your statement, that there's still a default validator list when there's more than one listed in the code?

A. So because the software is defaulting to the first one; and then if it doesn't work, it goes -- it goes to the second one.

Q. What is that based on?

A. Based on my analysis of the protocol.

Q. Is it your understanding that validators will only use the first working

[redacted] - Highly Confidential

listed UNL in the code?

A. While it works. Yes. While it replies.

Q. So it's your understanding that if there are two that are listed, that validators will only use the first one and never reach the second one as long as the first is working?

A. This is my understanding of software, yes.

Q. Are you -- are you a hundred percent sure of that?

MR. SYLVESTER: Objection.

A. Yes.

Q. Okay.

A. Let's -- yeah, let's say, because this was not the -- this was not the part of the software I was -- analyzed when I did, I would need more time to give you 100 percent answer. And I'm pretty sure this is the case.

Q. Okay. So your testimony is that you're pretty sure, but you're not a hundred percent sure.

A. I would need more time because this is a change that affected my report.

[redacted] - Highly Confidential

Q. Okay.

A. Under this understanding, this is what's happening.

Q. Okay.

A. Let me make sure that this is -- so with additional time, I can make sure that this is -- actually you understand.

Q. To be clear, I'm not requesting that you do anything.

A. Yes.

Q. Although I am requesting that you turn to the curriculum vitae that is contained in your report.

And my question is, when did you most recently review your curriculum vitae?

A. I think I reviewed it before submitting it to this -- before sending the report. So late September, early October.

Q. Okay.

MS. ZORNBERG: Can everybody on Webex please go on mute.

Q. Okay. So you last reviewed the curriculum vitae in September?

A. Yes.

[redacted] - Highly Confidential

Q. Okay. Is there anything that should -- that you would want that's new since October 4, 2021, that you would want to add?

(Witness reviewing document.)

A. So the first paper on the publication list on page 6 of the appendix that appears, in the meantime -- yeah. I don't think there are any substantial change.

Q. Okay. So I just want to briefly review with you your educational background.

A. Yes.

Q. You have a degree in electrical engineering from the [redacted] in 2021. Yes?

A. Yes.

Q. And you got your Ph.D. in distributed systems in 2008?

A. Yes.

Q. And that was from the [redacted]? Right?

A. [redacted] is the school at [redacted] is the university, [redacted]

[redacted] - Highly Confidential

[redacted]

Q. Thank you for that clarification.

How much of your educational training was in coding?

MR. SYLVESTER: Objection.

A. How would I -- what do you mean?

Q. Well, I'm trying to understand if you -- what is your coding capability?

MR. SYLVESTER: Objection.

A. How do you measure coding capability?

Q. Do you consider yourself a coder?

A. I consider myself a coder, yes.

Q. Yes. Okay. Do you consider yourself an expert in computer coding?

A. I -- we would need to define "expert in computer coding." There are certainly other people who can code better than me. Yes.

Q. For the development -- have you worked on development projects where you yourself are the coder of those projects?

A. Yes, I did.

Q. Okay.

What language do you code in?

A. The last contributions were in Go.

Go. Go on. Go. Go. Go.

Q. Can you spell that?

A. G-O.

Q. G-O. Okay.

A. Yes.

Q. Thank you.

Besides your undergraduate degree in electrical engineering and your Ph.D. in distributed systems, have you received any other formal education training?

A. Formal as in a degree? No.

I mean, I went to high school. You're not probably saying that. Yes.

I went to high school and elementary school, yes.

Q. Yes. Okay.

Do you hold a degree in economics?

A. I do not.

Q. Have you done any formal academic training in economics?

A. I did not.

Q. Do you have an MBA or an equivalent degree in business?

A. I have a micro MBA, which doesn't

[redacted] - Highly Confidential

qualify as MBA. I have a micro MBA from a course that I took while in [redacted]

Is it mentioned?

Q. Is that -- is that reflected in your CV?

A. No. It's a one-week course. You can disregard it if you want.

Q. Okay.

A. I was elected the best CEO of that week, but -- yeah.

Q. Okay. So it was a one-week training class on business.

A. You can put it that way.

Q. Beyond the one-week training class in business at [redacted] have you received any formal training in business or business management?

A. I did not.

Q. Have you received any degrees or formal academic training in the areas of innovation and entrepreneurship?

A. Can you repeat it again. Sorry.

Q. Do you hold a degree in innovation?

A. No. I mean, innovation as in -- what's a degree in innovation.

Q. You know, I'm not --

A. I mean, by getting a Ph.D. and doctor, I innovated something, so I got a degree in innovation. But I -- it's not called that way.

Q. Okay. Is it -- is it fair to say that to the extent there are universities that offer degrees in entrepreneurship studies or innovation studies styled in that way, you've not received degrees in those areas?

A. There is a degree in innovation and entrepreneurship. I did not.

Q. How about environmental science? Have you received any degree in environmental science?

A. I did not.

Q. Have you taken any academic coursework on environmental science?

A. I did not.

Q. Do you consider yourself an expert in the field of environmental science?

A. I did not.

Q. How about in the field of business? Do you consider yourself an expert in business management?

A. I do not.

Q. What is the distributed blockchain system?

A. Distributed blockchain system is a different definition. It's a distributed system, meaning there's several computers that are contributing that are working towards a common goal, roughly speaking. The famous definition of the distributed systems, by Tanenbaum that I cite in my report says that distributed systems appear to the end users as a single coherent system. "Coherent" is a bit vague there. It depends on the specification of the system.

But systems function as -- as one, regardless of the fact that it's executed on different machines, on distributed machines.

So that would be a distributed system.

Now, the blockchain system is typically a distributed system in which there is a data structure, which reminds of a blockchain. So there is a chain of blocks. There are -- there is certain data contained in the block. And the blocks are linked, usually

cryptographically to each other.

Q. Do you consider bitcoin, Ethereum, and the XRP Ledger all to be distributed blockchain systems?

A. I do.

Q. Okay. And do you consider the terms "blockchain system" and "distributed ledger system" to be interchangeable?

A. We can say that on a high level, yes. It requires definitions of both of the terms. But people, when they say "blockchain" and "distributed ledger," they tend to often mean the same thing.

Q. Okay. For purposes of today's deposition, if I use the terminology "blockchain system," is it -- can we agree that that will also encompass distributed ledger systems?

A. I think we just said that all three systems, we can classify them in distributed blockchain. So, yeah, feel free to call them blockchain or distributed ledger. I would go with it.

Q. Okay. On the -- still on your CV, at the bottom of page 2, you noted that you were

the PC co-chair of three peer-reviewed workshops with published proceedings --

A. Yes.

Q. -- in the period 2017 to 2019.

What does that mean?

A. Workshops are typically ranked below conferences and journals in academic quality, which is why I don't list workshops on my CV. When you are PC co-chair -- program committee co-chair, which means that you are, either alone or with other co-chairs, selecting which researchers are going to form a program committee.

And what the program committee does then is, that it reviews the papers submitted by other researchers. So like the editor of -- you're not the editor but you're organizing other -- you're inviting other researchers to contribute by -- to peer review the submitted papers.

So PC co-chair is the person who actually asks and oversee the entire process of the -- of the review process. It invites other researchers to join the program committee.

[redacted] - Highly Confidential

Q. Okay.

A. And this is how it works.

Q. You mentioned a ranking. Is that -- what do you -- what do you mean by that?

A. So, I meant that PC co-chairs, for example, they -- if they are co-chairing, they typically look at the process, inviting people to be program committee -- members of the program committee, and make sure that the reviews are detailed enough that they are timely, rather than reviewing the papers themselves.

Sometimes, you know, you're jumping into -- if it's needed that there is an additional review, but this is usually not the part of the -- so it's more the -- it's not the hierarchy, it's more the distribution of roles.

Q. Okay.

A. Yeah.

Q. Within scientific literature, what does it mean for a publication to be peer reviewed?

A. Yes, so what this means, that there were some peers, usually people who sit on the

set program committee, who would read the paper, and accept that this is acceptable in the -- so, it should be published. So basically there is a filter.

So program committee, which we discussed, poses a filter and selects, out of submitted papers, a fraction of them. Depending on the quality of conferences, fraction can be bigger or smaller.

Q. Are peer-reviewed publications considered to be more reliable than those that are not?

A. That's a good question. So, we will need to see by whom. There are some very valuable -- normally you would. In the scientific world, in the academic world, the general answer is yes.

This is not the only answer. Why? Because sometimes the impact is measured, for example, by the number of times people cite your work.

There are certain cases where people don't publish their work in a peer-reviewed sense. So they publish it, you know, as -- so

[redacted] - Highly Confidential

there is freely accessible and everything, but in the -- they're not peer reviewed. I don't know.

One example that comes to mind is the bitcoin's white paper. It was never peer reviewed, this was just out there, but you wouldn't say that this is a bad paper and that it has a small impact.

You would look at other metrics, for example, like the number of citations, and it would give you what people -- what impact on thinking and, you know, advancement of human knowledge this has.

Q. Okay.

A. So in general, yes. In practice, it's -- it's a bit more blurry, yeah.

Q. Okay. When you -- when you said "impact," I want to understand; in your mind, what's the relationship between a paper having impact versus being reliable?

A. Did you define reliable paper? Which means -- how we define reliable paper? That all the claims in the paper are...

Q. Well, what do you think of as a

[redacted] - Highly Confidential

reliable paper?

A. So that would be paper that has reproducible results. That has something that, you know, has -- basically comes with research that can be validated by others --

Q. Okay.

A. -- independently.

And this result is reproducible, and so we would call it reliable.

There -- there are also -- for example, the difference would be -- between reliable and impactful paper, would be a paper that has a bug, so describes a protocol that has a bug inside, but bug is difficult to discover, it's discovered only years afterwards. But in the meantime, there is a lot of citations to that paper, so the paper is impactful.

Q. Okay. Why did you decide to leave [redacted] to become self employed?

A. I decided -- so I worked in [redacted] since 2015, and I worked on blockchain projects. So, you know, we can definitely add permission to blockchain projects, to the space of blockchain projects.

[redacted] - Highly Confidential

And I worked on that, and in my classification of -- and methodology, we'll see a distinction between permissionless and permission blockchains.

So while working on permission blockchains, I was one of the coin mentors of [redacted]. I'm one of the three original architects of the flow, how that works.

And this was meant to be a blockchain that's used for businesses. Right? So, this is just a decentralized -- so this -- this distributed -- some cases, it could be in decentralized -- ledger, which is distributed across multiple companies, and they track certain information. It's like a distributed database which tolerates certain aspects of faults. Right?

Companies that participate in these blockchains, they're selected either by consortium, they select each other, they kind of -- so this is where the permissionness of it comes.

Whereas in permissionless systems, which are open for participations of anyone,

[redacted] - Highly Confidential

this is a more open system. They are more challenging to design.

And, I was trying to actually work on that for a long time. So you see that some of the projects that I mentioned on bitcoin and Ethereum, they were started even while I was working in [redacted]

So for a while, I was trying internally to make [redacted] just a step in the direction of permissionless blockchains, and for different strategical reasons or -- or like orientation if [redacted] did -- didn't work.

And then I just decided to step out to that space and to work in that space because this is what I like working on.

Q. Okay. So would it be fair to say that one of the reasons, or -- or perhaps part of the motivation for leaving [redacted] was to focus more of your attention on permissionless blockchain?

A. Yes.

Q. And would it be fair to say that most of your work while at [redacted] focused on permissioned blockchain?

[redacted] - Highly Confidential

A. This is fair to say. Again, I mentioned two projects in -- you know, one paper that came out while I was in [redacted] was actually the link between permission blockchains and Ethereum network, and so there was research not constrained only to permissioned blockchains, but -- you know.

So, it was -- definitely the larger fraction of the time and larger percentage of time was oriented to permission blockchains, indeed.

Q. Can a permissioned blockchain be decentralized?

A. It can.

Q. So both permissioned and permissionless blockchains could be decentralized?

A. They can.

Q. Okay.

How are you compensated for your work with [redacted]?

A. I have -- so basically, I have a monthly -- contract with monthly payment in U.S. dollars. And I have certain like compensation

[redacted] - Highly Confidential

in [redacted] tokens with a big -- so with a vesting period and everything.

Q. Does your compensation with [redacted] depend in any way on the success of the project, projects you're working on?

A. In some sense, it would. Because, you know, you would get the recognition, and you would climb up the certain compensation ladder, or you would be awarded more compensation if you are evaluated as a -- successful.

But it's not -- if you asked it's in the contract, it's not in contract. It's more --

Q. Okay. Why did you leave academia in 2014?

A. Ah, that's a good question. So, I left academia because of the so-called two-body problem. In academia, usually my wife is also a researcher. She has a Ph.D. in [redacted]. And normally if you work in academia, one terrible problem that you have as a family is to find two jobs at the same physical geographical location.

So we tried to do it when we were in

[redacted] - Highly Confidential

[redacted] My wife was a postdoc in [redacted] This is like a big government -- I mean public research institution in [redacted] But she has a temporary contract as a postdoc.

I was assistant prof-- well, actually, it was professor, but it's not, because it's tenured, which is why I also mentioned tenure. And we had a position there. At some point, she needed to -- she was kicked out -- not kicked out, but her contract --

Q. You don't need to -- I don't need to know the details.

A. So, I should jump in, then she got an offer from [redacted], and I was picking up phone from my, like -- you know, trying to get a position at the same geographical location as her.

And I knew people in [redacted] because I work there as a postdoc before. I was picking up the phone, saying, Guys, you know, is it okay I come. We were collaborating for a long time. They were, of course, happy.

And I went -- it's is more difficult to become at that time -- you know, I'm not sure

[redacted] - Highly Confidential

I could do it now, but I probably have bigger chances than I had at the time.

To be a professor at [redacted] it's the top thing. It's comparable to being professor at MIT and Stanford University. So it's not easy to just go there and be a professor, right? That's why I went to [redacted].

Q. Okay. How many people work for you now in your current self employment?

A. Myself.

Q. Okay. Have you ever run a company?

A. I was -- I didn't run a company myself. So I -- I was -- at some point, [redacted]

Q. Okay.

So is it -- you've never run a tech startup?

A. I never run a tech startup yet, no.

Q. Okay. Do you sit on and boards of any

technology companies?

A. No.

Q. Okay.

All right. Let's turn -- turning to another topic.

I assume you consider yourself to be part of the scientific community?

A. I do.

Q. What types of professionals, or people, do you consider to be within the scientific community?

MR. SYLVESTER: Objection.

A. I'm not sure I understand the question. Sorry.

Which types of professional is considered part of scientific community.

Anybody who follows the scientific -- I guess, very broadly, anyone who follows scientific principles, tries to publish papers, you know, following the scientific approach in a repeatable fashion. We -- we discussed this a bit.

Normally to get some -- so this could be people who have formal academic education,

like Ph.D.s, master's students, but it doesn't really have to be.

Q. Okay.

When did you first read the 2017 Troncoso paper?

A. I read it while I was preparing for the -- this deposition. In details, yes.

Q. Okay. So, when was that that you first read Troncoso?

A. That must be June and July, yes.

Q. Of -- of 2021?

A. Yes.

Q. How did you come to read the Troncoso paper?

A. I was searching for -- to formalize my intuitive understanding of what decentralized systems mean. And I was looking through the literature to understand if somebody had done this before.

It's easier, much, much easier, much -- in some sense -- well, easier to convince other people, right, if you find the prior art which did it.

So I was doing this, and the one of

[redacted] - Highly Confidential

the papers that stand -- stood out because it systematized 15 years, as the title says, of research and decentralization and privacy, was that paper.

Since I know Carmela Troncoso, and George Danezis, so I know them. So, this was a paper that stood -- ah, these are the people whose opinion I value. They're very well known researchers in the community.

Q. How do you know Carmela Troncoso?

A. While we were working in [redacted] on COVID passports, she was -- we were proposing a [redacted] blockchain-based solution for basically how COVID passes work today. This was one of the ideas I contributed in March last year.

And we were developing a blockchain solution, and Carmela Troncoso -- whilst we talked to Swiss government to adopt this solution for their COVID pass, Carmela Troncoso was on the board that reviewed the solution.

Q. Have you discussed this -- your work in this case with Carmela Troncoso?

A. No, I did not.

[redacted] - Highly Confidential

Q. Okay. The Troncoso paper, by the way, that we've been referring to, is Reference 21 in your report. Correct? On page 30.

A. Yes, it is.

Q. The -- that reference, 21, lists the other authors. Which of other authors of that paper do you know personally?

A. I spoke to George Danezis.

Q. When did you speak to him?

A. September or -- August or September. This year.

Q. Of 2021?

A. Yes.

Q. What did you discuss with him?

A. Collaboration, because the -- George Danezis is a very well-known researcher in the blockchain space. He worked for many blockchain projects, including Facebook's -- or Meta's -- Libra or Diem project, and I was trying to get him on board that we collaborate on the same projects.

Which you could call, these are the projects that I do in the context of [redacted] but as you see, this is in the whole

decentralized computing research space, so we were discussing the possibilities if we collaborate together.

Q. Did you talk to Mr. Danezis about your work on this case?

A. No.

Q. Did you talk to Mr. Danezis about your plans to cite the Troncoso paper?

A. No.

Q. You said earlier this morning that the Troncoso paper itself had a motivation of -- of coming up with a definition of decentralization because there was no consensus at that point. Is that right?

MR. SYLVESTER: Objection.

A. One of the lines in the paper is that the motivation of the paper is that there are different definitions of the decentralization. And this was one of the motiving points for them to, in 2017 or earlier -- you usually do the research a bit earlier than -- than when the paper is published -- that they -- I guess like I'm giving an expert opinion here because fixing this is important for people, and they started

looking, like few years ago, including Troncoso. So at that moment we could say that it was not as clear as today what this means.

Q. Is -- today as you sit here, do people in the scientific community use the term, "decentralized," consistently, in discussing distributed systems?

MR. SYLVESTER: Objection.

A. Can you define "consistently"? Do they use the very same wording? Probably not. Do they think the same thing? That's a different thing. Well, what do you mean by "consistent"?

Q. Well, do you -- do you believe that there is consensus in the scientific community about the proper way to define decentralization in blockchain systems?

A. I think there is a consensus on what is the minimum. If not explicit/there is certainly -- there is certainly. To my understanding, there is implicit consensus of what requires the basic or minimum definition or if you want the necessary definition for a system to be considered decentralized.

[redacted] - Highly Confidential

Q. What are you referring to there? What -- what is -- what do you think there is consensus about?

A. So the minimal conditions that a the -- that system needs to satisfy in order to potentially be called decentralized. So, people might differ, right, if this is not satisfied, I don't know if any expert, my colleague, or anyone who would call the system decentralized even if this -- basic definition is not satisfied.

Then again, some might put the bar higher. So even if you pass this basic definition, some people would probably not still call it decentralized because you're not passing the higher bar. And the bar that we are discussing is the Troncoso definition.

Q. So, based on what you just said, doesn't that mean that people in the scientific community still today have not reached consensus on where to place the bar on decentralization?

MR. SYLVESTER: Objection.

A. It's -- I said, so they can -- there is -- to my understanding, there is a consensus

on the minimal condition.

Q. What is the consensus?

A. So, this is -- the fact, the fact, this is the -- to my understanding, no one would call the system -- no researcher who considers him an expert in the field would call a system decentralized, even if it does not satisfy the Troncoso definition.

Let's me put this way.

Q. What is the minimum condition for decentralization that you think there's consensus about?

A. That there is no single authority trusted by all, in the system. In a distributed system with authorities controlled by different parties, so with components controlled by different authorities or different parties, there must not be the one which is fully trusted by all.

I don't know if anyone who would call a system decentralized which does not satisfy this. Which means, you get a system in which there is a party which is fully trusted by all, and you get an expert who says, This system is

still decentralized even though there is a party which is fully trusted by all.

This would be negating the Troncoso definition and still -- still calling the system decentralized, I think there is a consensus that this is not case.

Q. Is it your position that the scientific community has reached consensus that Troncoso's definition of decentralization is the correct one?

A. I didn't say that. So you can phrase what I said in different ways.

For example, one of the papers that -- for example, Adriaens, Professor Adriaens cited in his rebuttal, it's not citing Troncoso but it's using the same definition, same wording, of -- what I just said, to say whether -- which system is decentralized.

It's not even citing Troncoso, but it's using the same wording. So, you know, if you ask whether, word for word, Troncoso definition is consented upon, that's probably -- we can discuss that, but the essence of it is -- what's emerging is the -- what emerged as a

[redacted] - Highly Confidential

minimal definition of decentralization.

So you need to pass the definition in order to be called decentralized. Some people might call -- still call it centralized, even if you pass the definition.

Q. Dr. [redacted] did you speak at the [redacted] --

A. I did.

Q. -- [redacted]?

A. I did.

Q. Do you recall -- and there's a -- there's a [redacted]

A. Not of my remarks but of my talk, yes.

Q. Of your talk.

A. Yes.

Q. Do you recall stating, [redacted], that you had an impression there was no consensus in how to define decentralization, but then you found a nice PETS paper by Carmolo -- Carmela Troncoso and others.

A. I don't recall the -- the exact

[redacted] - Highly Confidential

wording, sorry.

Q. Okay. Let's play it for you.

And I think the way we'll do this is -- because of the limitations here, I don't think we can put it on the screen.

Can we? You want to try?

MR. FORD: I could, but it would get rid of the Webex.

MS. ZORNBERG: Okay. Why don't you just take it over there and show Dr. [redacted]

We're going to -- Exhibit 33 is the clip that we'll show you from your -- from you [redacted]

(Recording played.)

A. You can stop it. Thank you. Very good. So...

Q. So let me -- let me put the question.

Having watched the video clip, do you agree that you said, on [redacted], I had an impression that there was no consensus in how do you define decentralization. Then I found a nice PETS paper by Carmela Troncoso and others.

And you go on.

Is that accurate?

A. That I say. I said that, yes.

Q. Okay. So, did you -- would you agree that, at a minimum, until you found the Carmela Troncoso paper, which you said occurred in June or July of 2021 -- before that time, you had the impression that there was no consensus in how to define decentralization?

A. I was -- that is fair.

That is fair --

Q. Okay.

A. -- to say. Yes.

Q. So, since finding the Troncoso paper in June or July of 2021, what have you done to determine whether others in the scientific community also adopt the Troncoso definition?

A. When I -- basically -- they don't need to adopt it. Again, we discuss that somebody can put the bar higher. When you put the bar higher, there are papers who require you, you -- a blockchain system to be called decentralized, to work with honest majority -- or something like that -- by allow -- allowing that a

minority of parties is considered Byzantine. So that's higher a bar.

So if you're allowing, you agree with me. So if you have a Troncoso definition, you would have these things.

But in order for Troncoso definition to be minimal, and I like that it's very permissive, it's very general, it admits a lot of systems so the not bar is not set high so it's debatable.

What I liked is that it puts the bar very low and goes into the essence of trust in a single authority. So I was -- and actually, that was my understanding.

If you ask me if I wrote the report without actually looking -- refreshing like what happened in last four years, this would be my definition. I would actually not put the bar higher because I don't think this is fair.

For example, I mention -- in the rest of the talk, I mention the four-node BFT protocol. This is a permission system that runs on four nodes and tolerates any malicious party among them.

[redacted] - Highly Confidential

It's a closed system with closed membership, and I was -- I think -- I still think it's fair to call it decentralized.

Q. Okay.

A. Now, when I saw -- when I looked at the Troncoso definition, I was like, Okay. So, I mean, before I looked at this from the -- from the formal perspective, I thought -- and it was open.

When I -- when I -- when I started writing about methodology, one possible outcome was that we still didn't come up to the minimal definition, as a scientific community. That could be one outcome.

So, while I was doing that -- and I didn't write the report, so that was one possible outcome.

Now, when I started diving into the literature, I saw that people had been looking into this, and the bar is actually set very low.

And -- yeah. And I couldn't find the definition, I couldn't find any definition which goes against -- that, again, would admit a system is decentralized if it does not satisfy

[redacted] - Highly Confidential

Troncoso definition.

So we are talking about a system in which there is single authority which is trusted by all, and you call that thing decentralized.

Q. What alternative definitions of decentralization, besides Troncoso, did you consider when you dove into this subject in the summer of 2021?

MR. SYLVESTER: Objection.

A. So, one of the papers that I cite in my report, which is the paper by Sai and others, it puts the bar high. So basically discusses decentralized systems, which require an honesty majority.

So basically with any honest majority, the system would still be called decentralized, which means that it tolerates dishonest minority. That puts the bar higher.

Q. Okay. If fewer than all participants in a system trust only one party, would you degree that's not centralized?

A. I think you are getting something wrong. At least in my -- from my brain. Can you repeat, please?

[redacted] - Highly Confidential

Q. If fewer than all participants -- sorry.

A. Yes.

Q. If fewer than all participants trust any one party, would you agree that's not centralized?

A. If I and all other participants, we trust the same party, would I agree that this is not centralized.

No?

Q. Rephrase it. Rephrase it.

A. I would say -- so the way I understand your system here is, driving, I would say it's centralized and not decentralized.

Q. Before you settled on the Troncoso definition in your report, with whom did you discuss the definition of decentralization?

MR. SYLVESTER: Objection.

A. I was reviewing and discussing with myself. I'm giving opinions, so I'm consulting the literature and -- yeah.

Q. Okay. Now, the Troncoso definition refers to decentralized distributed systems having multiple authorities that control

different system components.

A. Yes.

Q. Right?

Might those multiple authorities provide updates to the system components over time?

A. You mean can they change software on which they're running or --

Q. Yes.

A. They can.

Q. Can they improve the system components over time?

A. They can.

Q. Can the multiple authorities fix bugs in the system over time?

A. It depends on how the system -- if it's an open-source system and depending on the governance of that open-source project, they could. They -- in some cases, they might not be able to because they don't have the rights. It depends.

Q. Okay. Does the fact that multiple authorities can provide updates to the system over time affect whether the system is

decentralized?

A. Again, to -- in my report, and the way I think about this systems, you need to fix the software before you call it decentralized or not.

What these authorities in your example would be allowed to do is to change their own copy. If I am running a validator node on blockchain X, I could change my validator, and this is the -- so change and basically put any code that I want to run there. That I can do, even with the fixed code of others.

Then if I'm doing that, I'm trying to -- I'm considered Byzantine because I'm not playing by the set rules.

What's important is that that -- at that moment, the system maintains property not with respect to me because I violated the contracts by running the code that's -- that I'm not supposed to run, but I'm not supposed to influence others.

So you -- these nodes are usually caused the honest nodes. Does this answer your question?

[redacted] - Highly Confidential

Q. Not quite. But let me -- let me ask it again.

We agree that multiple authorities, in certain blockchain systems, can contribute to updates to the system that do get accepted into the protocol over time?

A. We need to fix -- again, we need to fix the software version, and then discuss its decentralization.

Once we do that, we need to exclude your case where you propagate updates to others, because we need to -- so we need to take a snapshot. You can make a decentralized system centralized by code changing. You can make a centralized system decentralized by code changing. You have to do both.

Q. You can do both?

A. You can do both.

Since we can do both, you need to take a snapshot in time, stop software changes that you propagate to others that others adopt, and basically focus on that particular software, and maybe changes -- if you're a Byzantine node untrusted by others, you are allowed to change

the -- your software that you are running however you want. But that's your software. You are not propagating the changes to others.

Q. Okay. Troncoso says that all parties must trust one authority --

A. It doesn't say that.

Q. -- for the -- well, I didn't finish the question.

A. I'm sorry.

Q. If a system is set -- in a centralized system, Troncoso says that all parties must trust one authority?

A. This is not -- so there must -- negation of the property will say there exist authority which is trusted by all.

Q. One authority trusted by all?

A. At least one.

Q. Okay. So my question is, if fewer than all parties trust any one authority, does that meet Troncoso's definition of decentralized?

A. No.

Q. Why not?

A. We used it in centralized. We just

negated the Troncoso defi-- the Troncoso says no parties fully trusted by all. If you have a party which is trusted by all, that negates the definition.

Are you -- do you agree?

Q. If fewer than all parties trust --

A. Fewer than all --

Q. -- one --

A. -- fewer than all parties. Okay.

Q. -- then do you agree that meets the Troncoso definition of decentralization?

A. If --

Q. I'm sorry, did you answer?

A. Yes, yes, yes, I'm thinking.

So you could build systems like that. That -- that could -- that could happen, yes. That could be allowed by the -- by the definition, yes.

Q. Okay.

All right. You mentioned the Sai paper. We've marked it as Exhibit 4.

(Sai paper was marked [redacted] Exhibit 4 for identification, as of this date.)

Q. And the Sai paper is a paper you

[redacted] - Highly Confidential

repeatedly recite -- repeatedly cite in your report as Reference Number 17 in your reference list. Right?

A. Yes.

Q. I'm going to refer to it, Exhibit 17 as the Sai paper, or Sai.

Are you aware that this is a peer-reviewed -- this paper was published in a peer-reviewed academic journal?

MR. SYLVESTER: Sorry, Lisa, the Sai paper that I'm looking at is marked [redacted] 4.

MS. ZORNBERG: Oh, thank you for the correction. It's Reference Number 17 in Dr. [redacted] report, but we're marking it here as Exhibit [redacted] 4. Thank you. Thank you.

Q. Okay.

Looking at Exhibit 4, Dr. [redacted] are you aware that this paper was published in a peer-reviewed academic journal?

A. Yes, I am.

Q. Okay. And the purpose of the Sai paper was to conduct a systematic review of academic literature that discussed

[redacted] - Highly Confidential

decentralization to --

A. In public block-- blockchain systems.

Q. In public blockchain systems.

A. As the name says, yes.

Q. Okay. And in the abstract of paper, it references that Sai reviewed 89 research papers published between 2009 and 2019, to arrive at a taxonomy of centralization.

MR. SYLVESTER: And, [redacted] if you don't recall, take your time to take a look at the paper to answer her question.

A. Yes.

I -- at some point, I need to go to the toilet.

Q. Then why don't we take a break now?

A. Is this the right time.

Q. Yeah, it's fine. It's totally fine.

A. Okay. Thank you.

THE VIDEOGRAPHER: The time is 10:52 a.m. We're going off the record.

(Recess from 10:52 to 11:10.)

THE VIDEOGRAPHER: It is 11:10 a.m. We are back on the record.

Q. Dr. [redacted] a little while ago we

were speaking about permissioned and permissionless blockchain systems. What is a permissioned blockchain system?

A. Permissioned blockchain system is, in a nutshell, a system in which you cannot join without permission of some entity. This can be a centralized entity. This can be a decentralized entity, like current members in the system could vote to admit another one into the system and so on.

As opposed to that in permissionless systems, this permission is not necessary. So you would just -- if you want to run a validator in a -- in some kind of blockchain effort, you would download the code. You would join the game, start validating transactions.

Q. You said earlier that a -- a permissioned system can be either centralized or decentralized. Correct?

A. Yes.

Q. Can you give an example of a decentralized permission system?

A. So we could -- if you have four validator nodes, and they run a consensus

protocol and they tolerate any malicious action of any one of them. So usually -- I mean, depending on the failure thresholds, this number of Byzantine nodes that tolerate is less than one-third of nodes, sometimes one-half of nodes. And usually in the literature, that depends -- so this is the best you can do.

And that distinction, whether it's one or the other, it depends on network assumptions, how timely is the network, which means if I send a message to you, is it delivered in, like, limited amount of time? So does every message, for example, take up to two seconds, not more, for me to reach you? If it takes more and albeit a long time -- we talk about asynchronous network. So if network is asynchronous or synchronous, these bounds --

Q. If a network?

A. Is asynchronous -- asynchronous or synchronous --

Q. I don't know that word.

A. If it takes unbounded amount of -- so I send -- so my computer is sending --

THE COURT REPORTER: I'm not hearing

your words now.

THE WITNESS: Okay. Sorry.

THE COURT REPORTER: If it takes what?

A. If it takes unbounded amount of time and for -- in the worst case, for my message to reach to you, which means that probably on the network there are some network outages, network partitions, so maybe there are, like, you know, cable under water, cable is broken down and somebody needs to repair it, and I keep trying to reach you and only eventually my message reaches. And this time period is unbounded. We are talking about asynchronous network.

Q. Can you sell that word?

A. Asynchronous.

Q. Spell that.

A. A, like letter A, synchronous.

Q. Asynchronous?

A. Yes, asynchronous. Yes.

Q. Okay. Thank you.

A. Sorry. Anyways, so depending on the underlying network assumptions, Byzantine fault tolerance protocol, which can be used in the permission blockchain systems, tolerates less

than one-third of the total number of nodes or less than one-half.

This can be smaller. This can be less than one-fifth or so on.

But these are usual bounds that appear. So if I have four nodes, four validator nodes, I could come up with a -- Byzantine Fault-Tolerant protocol that tolerates to certain extent; and there are technical details what the certain extent means, this asynchronous network.

And it tolerates any Byzantine behavior of any one of them. But if two of them misbehave, they could break the safety and liveness properties.

So why is this decentralized? Because we could have four nodes and not any one is trusted by all. Actually, not any one is able to subvert the key proprietors of the system. Then basically, this would qualify under Troncoso definition as a decentralized network.

Q. Okay.

A. So in that sense, the Troncoso definition sets the bar pretty low. This is

what I mentioned before.

Q. Okay. So I would like you to take a look at Exhibit 4, which is the Sai paper.

A. Yes.

Q. Does the Sai paper cite to the Troncoso definition of decentralization that you adopted in your report?

A. It does not. What it does, it provides a stronger definition of decentralization.

Q. Okay. Is it fair to say that Sai surveyed 89 research papers over a ten-year period, to address the taxonomy of centralization, and it did not cite Troncoso, among those 89 research papers?

A. It is fair to say that they did it, yes.

Q. And in your own published writings before 2021, have you ever cited to the Troncoso paper?

A. I did not.

Q. I want to direct your attention to the abstract on the first page, of the Sai report.

Around midway down, where it -- the

[redacted] - Highly Confidential

Sai paper states, quote, Our study contributes to the existing body of knowledge by highlighting the multiple definitions and measurements of centralization in the literature.

Closed quote.

Do you see that?

A. Our study contributes to the existing body --

Yes.

Q. Okay. The Sai paper was published in 2021 --

A. Uh-huh.

Q. -- right?

A. Yes.

Q. Yes? And do you agree that Sai, at least, states that the literature includes multiple definitions and measurements of centralization?

A. By highlighting the multiple definitions and measurements of centralizations, yes, he says that in the abstract.

Q. Do you agree that as of when the Sai paper was published, there were multiple

definitions and measurements of centralization in the scientific literature?

A. Clearly, there are still even after. If you take Sai paper, it proposes a different definition of centralization than Troncoso. So the answer is yes.

Q. Okay.

I would like to direct you to your report to the top of page 5.

And the top bullet, you wrote, quote, I adopt the basic definition of a decentralized system as defined by Troncoso, et al.

Closed quote.

Did I read that correctly?

A. Yes.

Q. Was it your intention in the report to present the Troncoso definition of decentralization as the authoritative definition in the scientific community?

A. I -- my intention was to refer to it as I did, as a basic definition of a decentralized system.

Q. Why --

A. In more mathematical terms, this

could -- at some point I call it minimal. I refer to it as minimal. And you can think of it as necessary.

In mathematical terms, necessary and sufficient is -- it's necessary. I'm adopting it as a necessary definition.

Q. Why did you describe it as "the basic definition," instead of "a basic definition"?

A. Can we attribute it to my English? But -- English is not my first language. I normally have issues with -- with these things.

Q. Did you mean to suggest in your report that the Troncoso definition is the only basic definition of a decentralized system?

A. Again, it's -- what I think is that it's necessary. If you don't -- when I say "basic," what I mean is necessary. If a system does not satisfy the -- this definition, according to my understanding, my expertise, my understanding of this field, and backed by all the evidence that's written here, including the Troncoso definition, I would say that this, such system could not be qualified as decentralized and, hence, it's centralized.

[redacted] - Highly Confidential

Q. But would you agree -- would you agree, Dr. [redacted] that there are other definitions of decentralized systems that you can find in the scientific literature?

A. You can -- one can find different definitions of decentralization in the scientific literature, none of which, to my understanding, would admit a system is decentralized, if it follows Troncoso definition. Do you see the -- where I'm going with "basic" and "minimal"?

Q. So your position is that there is no definition in the scientific literature of "decentralization" that doesn't have the Troncoso definition as a basic minimum?

A. To my understanding, there is no definition of decentralization. And certainly I didn't see any -- and I doubt it exists -- that would admit a system is decentralized if it doesn't satisfy Troncoso definition.

Q. Did you consider the definition of decentralization provided in a 2020 paper by Keke Wu, spelled K-E-K-E, W-U, title "A Coefficient of Variation Method to Measure the

Extents of Decentralization for Bitcoin and Ethereum Networks"?

A. Do you have that paper as a exhibit?

Q. No, not right now.

But is that -- are you familiar with that paper?

A. I'm familiar with that paper, yes.

Q. When did you review it?

A. I reviewed it after Adriaens' rebuttal.

Q. Okay. So I'll just read you one sentence from the paper where it Wu wrote that in blockchain systems, and I'll quote it, quote, Decentralization means that no single individual can destroy transactions in the network, and any transaction request requires the consensus of most participants.

Closed quote.

A. Do you have that paper in front of yourself?

Q. I don't have it here right now. But --

A. Okay. So this is the thing. This is what Adriaens points out in his rebuttal.

[redacted] - Highly Confidential

Unfortunately, he skips -- and this is what Adriaens does in his rebuttal. He takes things out of the context.

That very same paper. Section 2, if I'm recalling like -- don't take my -- because I don't have it in my head.

But Section 2, Subsection B, it opens with the definition of "decentralized systems," which is the same as Troncoso definition.

Q. Okay.

A. We can have -- so -- I mean, I don't have the paper before me.

But what it does, it discusses -- so it cites the early work of Baran from 1960s and it points out to Vitalik Buterin's blog post to basically define in the same way -- I'm not saying word for word, but almost the same words because it talks about single authorities fully trusted by all. As Troncoso does.

Adriaens doesn't point --

Q. What are --

A. Adriaens doesn't point that out in his report. And he skips, so that's not a definition. So that particular paper to which

you are referring to opens the definition of "decentralization" in the decentralization section by having the same wording or almost the same exact wording as Troncoso.

Q. All right. Let me direct you back to the top of page 5 of your report.

A. Yes.

Q. So in the first bullet which we looked at, you say, I first adopt the basic definition of a decentralized system as defined by Troncoso.

And then in the very next bullet, you wrote, quote, I then refined this basic definition.

Closed quote.

And it goes on.

A. Yes.

Q. Why did you see a need to refine Troncoso's definition of "decentralization"?

A. That's -- that's a good point. So, for example, Sai paper and multiple other papers, they would try to understand, which system is more centralized and which system is more decentralized. They most often focus on

bitcoin and Ethereum more.

So if you look at bitcoin and Ethereum, the -- the way I treated them in my report, they would both pass Troncoso definition.

But still, people would be discussing which one is more decentralized than the other.

So if you want, with this methodology, there is one definition which sets the bar very low. And I'm actually surprised, if I may make a comment, that we are discussing this because the aspiration of Ripple consensus, the way it was written, is to be a Byzantine Fault-Tolerant protocol and to actually pass the Troncoso definition easily. It's just that it doesn't. So I'm surprised that we are questioning --

Q. I'm sorry. I didn't -- I didn't catch what you said. To pass the Troncoso test, you said, is easy?

A. It would be if Ripple was actually a-- Byzantine Fault-Tolerant protocol that tolerates Byzantine -- Byzantine fault of any component in that system, it would pass Troncoso definition.

It's just that it doesn't. It's

marketed as such. But it basically hides extreme complexity in the dUNL membership series. So that's -- if you want, when you design these protocols, this is the most challenging part. And you're hiding it in a -- in the -- you're hiding the complexity by having the trusted service that ships the UNL others.

Q. Is it -- is it your position, Dr. [redacted] that the XRP Ledger fails to meet the Troncoso test because of the way the dUNL, what you call the dUNL, operates?

A. This is what I point -- this is the main reason.

Even with that fixed, there could be other reasons. Other reasons are pointed in my Appendix B, which are not necessary for my opinion, as I stated my report, because of the main problem is how dUNL operates.

Q. Okay. Do you consider decentralization to be binary such that a system is either completely decentralized or completely centralized?

A. I -- in my methodology and in this -- assuming that we would find a definition that

admits a system is decentralized, so this is where Troncoso definition comes. I think this is the bar which says this is either centralized or some people might call it still centralized or decentralized if you pass that filter of Troncoso, so you are satisfying Troncoso definition.

I would call it decentralized -- being very generous, I would call it decentralized in this methodology. We'd call it decentralized. Then probably you could find other expert who would say, No. No. No. Wait, wait. Wait. It's not sufficient that it passes Troncoso definition. Let's still see. And there are these different aspects of -- that I discuss in my report, and they -- the others discuss.

Q. So why did you feel the need to refine Troncoso's definition of decentralization?

A. This is mostly -- I was asked to opine on bitcoin and Ethereum. So, you know, if you have bitcoin and Ethereum, you -- there are certain aspects of them that influence, like this one is more decentralized, and this one is less decentralized. They are decentralized,

[redacted] - Highly Confidential

according to Troncoso definition.

And the way the -- not only because of Troncoso definition, because the way current system -- current software operates and current circumstances in the world in which the network operates, they allow them to pass Troncoso definition.

Now, it's also when you build a methodology, it's supposed to be able to distinguish different aspects of decentralization. As they are presented in the literature, you will see that my methodology that I adopt very much looks like different measurements and aspects of centralization that Sai has.

To be able to evaluate once you pass Troncoso definition, which system is more decentralized than the other.

Q. So do I understand correctly, you're saying that you view the Troncoso definition as the bare-minimum definition for decentralization; but beyond that, decentralization can move along a continuum?

A. That's a fair way to put it, yes.

Q. Okay. And so would you agree decentralization in a blockchain system can change over time?

A. It can certainly change with the change in the software. We discussed this already. That's certainly the case. Yes.

It doesn't depending only on changes in software but changes in the whole circumstances of the Newark and et cetera. It can change in time.

Q. What factors could contribute to a blockchain system becoming more centralized over time?

A. Convergence to -- again, in the -- in the world of Troncoso definition, if this is the minimum bar, you want to stay away from the world in which a single authority needs to be trusted in order for other entities in the systems, other authorities or participants in the system to maintain the desired properties of the system. Desired properties in my report are referred as safety and liveness and usually in distributed computing.

Q. Okay.

[redacted] - Highly Confidential

THE COURT REPORTER: Usually what?

A. Usually in distributed computing.

Q. What factors could contribute to a blockchain system becoming more decentralized over time?

A. So this -- what can contribute is ensuring that there is no such part that controls vital parts of the system. And you usually do it by -- one way to do it, I -- rather than usually. One way to do it is to let go of power, let go of any specific thing that this entity is doing that others are not. Right?

Q. Uh-huh.

A. So example would be, one of the steps -- I'm not saying if -- if XRP Ledger does it, but one the steps toward such a world would be removing validator list sites completely from the code. That's an example. I'm not saying that's sufficient, but that's a step there. Because suddenly, you would go to the world in which no one is really favored over the other, by its own inclusion to DNLs, you're removing that.

[redacted] - Highly Confidential

Q. In your view, does a blockchain system that includes -- let me rephrase.

Is it your position that by including any validator list in the rippled code, that automatically renders the ledger centralized?

A. I didn't say that.

Q. So explain what you're saying. Can -- can the rippled code include any validator list and still be decentralized?

MR. SYLVESTER: Objection.

A. I would need more time to -- you're speculating on -- on possible future.

So we are speculating on changes of the code that happened, and I would need to review them carefully.

Q. I'm not -- I'm not sure -- maybe I -- I wasn't clear in my question.

Even under the version of the code that you reviewed where there's -- I'm asking you, ideologically, do you have a belief that by having any validator list in the rippled code, that mere fact renders the ledger decentralized?

MR. SYLVESTER: Objection.

A. Again, I'm not saying that. What I

said is, you're asking to -- me to opine on something that I didn't write in my report.

Whether -- I believe it is possible -- let me put it this way. I believe it is possible to have similar concepts that are -- that the designers of the protocol tried to express but just implemented in a different way, which would yield a decentralized system.

Does that help?

Q. Your report does talk about the fact that the rippled code has a validator list in it, a UNL list in it, correct?

A. Yes.

Q. And I thought the central view expressed in your report is that it's the existence of that Ripple-published UNL that, in your view, renders the ledger centralized.

MR. SYLVESTER: Objection.

A. No, it is not. This is not what I wrote.

Q. So then explain.

A. What is rendered centralized is the ability of a validator list site, of the validator list site as of 1.7.3, to serve

[redacted] - Highly Confidential

different UNLs to different. So if -- it's -- it needs to be trusted not to do what I'm just describing. If it does serve different UNLs completely -- let's say completely different UNLs, to completely different nodes, what it does, it puts these validators that did get different list out of consensus. They cannot reach consensus without one another.

I mean, they could. But, like, the chances that they do not are really real. So this is what this -- so you have this entity. And it's a special entity because it's designated in the code. The code designates this special entity.

It's like, you know, there is a special component in the system that has the power to tell others what a UNL does in Ripple code. It tells validators, listen to these validators which are on this you list and, basically, try to understand how many of those validators are telling you something.

And if all -- not overwhelming, but a large majority of these validators tells you something, then do that. So now if you have the

power of the entity, which can serve this list to validators, that's -- that's a -- that's a large power. And the way the protocol was designed, it requires trust into this part.

Q. Okay. In the context of an XRP -- of the XRP Ledger, what is a Unique Node List?

A. The Unique Node List is the -- the list of validators that validate the transaction. So basically, they communicate with the given validators. So each validator has locally its own UNL, which is the list of validators, that it considers. So as it accepts messages from different validators, essentially, it looks only the validators at its own UNL to establish which ledger should be -- a ledger means the block -- XRP Ledger should be added to the blockchain.

Q. What did you do in this case to research your understanding of a Unique Node List?

A. I reviewed the code. I read the -- the Chase MacBrough paper. I made sure that my understanding of rippled code matches the explanations in Chase MacBrough paper. And I

looked at critical parts of the code, notably at the quorum sizes, and -- basically how one particular -- how particular parts of -- of the protocol work. And this is what I did, yes.

Q. Okay. Let me direct you to page 6 of your report.

A. Uh-huh.

Q. Under number two at the top of the page, you write that Ripple controls the web domain which hosts the service that provides the dUNL to the XRP Ledger participants.

Correct?

A. Correct.

Q. What is the dUNL, as you use that term in your report?

A. So the one item before that, so page 6, Item 1, says, Participants required for the proper operation of the system, in brackets, nodes, are curated, under quotation marks, by Ripple for inclusion into a specialist called the dUNL, which is to be understood as default Unique Node List.

So dUNL refers to the validators that are included by Ripple in the special list that

[redacted] - Highly Confidential

is published from the validator list site, at vl.ripple.com.

Q. Okay. Now, on page 6, you write that your -- the statement that Ripple controls the web domain which hosts the service that provides the dUNL to XRP Ledger participants is true as of the latest release of the XRP Ledger software referred to as rippled Version 1.7.3. Right?

A. Uh-huh.

Yes.

Q. But, in fact, that's only true as you note in number 3, For participants who use the unmodified code of rippled Version 1.7.3.

Right?

A. Yes.

MR. SYLVESTER: Objection.

Q. You didn't consider any other version of rippled other than Version 1.7.3 in reaching the opinions in your report. Correct?

A. As we discussed, so there is -- you need to fix the software in order to understand what it does. So I was fixing the software to default Version Ripple dot -- this 1.7.3.

Q. Okay.

[redacted] - Highly Confidential

Okay. Let me also direct you now to the bottom of page 20 of your report.

And this is the paragraph just before the bottom where you write that, quote, The software fetches the latest published recommended validator lists from the validator list site at regular intervals.

Closed quote.

You see that?

A. Yes.

Q. For that statement, you rely on the validator site .h file that's part of rippled?

A. Yes.

Q. Okay. I'm going to show you now what's marked as [redacted] 14.

(Report Citation was marked [redacted] Exhibit 14 for identification, as of this date.)

Q. Okay. My question to you is whether you recognize this document.

MR. SYLVESTER: This has several pages, so take your time to take a look at it.

(Witness reviewing document.)

Q. Okay. Dr. [redacted] is Exhibit 14

the -- the same thing that you referred to in your report as the citation for the sentence that the software fetches the latest recommended validator list?

A. It appears to be, yes.

Q. What role does the validator site .h file play in the rippled code?

A. So as the comment says, This class manages set of configured remote sites used to fetch the latest published, recommended validator lists.

Q. Where are you reading from?

A. Lines 43 and 44.

Q. Okay. Can you point to me the -- the line of the code that you're looking at for that portion of your opinion?

A. I'm looking at lines 43 and 44, comments what the validators list -- validator site does.

Q. Okay. And what role does line 46 play?

A. This is a comment.

Q. Also a comment.

Let me direct your attention to

line 24.

That code -- what is -- do you understand what line 24 is?

A. It includes validator list .h into this C file, yes.

Q. Did you review that file, validator list .h, when preparing your report?

A. I do not recall for certain. I might have. I might have not.

Q. Okay. Let me show it to you. It's marked as Exhibit 15.

(Document was marked [redacted] Exhibit 15 for identification, as of this date.)

Q. And you should, you know, please take a moment to review it and let me know when you're ready. I'll let you know that the section that I'm going to direct your attention to starts on line 375.

(Witness reviewing document.)

Q. Dr. [redacted] do you recall reviewing this document in preparing your report?

A. I -- I think I saw this document. Yes.

Q. When role does the ripple -- excuse

me. Let me rephrase.

What role does the validator list .h file play in the rippled code?

A. I would need more time to tell you exactly the answer to that question.

Q. Are you sure you've seen this document before today --

A. I'm not sure.

Q. -- Exhibit --

A. I think I did. I cannot vouch I did.

Q. -- Exhibit 15?

A. Yes. I cannot vouch I did.

Q. Well, let me direct you specifically to lines 375 and 376.

A. Yes.

Q. And those state, quote, Apply multiple published lists of public keys, then broadcast it to all peers that have not seen it or sent it.

Closed quote.

Did you review these comment lines in preparing your report?

MR. SYLVESTER: Objection. Asked and answered.

[redacted] - Highly Confidential

Q. You can answer.

Dr. [redacted]

A. I don't -- I don't recall...

I don't recall evaluating these -- these particular lines of code.

Q. Okay. So you don't recall looking at the comment lines in 375 and 376.

Correct?

A. Yes.

Q. Okay. So let me direct your attention now to lines 404 through 413.

A. Uh-huh.

Q. Did you review those lines of code in preparing your report?

MR. SYLVESTER: Objection.

A. I stated in my report which lines of -- basically which lines of code I reviewed in my report.

So --

Q. Where do you do that?

A. Basically, when I say, According to this line and that line, basically, these are -- this is where I do it.

Q. Can you -- my question is, did you

[redacted] - Highly Confidential

review lines of code 404 through 413 of Exhibit 15, in preparing your report?

A. I do not recall doing that.

Q. Did you -- did you review any part of the rippled code other than the -- than the portions expressly cited in your report?

A. I did.

Q. Okay. What do lines 404 through 413 of the code in Exhibit 15 mean?

A. To give you the full answer to that, I would need to review this in more details.

Q. Do -- take a look at those lines of code. Do they mean that the node will broadcast its trusted Unique Node List to peers that have not seen or sent it?

MR. SYLVESTER: Objection. Asked and answered.

A. This particular code -- so this particular signature doesn't say what happens. It's just a signature of a function. So it doesn't say what happens.

It's called in a certain way, but implementation is missing.

Q. I'm sorry. I didn't follow that

answer.

A. The answer is, no, it does not.

Q. Your testimony is it doesn't mean that the node will broadcast its trusted unique node --

A. It has a signature -- it has a signature of the function. It misses the implementation of the function.

Q. Did you take this code into account in forming your opinions in this case.

A. So this particular signature of the function, I didn't take into account.

Q. Okay. So backing off from the code, let's assume for a moment that the rippled code, provides for peer-to-peer sharing of UNLs.

A. Uh-huh.

Q. First, do you know if that's true or not?

A. I know that the -- the -- the -- the UNLs are rebroadcasted. That I know. So if you call this peer-to-peer sharing of UNLs, this is possible, yes.

Q. Do you discuss that manner of sharing UNLs in your -- anywhere in your report?

[redacted] - Highly Confidential

A. I do not.

Q. Why not?

A. It is not relevant to the need that you trust -- need to trust this particular issuer of the UNL.

Q. Why is peer-to-peer sharing with UNLs irrelevant, in your view?

A. So what's the sharing going to achieve? Is it going to achieve that we agree on the same -- if it combines, even, the UNLs, and sends it to all, there needs to be a consensus protocol there, which make sure that we look at the same view of a UNL. That's the first thing.

The other thing I'm pointing out in my report is that the UNLs need not to contain malicious nodes. So you need to trust that the UNL is sure even. If it doesn't serve different UNLs to different nodes, you need to trust it not to include malicious nodes.

Q. Okay.

A. So the trust in the UNL remains. The -- my conclusion doesn't necessarily -- doesn't depend on the outcome of what the

[redacted] - Highly Confidential

mixing -- potential mixing of UNL is trying to achieve.

Q. Let me focus back on the same sentence in paragraph -- on page 20, where you cite -- you stated that the software fetches the latest published, recommended validator list from the validator list site at regular intervals.

A. Yes.

Q. If the rippled code provides for peer-to-peer sharing of UNLs, would you agree that that's another way that nodes might receive an updated UNL that does not require loading the validator list site?

MR. SYLVESTER: Objection.

A. So the -- the source of the file remains the same. You can get it directly from the source or not. It is authenticated by the source, and the source remains the same. So if you get it from somebody else, you're getting the same information, that this validator list site published.

Q. Okay. Can you -- I want to know if you're able to answer this question yes or no.

Can you answer yes or no: Would

peer-to-peer sharing be another way that nodes might receive an updated UNL that does not require loading the validator list site?

A. It might be another way to do that. Yes.

Q. Okay.

A. It's a -- yeah. It's also not very -- not necessarily a reliable way, but it's one way to do it, yes.

Q. Okay. In -- in -- in preparing your report in this case, did you consider the impact of peer-to-peer sharing of UNLs on your opinions?

MR. SYLVESTER: Objection.

A. What I considered in my -- in my report, I presented it. And yes. So --

Q. Well, I'm not sure I understand what you're saying yes to. Earlier you acknowledged that your report does not address peer-to-peer sharing. Correct?

A. Yes -- well, I was aware that validators, if they download the list, they can forward it to other nodes.

Q. Did you consider the impact of

[redacted] - Highly Confidential

peer-to-peer sharing of UNLs on the opinions that you've included in your report?

MR. SYLVESTER: Objection.

A. I mentioned it, so I was aware that this is happening. And, again, this -- to my understanding of the system, it doesn't impact my conclusions.

Q. So does the operation of peer-to-peer sharing of UNLs affect your contention that if a corrupted dUNL publisher served totally different UNLs to different validators, that would prevent the correct operation of the XRP Ledger?

A. If it happens, and you have a protocol that exchanges the UNLs among nodes, you will still need to prove that the UNLs exchanged -- actually, somehow magically combines into the same UNL. Because with the -- without sufficient overlap, and there is no point in the code that suggests that.

Q. But that -- you're talking now -- you're talking about other conditions that might need to be met. I'm -- I'm just restricting myself to the -- your opinion that you share on

page 22 that -- where you wrote that if a corrupted dUNL publisher -- a corrupt -- I'm sorry. Let me make sure you're -- let me direct your attention to page 22 in the middle.

Do you see your sentence where you write, quote, As a simple example, a corrupted dUNL publisher may serve totally different UNLs, i.e., 0 percent intersection, to different validators, preventing the corrupt -- the correct operation of the ledger.

Do you see that?

A. I see that.

Q. Does the operation of peer-to-peer sharing of UNLs affect that contention?

A. It does not, because the -- still, the publisher can serve different UNLs to different validators without the necessary intersection among the UNLs. So my sentence would stay as it's written.

Q. Okay. If the publisher did that, served a corrupted -- hold on. Restate.

If the publisher did that, would peer-to-peer sharing render that action ineffective?

[redacted] - Highly Confidential

MR. SYLVESTER: Objection.

A. How do you define "ineffective"?

Q. Could the ledger still make forward progress and operate?

MR. SYLVESTER: Objection.

A. Yeah. To my -- to my best understanding, it would not.

Q. It would not operate.

A. It would -- it would be possible that it -- that it does not operate. It would not guarantee that the problem is fixed.

Q. Could it still operate? I'm trying to understand. Are you saying that, if there's a corrupted dUNL publisher, even if UNLs are shared through peer to peer, that's it; the ledger would stop operating?

A. So when you say "could," even if there is no peer-to-peer sharing, even if there is -- Byzantine dUNL publisher serving lists to different nodes, completely different validator lists, and they operate on validator lists, there is a possibility that the ledger continues even though. So basically this is where you agree on the same -- on the -- on the -- on the

same information.

Q. Okay. So it's still -- there is still a possibility, that the ledger could continue to function.

MR. SYLVESTER: Objection.

A. There is always possibility that it would. There is possibility that it wouldn't.

Q. Okay. So if there's a corrupted dUNL publisher, your position is that it's possible the ledger could continue to function, or it's possible that it wouldn't?

A. It's probable that it wouldn't.

Q. You're not saying that for a hundred percent, correct?

A. I'm not saying --

MR. SYLVESTER: Objection.

A. To my understanding of the -- of the opinion, I would need more time to understand it.

Q. Okay.

A. Is it 100 percent that it stops, or is it just probable that it stops.

Q. Why would you need more time? Why did your work on the case to date not sufficiently

allow you to answer that question with a definitive answer yes or no?

MR. SYLVESTER: Objection.

A. I did this work three months ago. So I spent the time I spent. It's a complex system which has different properties to it. And I don't necessarily recall all what I learned then about the system. Unfortunately, my understanding of the system today is not at the -- as detailed level as I understood then. That would be the best answer I could give.

Q. Okay. All right. Turning to a different subject.

Is it -- I think we've talked about this, but I just want to make sure. Is it possible, in your view, that a blockchain system could start out as centralized and become decentralized over time, with changes?

A. I believe this is possible.

Q. Are you aware of any accepted scientific tests for determining the moment in time when a blockchain system goes from centralized to decentralized?

MR. SYLVESTER: Objection.

[redacted] - Highly Confidential

A. If we adopt the approach that I'm suggesting, with my approach, so basically that in each point of time when software changes and the circumstances changes, you validate a system. Then if you applied this fine granularity, you could come to the point where it happens. It could go back and forth probably. It could be decentralized and centralized again and so on.

Q. But my question is if you're aware -- I understand we'll talk about your methodology that you've proposed here. But are you aware of any generally accepted scientific test for determining that moment in time when a blockchain system goes from centralized to decentralized or decentralized to centralized?

A. So many in the bitcoin and material world, many papers talk about, for example, centralization in the mining pools. So that's a fairly subjective -- subjective -- maybe debatable assumption, because it's -- it assumes, so that assumption assumes that the mining pool operator controls all the nodes in the mining pool.

And then -- so some authors analyze the mining power concentration in bitcoin and Ethereum. And they would say this many mining pools, if they come together and combine their hash power, they would go over 51 percent.

And at that point, I saw some basically -- you know, I'm pretty -- I'm aware that there is some analysis, at which points this number shrinks, for example, from four mining pools to three mining pools to five mining pools and maybe to one mining pool. And at that point of time, blockchain system could be so.

There is a reason to call it centralized, because there is still not -- again, coming back to our probability versus possibility, it's possible. But let's say if it's possible that the violation happens, if you're conservative, you would assume that it could actually happen.

Q. Okay. You were just talking about concentration in mining pools, correct?

A. Yes.

Q. Would you agree that's one aspect of a

decentralized system?

Or let me -- that's one -- one aspect to consider, of whether a blockchain system is decentralized?

A. The consensus protocol is the most important one. So in the Sai paper that you -- that you submitted as Exhibit [redacted] 4, Sai actually for the different aspects of decentralization, they perform the interview with the experts. Like, do you believe -- asking them, Okay, we have these different aspects of decentralization, and do you believe this is relevant or not.

So if you look at --

Q. I'm going to -- I'm going to --

A. Yes.

Q. I don't think you're answering my question, so I want to rephrase it. And I want to try to ask you to focus on the questions that I'm asking.

A. Uh-huh.

Q. So, first of all, one question I asked, was, are you aware of any scientific test for determining the moment in time when a

blockchain system goes from centralized to decentralized?

MR. SYLVESTER: Objection.

A. I believe I described you such a moment. It's the moment -- for example, in the case of proof-of-work mining pools, it's the moment where the one mining pool goes beyond 51 percent of power. I tried this convey this is one possible test. So I'm aware of such a scientific, accepted test that you can verify.

Q. So in the comparison you just gave with a 51 percent attack, isn't that example of a system going from centralized to -- from decentralized to centralized?

A. It's the same the other way around. If you go from -- if you had a snapshot in time where one -- one mining pool controlled 51 percent of power and you go to the world where two mining pools actually have it or more, you would go from centralization to decentralization.

Q. Outside of proof-of-work consensus protocols, are you aware of any accepted test for determining the moment when a blockchain

system goes from centralized to decentralized?

A. I would say this is the moment where a system passes Troncoso test.

Q. And is the Troncoso test the accepted scientific test?

A. I would say, if we -- so we argue -- we discussed this for one hour before. So we discuss the minimality of the Troncoso definition.

And, what do you mean by "accepted"? So accepted by whom?

Q. Well, as of October 6, 2021, you -- you spoke about there being no consensus until you saw the Troncoso test.

A. I'm speaking --

MR. SYLVESTER: Objection.

A. I'm speaking about past.

Q. Okay. Do you think that the whole scientific community has accepted the Troncoso test as the accepted test for determining the moment when a blockchain system is decentralized?

A. I will repeat again what I said before. So, I'm not aware of any definition of

[redacted] - Highly Confidential

decentralization that would go against Troncoso definition and that would still call the system decentralized.

If you ask me that question, I can only repeat what I said before, is that I think there is a consensus on this minimal and necessary definition.

Q. Okay.

All right. I'm going to show you another exhibit, Exhibit 5.

(Position paper [redacted] was marked Exhibit 5 for identification, as of this date.)

Q. Do you recognize this document?

A. I do.

Q. What is it?

A. This is my invited paper [redacted] peer reviewed by [redacted], editor of the [redacted], journal to which this paper

[redacted] - Highly Confidential

was invited.

My invitation was done by [redacted], who is another editor of the journal. They invited me to give my opinion on decentralized computing as an expert in the field.

Q. Okay. Now, is Exhibit 5 what -- the same article that you cite to in your references in your report as Reference Number 22?

A. Yes, it is.

I believe it is, so I should look at all pages, but it appears to be, yes.

Q. At the time that you issued your report in this case on October 4, 2021, had this paper, Exhibit 5, been published yet?

A. It was accepted by the -- by the reviewers, which are the editors of the -- of the journal, which is why I cite it as -- under the name of [redacted]. So at that very moment it was peer reviewed, and it was pending publication; it was in the process of publication.

And I made it available on my website

[redacted] - Highly Confidential

as a preprint, which we usually do when -- when we have this like small window between acceptance and publication, this is what we do.

Q. Okay. I'm going to refer to Exhibit 5, using your term, position paper. I'm going to refer to it as your position paper.

A. Uh-huh.

Q. Is it -- is it your understanding that the [redacted] is an academic journal?

A. Yes, it is.

Q. Okay. Is it -- does it represent itself, as a peer-reviewed publication?

A. This is a peer-reviewed publication. There are contributed publications -- I believe there are contributed publications which are not peer-reviewed. And this one is.

Q. When you're saying "this one is," you mean your article was peer-reviewed?

A. My article is, yes.

Q. And specifically it was peer-reviewed by [redacted]?

A. Professor [redacted], alumnus of [redacted] and professor at [redacted]

[redacted] - Highly Confidential

Q. Did anyone besides [redacted] peer review this paper?

A. So I know it was read, although no particular feedback was provided, except as high-level comments by [redacted], another editor, Professor [redacted], who is another editor of the journal.

Q. Okay. Were you the only author of your position paper?

A. I am.

Q. So, when your position paper uses the term "we," is that a writing convention, the royal we, and you're really referring to I, meaning yourself?

A. Yes, this is -- this is normal, and it basically downplays your ego, and that's an accepted approach in scientific writing. You don't want to bother the reviewer by saying I, I, I, I, and it feels better that -- at least the way I was educated as a scientist, to write we. That's a common -- commonplace.

Q. Okay. Let me direct your attention to page [redacted] of Exhibit 5.

[redacted] - Highly Confidential

In the abstract --

A. Yes.

Q. -- at the top.

Do you see in the second paragraph, you wrote, quote, [redacted].

A. I do.

Q. Okay.

So, as of [redacted], were you acknowledging in this position paper that there are existing definitions, plural, for decentralized systems?

MR. SYLVESTER: Objection.

A. I do not.

Q. What did you mean by [redacted]?

A. So, we start by releasing the definition of decentralized systems, briefly surveying the literature on taxonomy and different facets --

Q. Really, you may have to slow down for the court reporter.

THE COURT REPORTER: I would

[redacted] - Highly Confidential

appreciate that. Yes.

THE WITNESS: Sorry.

A. Second paragraph, page [redacted]

[redacted]

Q. So, are you saying that when you wrote, [redacted], you didn't mean existing definitions of decentralized systems?

A. Concretely including this complements the definition -- the distinction between permissionless and permission systems.

As we discussed today, I believe, and the methodology that I adopt supports, that both

permission and permissionless system can be decentralized.

So what this particular inclusiveness does, it -- you know, what I say in the paper is -- and also in the report -- are permissionless system truly permissionless? Or they basically allow certain players to join the game in a special role? Or are -- they are permissionless in the sense they don't require -- basically they give equal opportunities, which is the same term, the -- the -- the term that I use for inclusiveness.

Q. Okay.

A. And in which case they would be called truly permissionless.

Q. So --

A. So that's my attempt and contribution to the -- contribution to discern -- for example, it's very important if you discern proof-of-stake and proof-of-work systems.

It's applicable -- this -- this report doesn't write about XRP Ledger, but, for example, if you have a system such as XRP Ledger in which certain nodes are preferred, for

example, by their inclusion into the UNL, they're more preferred than others, it allows you to discern these categories.

Q. So, is inclusiveness about the degree of permission rather than about the degree of centralization?

A. I can give you the definition of inclusiveness.

Shall I read it out for you or --

Q. No. Just tell me the page number you're referring to.

A. [redacted]

Q. Okay. We can come back to that later. I want to first direct you to page [redacted]

A. Uh-huh.

Q. In the first full paragraph, at the top. You refer to, quote, [redacted], close quote.

What did you mean by that?

A. I meant -- let me just -- let me read it. Sorry.

(Witness reviewing document.)

Where -- which line do you have that?

Q. It's the first full paragraph on the

[redacted] - Highly Confidential

top of page [redacted] And you write at the -- in the last sentence, quote, [redacted] -- I'm sorry, the -- right before that.

You write, [redacted]

Do you see that?

A. Yes.

Q. What did you mean by [redacted]?

A. So these are the -- this is what is explained in the following sentence. So, the following sentence is actually describing in more details what the sentence that you read out does. So, I can read it out, we can discuss it.

[redacted]

So, flavors should be related to definition of Troncoso and different facets.

Q. Okay.

[redacted] - Highly Confidential

All right. Let's turn to page [redacted] at the bottom, where your [redacted] position paper proposes [redacted] of inclusiveness, and argues that inclusiveness should be added as a key property of decentralized systems.

MR. SYLVESTER: Can -- can you point us to [redacted] please?

MS. ZORNBERG: It's on page [redacted] actually. The use of that language.

At the -- the paragraph at the -- in the middle of the -- the paragraph at the top, you wrote, [redacted]

Do you see that?

A. I see that.

Q. Okay. So do you agree that your [redacted] position paper [redacted]

A. I agree.

Q. Were you the first to make that

proposal?

A. I was.

I am.

Q. Okay. And you felt that you were making a contribution to the scientific community by -- by making that proposal --

A. I do.

Q. -- correct?

A. I still do. I did, and I do.

Q. Okay.

And you provide a -- a definition of inclusiveness on page [redacted] and you provide a definition of equal opportunities, which is part of your definition of inclusiveness, at the [redacted]

Right?

A. Yes.

MR. SYLVESTER: Take your time if you need a second to read it.

A. So Definition 2, inclusiveness, says that basically it's -- you can consider it renaming. So the system is inclusing if and only if it satisfies equal opportunities, and equal opportunities is then defined in

[redacted] - Highly Confidential

Definition 1.

Q. Okay. Can a -- can a system be decentralized but not inclusive?

A. It could. According to Troncoso definition, it could, and we discuss. So permission systems, we already admitted in the earlier part of this deposition that permission systems can be decentralized.

And clearly, if you -- if you read this, you will see that permission systems are not inclusive, which answers your question.

So it's not a necessary requirement.

Q. It's not -- inclusiveness is not a necessary requirement for --

A. It's --

Q. -- decentralization --

A. According to --

MR. SYLVESTER: Let her finish the question, please.

THE WITNESS: Sorry. Sorry.

Q. So just to rephrase, so do I understand you to be saying that inclusiveness is not a necessary requirement to decentralization; rather, a decentralized system

[redacted] - Highly Confidential

can be inclusive or not inclusive?

A. You got it right.

Q. Okay.

That will -- that's at least one thing. At least one thing.

A. No, you got many things right.

Q. Okay.

So, let's focus on your definition of equal opportunities, at the bottom of [redacted], [redacted]. Did you come up with that definition?

A. I did.

Q. Okay. And is that also a new definition that you put out into the scientific community?

A. As you see --

MR. SYLVESTER: Objection.

Go ahead.

A. As you see, we already discussed this, and yes, this is one of the -- in the abstract, I even say we complement. In abstract, you typically say what you did in the paper, and I'm proposing inclusing this, and I'm arguing it's a critical facet, so that's a new contribution

[redacted] - Highly Confidential

to -- that's a new contribution, you -- you are right, yes.

Q. Okay. To date, do you know whether your definition of equal opportunities has been adopted by the scientific community?

A. We need to define "adopted." I will say, you know, adoption in a sense that people cite this work, and it has been a month or two. So I gave a few talks about it, so I talk about this, in the video that you -- that you played, during [redacted]

I gave already two invited lectures on the topic. So, at the red chain workshop which is organized by the [redacted], I was invited to give a talk where I presented the concept.

And, let's say, so I -- it's not adopted yet but, you know, these things takes time. So nobody opposed it, nobody says, This is nonsense or anything. So far so good.

Q. To your knowledge?

A. Yes, to -- nobody told -- well, nobody told me, yes, so if there is -- yeah, let's speak in the open so...

[redacted] - Highly Confidential

And then the next lecture where I mentioned it is the -- I gave the lecture just this Monday on [redacted] so my alma mater, basically, where I did Ph.D., I was invited to give a lecture on decentralized computing, and there, I mention to the students this definition.

Q. Okay. Have you checked Google Scholar to see whether your position paper has received any citations to date?

A. I checked maybe last week. And in this one month or so, it didn't yet.

To my knowledge.

Q. Okay.

I'll represent we checked this morning and saw no -- no listed citations to your position paper.

A. It takes time.

Q. It takes time?

A. If you may add, may I add something? Or not?

Q. If it's -- if it's brief, sure.

A. Troncoso paper has like more citations than -- than others that came up into this --

[redacted] - Highly Confidential

so, you know, if you're measuring this -- if you're measuring the impact of the paper, for example, it's not a fair measure because Sai paper came in 2021 and Troncoso in 2017, but there is a considerable -- considerably more citations for Troncoso paper than other papers we mentioned today.

Q. Okay. When did you draft your position paper, Exhibit 5, in relation to your work on this case?

A. So --

MR. SYLVESTER: Objection. Go ahead.

A. Yes. So, I need to recall precisely. The concepts -- for example, the concept of inclusiveness, I got before I was contacted with [redacted] I'm not sure I called it my head inclusiveness.

But this distinction about specialized players in the system, for example, let's -- let's not bash XRP Ledger too much. Let's talk about proof of stake and proof of work.

So this distinction between the two that was trying to capture the essence of inclusiveness, that -- that was born early this

year. So before --

Q. Early 2021 --

A. Early 2021.

Q. -- you started thinking about inclusiveness?

A. Yes. I -- I started to -- I was trying -- for example, in proof-of-stake and proof-of-work comparison, I was trying to capture in my head, what's the difference. They appear permissionless to -- to anyone, but there is a difference, and it's not in these attacks.

So in the first hour of my deposition I talked about attacks and proof of stake and how you checkpoint in proof of work. So it's not about that. So here is more fundamental distinction.

So that was born before -- that was born before I was invited to write this position paper and before I was contacted by [redacted]

The writing that you asked me --

Q. Would you --

A. Yeah.

Q. I'm sorry, were you finished with your answer?

[redacted] - Highly Confidential

A. Yeah, I am.

Q. Okay. Would you agree that there's -- there's overlapping content between material in your report in this case and the material in your position paper?

A. I do.

Q. Okay. What about the -- the four aspects of a decentralized system in your report, in this case; you also cite to the same aspects in your position paper, correct?

A. Yes, I do.

Q. Okay. So which did you -- which did you -- did -- did you devise that methodology first for your work on this case, and then incorporate it into your paper, or did you devise it for the paper and then use it in this case?

A. So --

MR. SYLVESTER: Objection.

Go ahead.

A. Yes. So, I don't recall necessarily -- so -- I would say I was interested in defining decentralization. I was invited to write this position paper before I

[redacted] - Highly Confidential

started working on this case.

So the invitation came in -- definitely in the first -- before May this year, maybe a bit earlier.

I think it's -- it's earlier because I -- I was -- I was supposed to write something for the May edition. Yes. It was earlier. So I was supposed to not go for the October issue, but I was supposed to go for the May issue in the beginning, and then I postponed it because I was [redacted], et cetera, but I was supposed to write an article. So that invitation for the position came -- paper came before this work.

Then when I was reviewing the literature to -- in the -- for the context of this case, when you asked whether the system is decentralized or not, I realized, okay, you are invited -- your invited contribution should be on decentralized systems. This is how -- this is how it came to me, presented by editors.

But, you know, if you say "decentralized systems," you better include the definitions so the readers know what you're -- what you're talking about.

[redacted] - Highly Confidential

Since I was already looking into this -- of the case, I thought, Okay, why not -- you know, no mention -- as you see, no mention of the case or anything. Why not share this work with others.

And there are other contributions of the paper, so it's not -- it's not double-spending the report and publishing it, so there is additional things in the paper.

Q. Okay. [redacted] Was that coincidence?

A. It was -- it was accepted just recently. So it -- it's really like you see, the -- the date were like fitting in the same. We can call it a coincidence. I mean, so yes.

Q. To your knowledge --

A. It could -- it could go like -- you know, if the -- if the invitation -- if the -- if the paper was supposed to publish -- be published in November, I couldn't have -- not have done it.

And if -- I didn't think, but I was

supposed to submit my report in September, and then I didn't, and then I submitted it in October, so we can call it a coincidence.

Q. Okay. To your knowledge, was the SEC aware of your draft position paper?

A. Did -- did SEC review my paper or something?

Q. Well, did -- to your knowledge, did the SEC know that you were publishing this position paper?

A. I -- I advised -- I'm not sure I talk to SEC. I advised [redacted] that I'm going to use part of the methodology to -- for the paper. And I basically made that known.

Whether SEC knew it or just [redacted] knew it, I definitely made it clear, yes.

Q. Okay.

Did anyone from the SEC or [redacted] provide comments on your draft position paper?

A. No, they did not.

Q. Okay.

Turning to another subject.

Do you degree that there are different architectural layers within blockchain systems?

[redacted] - Highly Confidential

A. Within a softwares -- within a software system, computer system, there are different layers. Including -- if the blockchain is a computer system, there are different layers to the blockchain system as well.

Q. Okay. So if you still have Exhibit 4 in front of you, the Sai paper --

A. Yes.

Q. -- let me ask you to turn to page 12.

Do you see the chart that he has -- that Sai labels as Table 2?

A. I see.

Q. Okay. And in the left column of the chart, do you see that Sai identifies -- it looks like six different layers of -- within public blockchains.

A. I see it.

Q. Do you -- do you think that Sai has omitted any layers? In other words, are there additional layers of public blockchains not identified here?

A. That's a good question.

So, I think he covered them well.

[redacted] - Highly Confidential

Let's look excluded, there is, you know, something, but I think it's -- covers it well but -- you know.

Q. Okay. And in the -- in the next column, middle column, Sai identifies what he calls different factors of centralization within each layer of a blockchain, of a public blockchain system.

Do you see that?

A. Where do you find that?

Q. The middle column.

A. Centralization factor.

Q. So, for example, for the network layer, do you see that Sai identifies four distinct centralization factors to consider, just within the network layer?

MR. SYLVESTER: Objection.

A. I see that there is a "Network Layer" row. I see that there is a "Centralization Factor" column. I see that there are four different centralization factors in the "Network Layer" row.

Q. Do you agree with Sai that aspects of centralization at the network layer are relevant

to overall assessment of decentralization of blockchain systems?

MR. SYLVESTER: Objection.

A. I do. So I agree that the network layer centralization is important for evaluating whether the entire software system, distributed software system including blockchain, is centralize -- is decentralized or centralized or not.

Q. Do you agree that each different factor of centralization within an application layer may require a different measurement technique?

MR. SYLVESTER: Objection.

A. Can you repeat that again? I apologize.

Q. Yeah.

So, do you see how in -- in Sai's chart, Table 2, Sai also has a column on the right called "Measurement Techniques," where Sai lists different techniques for measuring each centralization factor within each layer of a public blockchain?

A. I see that.

[redacted] - Highly Confidential

Q. Do you agree that the scientific community may need to use a different measurement technique in order to measure different centralization factors?

MR. SYLVESTER: Objection.

A. What I think is that scientific community could use those, it could use some others. It's like what -- what are you measuring, doesn't necessarily -- is important. And then comparing what you're measuring doesn't necessarily depend on the metric you're using.

I can give an example. So, I can measure the height of people by a yardstick, or by a meter, or by a foot.

So these are different, you know, measurements, and they might come up to the same conclusions. In my example they would, but which person is taller than other, which -- in other cases, you know, some conclusions might be different.

So does this help?

Q. Well, I want to just make sure I clarify. Would you agree then that even today, there's ongoing dialogue in the scientific

community about which metrics to use in measuring different aspects of decentralization?

A. I would say which metrics you use, but not what are you measuring. So that's important distinction.

So, for example, geographic distribution, so, you know, if you're measuring geographic distribution, you would go and measure it something.

And then you can use what he says, Gini coefficient and latency, which is like, you know, just reading this, Gini coefficient of what? You need to say of what? Right? And things like that so that's a bit imprecise.

But yes, I mean, you can use different metrics. I would say it's more important to focus what are you measuring.

Q. Okay. In your report, did you consider centralization aspects for every blockchain layer?

A. So, you will see that my methodology points -- so focuses, and points out, resilience layer, which is essentially consensus layer. It maps to the consensus layer of Sai. If you want

to do the mapping, it maps to the -- maps to the consensus layer.

Then there is the openness layer. Ah, so you see, okay, openness that I discuss in my report, it's -- so Sai focuses on public blockchain systems. And then if you want -- so as the title says, "Taxonomy of Centralization in Public Blockchain Systems."

Then he goes -- they go and compare to bitcoin and Ethereum -- compare bitcoin to Ethereum, and this is their focus.

So, for example, they wouldn't -- this doesn't discuss permission blockchains, whether they can be centralized or not, so there is a point of contention maybe there, but, again, Troncoso definition would allow permission blockchains.

So you asked me before, and then I will need to complement, is there a layer that Sai doesn't consider? And that would be this openness --

Q. Okay.

A. -- layer that I'm considering.

Q. So let me just break it down. First I

[redacted] - Highly Confidential

hear you saying that one layer, not referenced in Table 2 of Sai, that you think is important to evaluating decentralization, is openness?

MR. SYLVESTER: Objection.

A. That's -- it's not that I think it is -- it is important, it's that also I think that it is important, and there are other people who think that it is important to look whether it's -- blockchain is permissioned or not, when we evaluate which one is more decentralized than the other.

So if I'm to point out the layer that not only me but also other researchers and other just -- whoever works in this space -- considers as an important aspect or facet of centralization, decentralization, is the openness.

This is related to permissionless, permissionness and inclusiveness that we discussed in this deposition.

Q. Okay.

Do you degree that your report, in evaluating and comparing blockchain systems, did not analyze every single layer that Sai lists in

Table 2?

A. In my report, I mention all the layers that Sai discusses.

And notably, you know, with respect to network and application layer, these are mentioned in my report in -- sorry, just a second. I got lost.

Q. Are you talking about page 11?

A. Maybe.

Yes.

Q. Okay.

A. So, for example, in the network layer I mentions -- I can read it out -- but some authors -- I'm citing Sai -- consider additional aspects of decentralization including decentralization of the net --

THE COURT REPORTER: Slow down a little for me.

MR. SYLVESTER: Yes.

THE WITNESS: Sorry about that.

A. Finally, I'm reading out the -- page 11.

Q. You don't have to read it out loud. But I --

[redacted] - Highly Confidential

A. Okay.

Q. I'm on the same page. You're -- you're referring to the paragraph in the middle of page 11 --

A. Yes.

Q. -- just above 3.2 of your report?

A. Yes.

Q. Is it fair to say that you -- this is the part of your report where you identify that some authors have considered aspects of decentralization that you are not focusing on in your methodology?

A. Focusing is the right word, although I say -- and I would definitely like to read this out -- decentralization at the network layer requires that no single authority can control all the participants of a decentralized system at the network and infrastructure layers.

So I'm pointing it out, and then I'm focusing -- in the next paragraph, I'm saying we are going to focus on these other aspects, which don't touch the network layer.

I can give you -- if you wish, I can give the justification, which is not included in

the report, my line of thinking, why this was the --

Q. Please do.

A. Great. Thank you.

So, all of three compared systems. They operate on wide area Internet.

Q. On?

A. On wide area internet.

So bitcoin, Ethereum and XRP Ledger.

In my opinion, there is no centralization at the network layer for either of the three.

And then I -- they're like more -- I'm not saying there are no differences. Of course, if you look at the network distribution of all three blockchains, it's actually very different, and we can discuss that in a moment.

The main difference is that XRP Ledger has much fewer nodes than bitcoin and Ethereum. And as such, if you look at the -- you know, if you start looking at Sai's metrics, I'm -- I'm pretty sure it would not turn out well, in comparison.

But what I'm implicitly doing here is

[redacted] - Highly Confidential

I'm -- I'm adopting the viewpoint that there is decentralization at the network layer in all cases; hence, let's look at the layers where there is not.

This is -- this is the line of thinking behind it.

Q. So just for completeness, which blockchain layers did you leave out, or not focus on, as part of the core focus of your report?

MR. SYLVESTER: Objection.

A. So, I considered all the blockchain layers and all the aspects. It is just that I said, we opt to focus on decentralization aspects of the system proper, and that says -- I can read this out. To maintain emphasis on the core distributed systems aspects.

In this report, we acknowledge these decentralization aspects that go beyond the core of a system, namely, network and application layer decentralization. Yet we opt to focus on decentralization aspects of systems proper.

Q. So, what are the core layers of a system?

[redacted] - Highly Confidential

A. So the core layer is the -- what Sai calls consensus layer, what I call resilience layer. So this is the distributed systems layer.

And then, I'm also focusing on governance. Operational layer in Sai's case is the part -- is part of my inclusiveness layer.

Maybe I should get -- taking it out, but it's included.

So if you look at operational decentralization, it's actually -- actually part of -- it's part of inclusiveness. And openness. In that context, I am discussing it.

So all the others are included, incentive layer as part of in-protocol incentives, governance layer.

Q. Okay.

I'm sorry, were you finished with your answer?

A. Yes.

Q. Okay. Did you -- did you consider every centralization factor for each layer, putting aside network and application layer, that Sai considered?

[redacted] - Highly Confidential

A. That Sai considered. Let's see, I -- storage constraint, specials equipment concentration.

I discuss special equipment. I am putting out as operational decentralization storage constraints, as an example.

Wealth concentration of the incentive layer I discussed in my report.

Consensus power distribution, so we are discussing -- so for me, this is captured by the resilience aspect. And there is owner control and improvement control -- improvement protocol, so these centralization factors that he has, I'm considering in my report, I believe all of them.

Q. Okay.

Would you agree that a reliable measurement methodology is necessary before you can compare different blockchain systems?

MR. SYLVESTER: Objection.

A. What does it mean "reliable" in this case?

Q. Well, earlier, you spoke about reliable as being replicatable results,

testable.

A. Yes. So, I -- in that sense, I -- I believe it does, yes.

Q. Okay.

Are there any challenges in comparing decentralization across different types of blockchain systems?

A. If you take the Troncoso definition as the basic point, so now again I need to read through this, but if -- Troncoso definition is very clear one. It sets the bar really low.

And for that, for me -- like the goal of the -- of what one needs to show or not is clear. Sometimes it is challenging to evaluate what's really going on in the network.

One example is, you know, does one authority control the interval mining pool, the entire mining pool or not, and in that case, we would make -- what I did in my report, I -- I was trying to -- yeah, sorry, I lost it.

Q. Why don't -- that's fine. Why don't I put a different question.

A. Yes.

Q. Your report offers an opinion that

bitcoin is a decentralized blockchain system. Correct?

A. It does, yes.

Q. Does your opinion -- have you offered an opinion in this case as to whether Ethereum is decentralized?

A. I mentioned, in the report, that Ethereum passes the Troncoso definition because it doesn't have -- especially on the consensus resilience layer, it doesn't have the trust in a single authority.

So --

Q. Do you know where in your report you say -- you say that Ethereum is a decentralized blockchain system?

(Witness reviewing document.)

Q. I'll represent that I haven't seen it written anywhere, so --

A. Probably -- it's probably specifically, you're right. I don't think I wrote it either.

Q. Was that in -- did you -- not -- was that a purposeful or unintentional omission?

MR. SYLVESTER: Objection.

[redacted] - Highly Confidential

A. I was -- I think the question said to what extent -- so I'm reading question for expert opinion E1. To what extent is the XRP Ledger centralized or decentralized when compared to generally recognized blockchain protocols such as those used by bitcoin and Ethereum.

So I was not really asked to say whether Ethereum is decentralized or not.

Q. So -- all right. Sitting here today --

MR. SYLVESTER: Lisa, sorry to cut you off. We've been going for about an hour and a half. Is there a good time to take a break?

MS. ZORNBERG: Yeah, let's break at one o'clock.

MR. SYLVESTER: Does that work for you, or are you hungry?

THE WITNESS: How much time there is until 1?

MR. SYLVESTER: 20 minutes.

THE WITNESS: 20 minutes.

MR. SYLVESTER: He's on a different

time zone too. He's on Switzerland time so --

MS. ZORNBERG: Can we continue till 1?

MR. SYLVESTER: If you need a break right now, we can take a break right now.

THE WITNESS: Let's finish the question and then break without going to -- to one o'clock. So just --

Q. Okay. So I'll finish this line of questions.

A. Yes.

Q. Are you offering any opinion in this case as to whether Ethereum is the decentralized system?

A. I'm not.

Q. Do you have a view as to whether Ethereum is decentralized?

A. I have a view. I have certain opinions. And -- yeah. But I'm not offering the opinion.

Q. In the past, have you cited to Ethereum as an example of a -- of a blockchain system that is totally decentralized?

MR. SYLVESTER: Objection.

[redacted] - Highly Confidential

A. To my recollection, I would never use those words. No.

Q. Okay. I'm going to show one exhibit, and we'll end on this -- on this point.

MS. ZORNBERG: Can we show Exhibit 8.

(Article titled [redacted] was marked [redacted] Exhibit 8 for identification, as of this date.)

Q. Do you recognize Exhibit 8?

A. I recognize it.

Q. This is a -- an article that -- that you and your co-authors published in [redacted] entitled, quote, [redacted]

A. Yes.

Q. Let me direct your attention to the only part I'm going to ask you about. It's on page 2 of the article, the first paragraph.

Can you read the first two sentences, starting with, The blockchain may?

A. Second page? Where should I look? I

apologize.

Q. I'm holding it up. Just in case that helps.

A. Okay. The blockchain may abide. Right?

Q. Yes.

A. [redacted]

Q. Okay.

And you cite -- for the sentence that, [redacted]

Can you tell me what -- what those citations were?

A. This is Satoshi Nakamoto bitcoin paper and Ethereum position white paper or yellow paper by Gavin Wood. This is cited.

Q. Okay. So were you citing here to Ethereum and bitcoin both as, Examples of

[redacted] - Highly Confidential

permissionless ledgers that are maintained across peer-to-peer networks in a totally decentralized and anonymous manner?

MR. SYLVESTER: Objection.

A. [redacted]

Q. Okay.

A. I'm a bit taken off guard here, so this is not -- as you're writing the paper, it's not a justification, but it's not something that I would write. So maybe my co-authors write it and it slipped through my cracks.

But this is definitely, you know, totally decentralized for the purpose of this paper, it's not even defined. So to understand if something is totally decentralized and for this paper to be clear on what's written here, we would need to define what totally decentralized means.

Q. Which you did not do in [redacted]

A. Which we didn't do for this -- practice of this paper, yes.

Q. Okay. But -- but do you agree that at least as written in [redacted] you cited both to bitcoin and to Ethereum as totally

[redacted] - Highly Confidential

decentralized?

MR. SYLVESTER: Objection.

A. Well, we cited, in this sentence, that [redacted] we cite both bitcoin and Ethereum, yes.

MS. ZORNBERG: Okay. We can take a break.

THE WITNESS: Thank you.

THE VIDEOGRAPHER: It is 12:46 p.m. We're going off the record.

(Luncheon recess at 12:46)

[redacted] - Highly Confidential

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

(1:38)

[redacted] Ph.D.

resumed, having been previously duly sworn by a Notary Public, was examined and testified further as follows:

THE VIDEOGRAPHER: It is 1:38 p.m. We are back on the record.

CONTINUED EXAMINATION BY MS. ZORNBERG:

Q. Dr. [redacted] you testified earlier that you view Troncoso's definition of decentralization as setting a minimum floor for a system to be decentralized.

Do you recall that?

A. Minimum -- low bar, minimum bar, let's say.

Q. Minimum bar?

A. Yes, we can agree.

Q. Are you aware of any academic literature that supports your view that Troncoso sets a minimum bar for a system to be decentralized?

A. I'm not aware -- I think I repeated

this at least two times. But I'm not aware of any definition that would admit a decentralized system if it doesn't satisfy Troncoso's definition. So people, while they're proposing definition of decentralized systems, they might not cite Troncoso, you know. Just cite that paper.

But they might come to the similar, stronger test that would admit a system is decentralized. So this is what I'm saying.

Q. Do you have -- I understand.

Do you have in mind, though, any literature -- scientific literature, that does cite the Troncoso definition or standard and agrees or acknowledges that that sets a minimum bar for decentralization?

A. Well, there is at least my paper that does it.

Now, whether explicitly, no -- well, one way to find it out would be to go to Google Scholar to look at the citations of the Troncoso and to basically make sure if somebody actually declares this as the -- as the thing.

Q. Did you do that work in preparing your

report?

A. I didn't go through 50-something citations of Troncoso in order to do that.

Q. Okay. All right. Moving to another subject.

Are you offering any opinion in this case regarding how the term "decentralized" has been used by the SEC as relates to blockchain systems?

A. I do not.

Q. Okay.

A. That wouldn't be fair, no.

Q. I take it, then, you're also not offering an opinion regarding what any SEC employee may have meant or not in using the term "decentralized"?

A. That is correct.

Q. Okay. More broadly, are you offering an opinion about how any United States regulators have used the term "decentralized"?

A. I'm definitely not an expert on U.S. regulations. And, no, I'm not doing that.

Q. Do you know if the SEC has ever cited to the Troncoso paper prior to bringing its

[redacted] - Highly Confidential

lawsuit against Ripple?

A. No. So -- if I rephrase the question, did SEC in any public or speech known to me -- maybe it's not public -- refer to the Troncoso paper before, let's say, me introducing it? The answer would be no.

DIR Q. As far as you know, did you introduce that paper and its definition of decentralization to the SEC through your work on this case?

MR. SYLVESTER: Objection.

That might be getting into privileged communications.

And I -- I'm going to ask you not to answer that one.

Q. Sitting here today, as far as you know, Dr. [redacted] did anyone at the SEC know of the Troncoso definition before you yourself found it while digging into this case in the summer of 2021?

MR. SYLVESTER: If you know.

A. That I couldn't know. So --

Q. Okay.

A. -- yeah.

Q. Do you know if the SEC has ever

[redacted] - Highly Confidential

defined the term "decentralization" for purposes of securities regulation?

A. I don't know if they did, which means they could or not, but not that I know.

Q. Okay. And you don't know if the word "decentralized" appears in United States securities laws or regulations?

A. I really don't know that, no.

Q. Are you offering any opinion in this case as to whether decentralization is relevant to the legal definition of an investment contract, under securities law?

A. I'm not offering that opinion.

Q. Okay. Are you aware that the SEC produced documents in this case, reflecting its communications about decentralization with blockchain market participants?

MR. SYLVESTER: Objection.

A. I'm not sure I understand the question. If you rephrase, maybe I can relate.

Q. Yeah, yeah, sure.

Do you know whether the SEC, in this lawsuit, has turned over documents from its own files, reflecting its discussions with people in

[redacted] - Highly Confidential

the -- in the blockchain industry, about decentralization?

MR. SYLVESTER: Objection.

A. Yeah. The -- to my understanding of the question, that would be no. So I'm not -- I'm not aware of that. No.

Q. Okay.

Let me show you [redacted] -- Exhibit [redacted] 9.

(Tweet from Neha Narula was marked [redacted] Exhibit 9 for identification, as of this date.)

Q. I think we discussed earlier this morning, that you -- you recognize the name, Neha Narula from conferences in the blockchain industry, right?

A. I recognize the name, yes.

Q. Okay. Do you know that she's the head of MIT's digital currency lab?

A. I know she's affiliated with MIT. I didn't know the -- what's the word? So I didn't know the -- which role she has at MIT, which position she has.

Q. Is the MIT digital currency lab part of the scientific community studying blockchain?

A. That's a good question. So I -- so MIT certainly is. Let's not go there. Right?

Was the status of the MIT this and that, what is their status in the community? In -- at MIT, that I don't know in details.

Q. Okay.

A. Know that Neha Narula writes scientific papers. They're not on my immediate radar. So I'm not, you know, often seeing her papers.

Q. Okay.

A. Does that make sense?

Q. Sure.

So I'm -- Exhibit [redacted] 9, is a tweet by Neha Narula, from June 15, 2018. I'll just read it for the record.

It says, quote, I'm a little worried people from government agencies are throwing around the word "decentralization" like we know what it means or how to evaluate it.

Closed quote.

Have you previously seen this tweet?

A. I might have.

Q. Do you follow Ms. Narula on Twitter?

[redacted] - Highly Confidential

A. No.

Q. Okay.

Do you know what Ms. Narula was referring to here when she stated that government agencies are throwing around the word "decentralization"?

A. I really do not know what she referred to. I don't know that. I don't know what's "we" referring to.

Q. Okay.

A. Who is "we" referring to?

Q. Have you personally read any speeches, or publications, by SEC officials, relating to the issue of cryptocurrency?

A. Speeches? How do you define speeches, or -- have I read speeches?

Q. Let's start with speeches. Have you read any speeches by the SEC relating to the issue of decentralization?

MR. SYLVESTER: Objection.

THE WITNESS: Yes.

A. So to my understanding, I did not, so no.

Q. No. Okay. I'll represent to you that

[redacted] - Highly Confidential

Ms. Narula tweeted out this tweet in Exhibit 9 one day after an SEC official gave a speech discussing decentralization of blockchain systems.

Do you -- do you agree with the concern Ms. Narula's tweet expresses that members of -- that -- that people from government agencies are throwing around the word "decentralization"?

MR. SYLVESTER: Objection.

A. I don't know in which sense throwing around, so I would not agree with "throwing around," the word.

Does that help?

Q. Okay. Are you involved in any of your work in advising -- putting aside your work as an expert in this case, have you ever advised United States regulators on the meaning of decentralization?

A. No, I have not.

Q. Okay. You can set that aside.

Is the -- is the term "sufficiently decentralized" a term that has any meaning to you?

[redacted] - Highly Confidential

MR. SYLVESTER: Objection.

A. It has certain meaning.

It has certain meaning. Yes.

Q. What does sufficiently decentralized mean?

A. I'm not sure. So I -- the term might mean something. I'm not sure.

Q. You're not sure?

A. Yes. So -- yeah. Sufficiently could be -- I can speculate.

Q. I'm not asking you to speculate.

A. Very good.

Q. Okay. But I guess my question is, in your experience, is there -- is there any scientific standard that you've seen, for determining when a blockchain system is, quote/unquote, sufficiently decentralized?

MR. SYLVESTER: Objection.

A. We spent a lot of time today discussing the minimum and basic condition which would go out for necessary decentralization.

Sufficient decentralization would probably be a spectrum of things that would mean different things to different people. I think

this is the only fair thing to say.

Q. Okay.

A. So I admit -- I admitted permission blockchains decentralized according to the Troncoso definition and methodology that I'm following. I'm pretty sure there are people around who would say that no permission blockchain is decentralized.

Q. Are you offering any opinion in this case on the -- what "sufficiently decentralized" means?

Sounds like you're not.

A. I'm not. I have my opinion, but I'm not offering it. Does that make sense?

Q. Okay.

Are you offering any opinion in this case on how the SEC or any employee of the SEC, has used the term "sufficiently decentralized"?

A. I do not.

Q. Okay. When does a blockchain system become operational, in your view?

MR. SYLVESTER: Objection.

A. That's -- you need to define "operational," to start with.

Q. So does -- does the term "operational" have one set meaning to you?

A. Operational, no, it does not. So operational could be something that works. Does it work as intended? That's one question.

Do I call that operational? Or you just -- it works and not necessarily is it intended, is it that operational? So that's basically what I'm struggling immediately. There might be other things which I'll be struggling with.

Q. Okay. If a -- if a blockchain system works as intended, would you agree that it's operational?

A. That could be one -- if operational is -- if the word "operational" means that, then I guess answer could be yes.

Yeah.

Maybe.

Q. Okay.

A. Maybe. It depends on the definition of the word "operational." So operational, work as intended, so what does it mean "intended"? So I guess there is specification, and the

[redacted] - Highly Confidential

system is proven to do that thing.

Q. So let me -- let's take an example. Let's take an example.

How soon after the bitcoin network launched did it become operational, in your view?

MR. SYLVESTER: Objection.

A. We would need to define what operation of a bitcoin means. Shall we try to do it? Or no?

Q. What do you think operational for a bitcoin means?

A. I don't know. You came up with the word. I really don't -- I'm not using the word. Yeah.

Q. Well, actually -- I'm not meaning -- this is -- I'm trying to get your understanding, of whether -- whether it has a scientific meaning. I -- whether the term "operational" -- how is it applied to discussions of blockchain systems, if at all?

I don't want you to assume any definition I'm giving it. I'm asking you if it has meaning to you to discuss when a blockchain

system becomes operational.

MR. SYLVESTER: Objection.

Go ahead.

A. Yes. I believe that it doesn't have -- determined meaning to me. So --

Q. Okay.

A. -- I would really then go -- if somebody -- if you were not you but just my colleague comes to me and comes with the same question, I would say, What do you mean by "operational"?

And then we would probably engage in a discussion of what "operational" means.

Q. Okay. Understood. So there's no -- okay.

Does the -- is the term "fully functional" a term that has any meaning to you in describing blockchain systems?

MR. SYLVESTER: Objection.

Go ahead.

A. Yeah. In some sense it is similar to operational. Again, we need to define "fully functional," so I guess there is a function of the blockchain, again, which relates to the

specification.

And then "fully" would be -- yeah, there are no missing features. It is really like what it's doing? What specification is supposed to tell the people that they're doing? And there are no bugs whatsoever.

This is how I would reason. But I'm online reasoning. You asked me the question. I just gave you online opinion about it.

Q. I see. Before sitting here today in this deposition, have you given thought to whether the term "fully functional" has a definition to the scientific community?

A. In this wording, "fully functional," no, I am not.

Q. Are you offering any opinion in this case on the definition of fully functional as relates to blockchain systems?

A. I do not.

Q. I think we -- we discussed this morning that the development of distributed networks can involve iterative processes with changes over time. Right?

A. Yes.

[redacted] - Highly Confidential

Q. Can a blockchain system be operational even if additional development happens --

MR. SYLVESTER: Objection.

Q. -- over time on that system?

MR. SYLVESTER: Objection.

A. It, again, goes back to the definition of operational. Since we didn't agree on the definition of the word, I presume there is a world in which there is a definition of operational that would permit your example.

Q. Well, let's use -- let's talk -- let's use for a minute the concept of operational that it works as intended.

A. Okay.

Q. Okay. Do you have a view on when -- when the bitcoin network became operational?

A. I'm not aware of the full specification of bitcoin as operating as intended.

You could say -- so depending on the standpoint you take, if the specification is the code, then it's always operating as intended. If there is a separate specification from the code, you would need to establish -- and I'm not

aware that there is a, for example, separate specification of bitcoin code apart from the code itself.

Q. Okay.

A. So if you take a standpoint -- now I'm really coming with this online. If you come with the standpoint that the code itself is the specification, then it's fully operational, yeah. It's just doing what the code tells it to do.

Q. I see.

A. Yeah, so --

Q. So if the -- if bitcoin was launched, and it operated as imagined and intended based on its code, one could say it was operational immediately when the code launched.

MR. SYLVESTER: Objection.

A. If this is the definition. If what the code does is -- is the specification, what the code should be doing and you would call this operational, then the answer is yes.

Q. Okay.

A. There would be other definitions of operational for which the answer would be no.

[redacted] - Highly Confidential

Notably when the -- as intended is separate from the code.

Q. Are you expressing any view in this case as to when the XRP Ledger became operational?

MR. SYLVESTER: Objection.

A. I'm coming back to the ambiguity of the word "operational," so I guess my answer would be no.

Q. And are you also not expressing any opinion in this case on when the XRP Ledger became fully functional, a term which you've also said is -- is vague?

MR. SYLVESTER: Objection.

A. I -- again, so I'm relating to the fact that we would need to define this notions fully. And, I'm not offering any opinion on that. So I'm not -- I think we're going -- so correct me, but I think we're going a bit in a circle, but I'm just repeating what I did. So yes.

Q. Okay.

A. I'm not offering any.

Q. Let's move on. I want to just -- here

is what I would like you to explain, though.

When a blockchain system is launched and it's being used and it's being used in the way that it was intended to be used, can additional functions still be added to that blockchain later?

MR. SYLVESTER: Objection. Objection.

A. So it is working and it's working as it's supposed to be working. And you're adding other things, which means that you're adding things that it was not how it was supposed to be working.

Right?

Q. I'm just asking how -- maybe I'm -- let me simplify. Isn't it very common for operating blockchain systems, for developers to continue adding added functions and features to those already operating blockchain systems?

MR. SYLVESTER: Objection.

A. Again, so the operating -- operating as running, so there is a code that's running on the nodes. And blockchain developers add the codes to the software. And it's updated regularly. Yes, this is a commonplace, of

course, yes.

Q. Okay. I would like to turn back now to talking about UNLs an the XRP Ledger.

Are participants in the XRP Ledger ecosystem required to use the UNL published by Ripple?

MR. SYLVESTER: Objection.

A. They are not required. To use the UNL published by Ripple.

Q. Can a participant modify their instance of rippled to use a UNL other than the default UNL?

A. They can do that, yes.

Q. Okay. So, for example, can an XRP Ledger participant modify their instance of rippled to exclude all Ripple-operated validators from their UNL?

A. The -- a validator could do that, yes.

Q. How would they accomplish that modification?

A. They would -- you -- it can be done in different ways. You could download the UNL from the Ripple site, basically just go and exclude those validators. That's one way to do it.

[redacted] - Highly Confidential

Q. Okay. And would a validator be required to obtain permission from Ripple before making that modification?

A. No. It wouldn't.

Q. Would they be required to obtain permission from any third party before making that modification?

MR. SYLVESTER: Objection.

Q. You can answer.

THE WITNESS: Yes.

A. So to my understanding, no.

Q. Could a participant write their own code to perform all XRP Ledger functions?

A. There is nothing preventing the -- the client to write a compatible code, not in C, but in some other language, for example. Why not? Yes.

Q. Okay. And if -- if other -- if others on the XRP Ledger decided to trust someone or persons other than Ripple, could Ripple do anything to stop that --

MR. SYLVESTER: Objection.

Q. -- to your knowledge?

MR. SYLVESTER: Objection.

[redacted] - Highly Confidential

A. To my understanding, no. Now, we are entering the field in which we need to understand. So, you know, we said we can -- can you change the software? Can you do this? Can you do that?

The question is what guarantees you have once you do that. So we should probably at some point discuss that.

But to come back to your question, the answer is, normally, there is no permission or third party for me, as a validator in the Ripple network, to modify my software. I can do that as I please.

Q. By "guarantees," are you referring to guarantees of liveness and safety?

A. That's it.

Q. Okay. Well, we're going to get to that shortly.

As of the date of your report, how many XRP Ledger participants used the UNL published by Ripple, if you know?

A. That I don't. I don't know.

Q. Okay. Do you know how many XRP Ledger participants used a UNL different than the one

published by Ripple as of the date of your report?

A. That I don't know.

Q. I don't take it -- let me rephrase.

Are you asserting that every XRP Ledger participant uses the UNL published by Ripple?

A. I'm not asserting that.

Q. Did you speak to any XRP Ledger validator in preparing your report?

A. Validator operator. Not -- yeah.

No. No, I did not. Validator would be software, but, yeah. So --

Q. Okay.

A. I cannot speak to the software, but operator --

Q. Okay. I understand. Okay. Thank you for that correction.

So did you -- did you -- so let me -- did you speak to any XRP Ledger node operator in preparing your report?

A. I did not.

Q. Do you have any basis to conclude that every XRP Ledger participant uses the UNL

published by Ripple?

A. I did not offer that conclusion, as we discussed.

Q. Okay. All right. So -- so let's turn now to the subject of resilience, which is the -- one of the four decentralization aspects you discuss in your report. Right?

Let me direct you to page 9 of your report, please.

So, first, in the context of your report's methodology, what is resilience?

A. Resilience of the system refers to ability to withstand Byzantine behavioral components of the system.

Q. Okay. And what is that definition based on?

A. That definition is based on the use of the word "resilience" in almost all papers I know about which deal with Byzantine Fault-Tolerant protocols and blockchain protocols. So all of them would be having an assumption on the adverse side that the protocol can tolerate and still provide its guarantees.

For different concerns with protocols,

this may come up in different flavors. You -- in proof-of-work protocols, it would be expressed as a percentage of the mining power that needs to be controlled in order for the adversary to be stopped if it controls less than that threshold or for adversary to succeed in mounting an attack to the system as I'm describing later.

In the group of Byzantine Fault-Tolerant protocols or just the protocols that vote by -- like one validator/one vote, or weighted voting, such as in proof of state, you weight -- you vote with your stakes or the more stake you have, the higher the value of your vote.

That would be a different -- this -- this also, the resilience threshold also appears. And it denotes the number of components or, like, number of validators, if you want, in the system, that -- which you can turn to the fraction, if you have a snapshot of the behavior of the membership of the current system. You can relate to the fraction as well.

So we discussed before in this

deposition for -- just to give an example, we discussed about one-third, up to one-third of nodes, up to one-half of nodes, et cetera. These are all impacting the resilience of the system. So that number, that critical number of Byzantine needs, that would be the number of tolerated.

Q. And when you refer -- when you refer to that critical number --

A. Yes.

Q. -- are you referring to the Nakamoto coefficient or something else?

A. So I'm referring to -- I point you to page 9.

Q. Yes.

A. So this is the last paragraph in the resilience section.

So I will read it out. So I say, In this context, the scientific literature and engineering practice is typically interested in the minimum number of authorities that the adversary needs to compromise to subvert the key property of a system, such as safety and liveness, full stop.

[redacted] - Highly Confidential

So I'm referring to minimum number of authorities. And when I say "scientific literature and engineering practice," I don't give exact.

Q. Okay. In the next sentence, though, you say that this number is sometimes referred to as the Nakamoto coefficient.

A. Yes. As you see, this is a mouthful. The first sentence is a mouthful. So since -- let's call it some way. And then I was considering -- honestly, when I was writing this, I was considering two things.

One, I call it coefficient of Byzantine nodes. And then I saw that some people who are in the space call that and also define that notion, and then you use it in the definition as Nakamoto coefficient.

I said, Okay. This is nice. This is not mouthful. It's interesting and may grab people's attention. Let's call it this way.

What it means is basically defined in the previous sentence.

Q. Okay. So prior to your work on the case, were you familiar with the term "Nakamoto

coefficient," or is that a term that you encountered while doing work on this case?

A. So I -- I was aware that people use it. I didn't use it in my work. I would usually refer to this threshold as the number of potentially Byzantine participants, which, again, for the presentation, because one of the -- when I was writing this report, one of the guidelines, so -- so -- that came up is this should be readable for nontechnical audience.

So I was trying to come up with a term that would -- you know, that I would use to refer to this notion without calling it coefficient of, you know, the threshold on the number of Byzantine nodes, which is again --

Q. Okay.

A. So I was aware of the -- of the term. I didn't use it much. I thought it would be nice for -- for a report that supposed to be read by nonexpert to call it that way.

Q. Can a system be resilient but centralized?

MR. SYLVESTER: Objection.

A. So resilient in the -- so resilient in

the context of my report, the way I'm defining things here, it could -- so some components of the system, at some layers, you could have a ability to tolerate Byzantine faults; but at some other layer, for example, you do not.

So you need to understand, if we discuss the network layer versus distributed systems layer, right? So we could have a centralization on either of the two, and it's really an end to call it decentralized.

Q. It's really a?

A. End function, end function.

Q. End, E-N-D?

A. Yes. So if it is decentralized at a consensus and the distributed systems layer, it would also need to be decentralized at the network layer would probably be centralized.

Q. Okay. But coming back to question, can a distributed blockchain system be resilient but centralized?

MR. SYLVESTER: Objection.

A. So let's read this as -- as -- as I specified here. So resilience, if this is the ability to withstand behavior of certain

components of the system, you could have a system that's -- is able to do so. But it's still centralized because of the -- when we come to the minimum number of authorities that the adversary needs to compromise to subvert key property in the system, this would still be one because there is, for example, some specific component of the system from which you can mount an attack --

Q. So the answer is yes --

A. -- so probably yes. Probably could be yes.

MR. SYLVESTER: Let me finish the answer, please.

Q. Please.

A. I believe the way you pose the question, the answer would probably be yes, yes.

Q. Okay. Can a system be decentralized, but not resilient?

A. No. I would say the answer is no.

Q. No.

So a system must be resilient in order to qualify as a decentralized system.

A. Yes.

[redacted] - Highly Confidential

Q. Okay. How do you measure resilience?

A. So we measure resilience, using this minimum number of authorities that the adversary needs to comprise to subvert the key property of the system, such as safety and liveness. In the context of blockchain, this number is sometimes, sometimes referred to as Nakamoto coefficient.

So that -- and as the text says later, the higher the Nakamoto coefficient, the higher the level of decentralization.

As per the definition of a decentralized system, we adopted, I'm citing Troncoso, if this number is one, which means if a single participating authority can compromise a key property of the system, the system cannot be decentralized.

MS. ZORNBERG: Okay. Let the record reflect that Dr. [redacted] was reading almost verbatim from a paragraph on the middle of page 9 of his report.

Q. Right?

A. Yes, that is correct.

Q. Okay. Are you familiar with the concept of partition tolerance in blockchain

systems?

A. I am.

Q. What is partition tolerance?

A. Partition tolerance, we mentioned it briefly, at the second, I believe, hour of the deposition. It's related to this asynchronous --

Q. This what?

A. Asynchrony, asynchronous, I was telling this --

Q. Oh.

A. Yes. So it's related to that.

So when the network exhibits asynchrony, we also call it network partitions, which means if my message is there, I'm trying to send a message to you and it takes a long time. And network partition is this temporary inability for you and me to communicate.

So some -- in some communities, this would be called asynchrony, asynchrony. And in some others, it would be called network partition. Usually refer to the same thing.

Q. Is partition tolerance an element of the resilience of a system?

[redacted] - Highly Confidential

MR. SYLVESTER: Objection.

A. That depends on the stated goals of the system, some -- some systems might opt -- so any system, when you discuss the -- any systems comes with a specification. So it should come with a specification that it's doing something assuming this, this, and that.

So if I can devise a system in which I am not tolerating network partitions and that would be fine so long, you know, I'm designing such a system.

Q. Okay, so, you would agree that -- a blockchain system can opt by design, to either be partition tolerant or not partition tolerant.

A. It could. Yes.

Q. Okay. So would you agree that a partition-tolerant blockchain is vulnerable to an involuntary fork?

A. Partition-tolerant system is vulnerable to involuntary fork -- can you repeat your question.

Q. Yes. Is a partition-tolerant blockchain vulnerable to an involuntary fork?

A. Not necessarily.

[redacted] - Highly Confidential

Q. Does that mean maybe?

A. Maybe.

Q. So a partition-tolerant blockchain system can be vulnerable to an involuntary fork?

A. It can be -- well, so involuntary, now, we need to dive into -- yes, it's definitely -- I -- it goes both ways. Both -- both worlds are possible.

Q. Okay. Why didn't you mention partition tolerance anywhere in your report?

A. Oh, I did.

Q. Oh, where?

A. I'm, like, whole my Appendix B. Whole my Appendix B is dealing with partitions. So, basically, I'm describing an attack to the -- to the -- XRP Ledger. This is assuming -- so this is apart from a dUNL. DUNL works correctly. The validator list site publishes consistently the same, UNL stored nodes. And now you can mount an attack in which you also introduce partitions to the network.

Q. Okay.

A. So that part is actually relying on that, and I call that unreliable network.

So now we talked about the asynchrony. We talked about partition network. And another way to say unreliable network. So you see, page 33, Appendix B, the third bullet, The network is called unreliable if it can drop and delay messages exchanged among correct validators. This is what I was trying to --

Q. I see that.

Now, Appendix B that you're pointing out here relates solely to scenarios for the XRP Ledger.

Correct?

A. Correct.

Q. Did your report talk about partition tolerance in relation to the bitcoin network?

A. My report did not talk about partition tolerance for the bitcoin network.

Q. Why not?

A. It's designed to -- one way to think about it is that, bitcoin network is meant for -- so the way it was built is that nodes can proceed independently from each other, if they're on the network partition. And that's by the feature of -- by the virtue of the -- that's

a feature -- that's actually -- you know, if we talk about operating as intended, this is operating as intended.

Q. So are you familiar with the CAP theorem?

A. I am.

Q. Okay. What's the CAP theorem?

A. CAP theorem is the basic distributed computing theorem that says that consistent -- CAP stands for consistency, availability, and partition tolerance. It's one way of stating -- restating the official Lynch-Patterson consultancy possibility result.

MS. ZORNBERG: Hold on.

Did you get that?

THE COURT REPORTER: I flagged it for a spelling. I will get the spelling later.

THE WITNESS: Thank you.

MS. ZORNBERG: Okay.

A. So it's another way to say that systems essentially if they're subject -- especially consensus systems, if they're subject to network partitions, they need to opt by design what property they will favor, when this

partition network happens.

By the way, again, as we discussed, you can design a system in which you opt not to tolerate partitions. This is usually ill-advised because partitions happen or not without your control. So they could happen just -- so now if you accept that partitions can happen, what the CAP theorem says is that the designer can pick, like on a high level, one -- two out of three properties.

Q. Two out of three. So the CAP theorem basically posits that there are trade-offs in designing --

A. Yes.

Q. -- distributed systems?

A. Yes.

Q. What does it mean -- let me rephrase.

Focusing on bitcoin for a moment, does bitcoin have partition tolerance?

A. It does.

Q. Are operational bitcoin nodes aware of whether they can reach all other operational bitcoin nodes?

A. I don't know. Normally they don't

know all matters. They don't even attempt. They usually sample the population of the whole network. So you're not -- in such a network, you're not even aware of how many nodes there are. So as such, you're not able to tell, can you reach all of the other nodes or not, because you're not even attempting.

Q. Okay. So -- so let me give you an example.

A. And you couldn't -- and you couldn't.

Q. Let me give you an example. If there were a eruption to the Internet connection between two countries, Country A and Country B, would bitcoin nodes operating in Country A know they could no longer reach nodes operating in Country B?

A. If they tried to reach them, they would know that they cannot.

Q. Through human contact?

A. No, not necessarily. If I'm connected, you know, if I know I'm connected to this and this IP address, then I can figure out that I am talking -- that this site here is -- is belongs to that country. I could basically

understand that my connection doesn't work. You can detect that in software.

Q. Okay. So sticking with the same example, if Alice submitted her transaction in Country A during a time when Country B was experiencing an Internet disruption, would her transaction be excluded from the bitcoin blockchain in Country B?

A. That really depends. So if network -- if Country A doesn't -- is unable to talk directly to Country B, because bitcoin operates on a gossip network, it might happen that there is a connection from A to B which goes via C, Country C. So A and C can -- A and C can talk. B and C can talk. And hence, you know, if subnetwork of -- that belongs to Country A of the miners that are located in Country A, they mine a bitcoin, they mine a block, they could be able to reach Country B, by the --

Q. Country --

A. Not necessarily. In a -- let's assume that the network splits in two, and then we can discuss that if you want to.

Q. Okay. Is it -- is it possible -- to

that example, is it also possible, that in the example I gave where there's an Internet disruption and Alice puts in her transaction in Country A, is it possible that bitcoin nodes in Country A, and Country B, would continue operating and adding new blocks independently?

A. There is a possibility. If the network is split into distinct parts that are completely unable to talk to each other, it is possible that the blockchain advances independently. Yes.

Q. That would be a fork?

A. That would be -- so at the -- at that moment, if you have a God's view on the system, you would call it a fork. At that moment, these nodes are not aware. They would be aware of -- so there are a lot -- lots of meanings of forks in this world, right? So this would be a fork on the blockchain as a data structure. Right?

Only when it comes together. So, once the network partition heals, these nodes start talking to each other. And how the bitcoin system is designed is it was actually designed -- the desired operation in that case

is that, when the network partition heals and nodes start talking to each other, bitcoin network just falls to this -- which longer fork. Basically, there is a history, this is Network A's blocks. This is Network B's blocks. You will take the longer one and default to that one -- not default, but actually the network reaches consensus on one of the two histories.

Q. Is any human intervention required to prevent a fork in the situation that we've been discussing?

A. We didn't discuss preventing the fork. But all what I described -- to maybe answer question, in all what I described no human intervention is needed.

Q. Okay. All right. On page 9 of your report, you talk about safety. And it looks like you basically explain that safety stipulates that bad things do not happen.

A. Yes.

Q. What is that based on, that definition based on?

A. My first -- the first time I encountered these two notions when Rachid

Guerraoui was teaching these notions -- Professor Rachid Guerraoui at EPFL was teaching these notions back in 2003. He used this wording. And this is common wording across scientific papers and across, you know, in different course, et cetera.

This is the way to explain on extremely high level. To give an intuition again, the wording here was adopted for the audience. And this is -- the one that even was used in introductory courses to us, as distributed systems designers. So, you know, this is a common thing to do. I didn't use it for the first time myself.

Q. Okay. Would you agree it's a good thing for a decentralized system to be safe?

MR. SYLVESTER: Objection.

A. We need to define "good," actually. So honestly, diving into that, it's a philosophical thing in the design of the system. For example, I was a lot -- spending a lot of my time working on systems that favor in the CAP theorem. So partition hits you and now you're a system designer picking one of the two.

[redacted] - Highly Confidential

So, we -- it turns out, to certain extent, this was the intention. The way I understand the XRP Ledger concerning this protocol, this was the intention of XRP Ledger designers. You tend to favor consistency. But it seems --so bitcoin was one of the systems that was opted.

So it's not a good thing or bad thing per se. You need to understand -- I would say it's good so long as the system behaves as you intended.

Q. Okay.

A. Yes. So I wouldn't say it's good or bad.

Q. Is safety necessary -- let me -- sorry. Let me rephrase.

Is it necessary for a decentralized system to be safe?

A. The safety can be specified in different ways.

So safety, yes, safety can be specified in different ways. So it's important that the safety is respected. Yes.

Q. I'm sorry. Are you saying that there

are different ways to understand safety?

A. Yeah. So safety is nothing bad. Nothing bad happens. So for the specific meaning, the specification of nothing bad happens when you go and specify the system, this would be different things.

Q. Okay.

A. So bad -- bad in bitcoin would be that -- one thing. And bad in -- in some other system would be something else. And they would both be considered the safety properties.

Q. How does the safety of a system bear on whether it is decentralized?

A. It does not.

Q. Does not. Okay. How do you measure the safety of a blockchain system?

A. You measure it -- well, measure is the -- there is a specification of safety. So the system will need to specify what it intends to do. What it tends to be done is split in safety and liveness.

Q. Okay.

A. Roughly speaking, safety means nothing bad will happen. And liveness means something

good will happen, so as you see the difference. It's easy to design safe systems. They don't do anything.

So that kind of by definition means nothing bad will happen. So you will not have force. You will not have whatever you can imagine. But that's not a useful system.

And then you have the liveness property that says, Okay, let's move on. Let's do something. And this is where the two --

Q. Okay.

A. -- things come.

Q. Is your definition of liveness as stipulating that good things eventually happen, is that based on literature or your professors? Or what is that based on?

A. Yes. Both. Both.

Q. Okay. What does it mean in your definition of liveness on page 9 that good things do eventually happen? What do you mean by "eventually"?

A. This means typically that if the system is let to be run for a very, very long time, eventually means unboundedly long time,

but you still wait and you don't know how much you will wait, but something will happen good, so it doesn't stop and just cease to be operational, right? That -- for eternity, right? So that would be not live.

Q. So what is -- can you quantify eventually? For a system to be -- for a system to have liveness, what's the outer range of how long someone would have to wait for a transaction to go through --

A. There are systems that even --

MR. SYLVESTER: Wait to answer. Wait for her to ask the question.

THE WITNESS: Yes. Sorry. Yes.

A. For some systems, they don't specify role. Usually depends -- it relates to the network. You remember we discussed this unreliable network. We discussed asynchronous network partition, forward network, et cetera. So it's related to this concept. So when you have a partition or unreliable network, it can last for very long time. You're not going to put a precise bound on that time.

Q. Okay. So your view is that a system

can be live with an unbounded degree of delay as long as it eventually goes through?

A. That is the -- often the case -- so liveness can be specified different. Liveness of the system could be specified. The system delivers a block every two seconds. You can specify it like that, like good luck in this world implementing that and maintaining that.

But it's usually, like, a relaxed requirement in the system.

Q. Is there any scientific agreement on a specific quantification of liveness?

A. So that --

MR. SYLVESTER: Objection.

A. There is agreement that it means, on a high level, what I'm describing here. There are different -- like, there are different -- different specification of safety. There are different specifications of the liveness. And this is totally normal, yes. You would still call it liveness and safety, but they would mean different things because they're attached to the system that satisfies these properties.

Q. Can a centralized system have

liveness?

A. It can.

Q. So how does measuring liveness tell you whether a system is it decentralized?

MR. SYLVESTER: Objection.

A. It doesn't. I didn't say it does. It doesn't.

Q. Okay.

MR. SYLVESTER: Just pause for a second for me to object.

THE WITNESS: Okay. Sorry.

MR. SYLVESTER: Thank you.

Q. Are there circumstances where by design, a blockchain system prioritizes safety over liveness?

A. There are.

Q. Can you give an example were?

A. Of a blockchain system?

Q. Yeah, that prioritizes safety over liveness.

A. Since we discussed -- since we admitted bitcoin Ethereum and XRP Ledger to be blockchain systems, in this world, it's XRP Ledger.

[redacted] - Highly Confidential

Q. XRP Ledger prioritizes safety over liveness?

A. Yes.

Q. Why do you say that?

A. Because in the cases of network partitions, it is designed to stop -- so, for example, if you have a partition which splits the network in two equal halves, XRP Ledger is designed to stop making progress. So it would wait for partition to heal, and two halves of the network to start to communicate to each other before you actually start that.

Q. Does prioritizing safety over liveness mean that a blockchain is not resilient?

A. It does not mean that, no.

Q. Okay. I want to talk about the Nakamoto coefficient, which you -- you reference on page 9 of your report, as we discussed earlier.

For the -- for the Nakamoto coefficient, you cite to reference number 19 in your report. What is that?

A. Again, for the -- the term, "Nakamoto coefficient," not the meaning, I spent some time

explaining where does the -- in the sentence before Nakamoto coefficient is introduced, I'm saying, Scientific and engineering literature uses this concept. So that's apart from calling it Nakamoto coefficient. I'm calling it Nakamoto coefficient for the purpose of bettering the ability of the document. It comes from Balaji Srinivasan, who is the ex-CTO of Coinbase.

THE COURT REPORTER: I'm sorry. Comes from what?

MS. ZORNBERG: I'll spell it.

THE WITNESS: Yes.

MS. ZORNBERG: First name, B-A-L-A-J-I. Last name, S-R-I-N-I-V-A-S-A-N.

A. Who was the ex-CTO of Coinbase, the publicly listed exchange. And in that sense, known figure in the space who used this term to denote the -- what's important to focus on is the definition of the notion that I'm trying to capture, not -- so, again, we could call it coefficient of Byzantine nodes, and this is my motivation to call it that way. I'm citing

either his blog post or YouTube --

Q. Right.

A. -- video in which he explains it. Yes.

Q. Okay. So, yeah, the -- the actual reference in your report cites to the YouTube video. Have you watched that YouTube video?

A. I did.

Q. When is the last time you watched it?

A. A few months ago. July, again.

Q. Have you also reviewed Mr. Srinivasan's blog post on the same subject?

A. I -- I read that blog post, yes.

Q. Okay. Do you consider Mr. Srinivasan an expert in blockchain systems?

A. I don't know if he was an expert or not. I considered that he is a known figure in the space.

Q. Did you consider the contents of his video to be reliable?

MR. SYLVESTER: Objection.

A. Reliable? How did you define "reliable"? The way we did few hours ago?

Q. That's fine.

A. Yes.

I think the -- the -- the notions that he discussed in that video, to my recollection, are pretty much reliable in a sense that, you know, it's pretty clear what he talks about in that blog post, yeah, or video.

Q. Have you ever spoken to Mr. Srinivasan about his use of the term "Nakamoto coefficient"?

A. No, I did not.

Q. Okay. Are you aware that the presentation that Mr. Srinivasan gave in that YouTube video was at the 2017 Blockstack Summit?

A. That sounds familiar, yes.

Q. Were you present?

A. No.

Q. Okay. So in the YouTube video, Mr. Srinivasan begins by saying that decentralization has not yet been quantified.

Do you recall that?

A. I don't recall word for word. I trust you. Yes.

Q. I'll proffer to you that he says in the video, quote, So everybody agrees that

decentralization is important. And the issue, though, is it hasn't yet been quantified.

Closed quote.

A. That is possible. We're talking 2017. For example, that seems to predate Troncoso paper. As we see in the recent years, there is more and more people. So if -- I don't know. You mentioned Neha Narula. You mentioned this. There is Balaji Srinivasan. I mentioned that. And there is an ongoing interest. But this is still 2017, and there is -- there are things happening in between.

Q. Okay. So you're not disputing that as of 2017, decentralization had not yet been quantified.

MR. SYLVESTER: Objection.

A. Again, the quantified, we would need to understand how you quantify, if you -- because discuss the measures or not -- what I could tell is that -- that understanding that I'm defending my report, which relates to the papers that we discuss and the understanding, that we, as a humanity and scientific community and blockchain communities and call it whatever

you like. It advanced since 2017. So pulling out -- I mean, not pulling out. Sorry. That's not the right word.

Quoting sources from 2017 may not be the right description of the -- of the situation that we are currently facing in understanding what decentralization is.

Q. How did Mr. Srinivasan derive the Nakamoto coefficient in the system that he presented in that presentation?

MR. SYLVESTER: Objection.

A. So my recollection of the -- of that YouTube video, so he uses it in the way I define it in this paper.

So this is the minimum number of authorities that the adversary needs to control in order to subvert key properties of the system.

He looks at Nakamoto coefficient, a different -- so most -- mostly he looks at Nakamoto coefficient in the terms of mining pools for bitcoin and Ethereum, which is what, I guess, people are doing. And I did it in my report, because we cannot -- it's really

difficult to understand.

Usually we assume that this Nakamoto coefficient for these two networks is considerably higher because the individual mining tool does not control all the miners in the pool. I could join one pool. I'm still controlling my miners with some methods I could detect if my mining pool -- my mining pool -- the mining pool that I'm contributing to is trying to subvert some of the key properties of the system. And if it happens, so I can decide to leave that pool. So the assumption that the pool operator -- the pool operators basically take a fee -- like 2 percent, 4 percent is a good ballpark. Don't quote me on this -- to even rewards of miners over time. So ordinarily, by joining the pool, you get less rewards. But you get them more often, and more evenly distributed, like. So --

Q. But --

A. Yes.

Q. I'm sorry. I think you've moved beyond my question.

A. Perhaps I did, yes. You want to

repeat?

Q. Well, I'll just move on.

Is there agreement in the scientific literature about how to measure the Nakamoto coefficient of a blockchain system?

A. In the Nakamoto coefficient, so, again, you use the Nakamoto coefficient the way I use it in -- in the report. So as the minimum number of authorities that the adversary needs to compromise in order to subvert key properties of the system, for the class of protocols that's not proof of work, that's kind of easier. Because you would always have a threshold of faulty -- all XRP Ledger has it. It's not only XRP Ledger. Other protocols that are -- belong, let's call it, to this family of protocols have that threshold.

It's easier to estimate this than, for example, for proof of work. I was digressing a moment ago, trying to explain the difficulties of estimating that and proof of work. But actually, in other consensus protocols, it may be and it often is much easier.

Q. Do you know if everyone in the

[redacted] - Highly Confidential

scientific community uses the term "Nakamoto coefficient" the same way you do in your report?

A. I'm pretty sure there are some researchers who don't know about the exact term. If we define it for them -- and this is what I would -- you know, this is the essence of it. Like, one should focus when it reads my report on the definition, what it means.

And we can call it, you know, if we can call it -- we'll call it [redacted] partition. We can call it that way. If you want to call it coefficient of Byzantine nodes, we can call it that way. Or Nakamoto coefficient, we can call it that way. That's less -- that's a handle which we use to refer to the concept.

Q. Just for clarity, when you use Nakamoto coefficient in your report, you're using it as a shorthand for your own definition that's provided in the sentence prior that you read into the record.

A. No. I wouldn't agree fully. I -- it's not my definition. It's the definition that I wrote in the report.

In that sense, it's my definition.

[redacted] - Highly Confidential

But it's not that I came up with it. As you see, I'm writing about scientific and engineering community has been using this for a very long time.

Q. Okay.

MR. SYLVESTER: Lisa, we've been going for about an hour, so whenever is a good time to take a quick break.

MS. ZORNBERG: I would like to finish on this -- on this note.

Q. Does Mr. Srinivasan derive his use of the Nakamoto coefficient from the Lorenz curve and the Gini coefficient?

A. He does not. He relates to them, but he does not. So that's one of the points in the Adriaens rebuttal that's misrepresenting the facts.

Q. Okay. Let me show you Exhibit [redacted] 10.

MS. ZORNBERG: Mark, once we get through this exhibit, we can take a break.

MR. SYLVESTER: Do you know about how long it will be?

MS. ZORNBERG: I don't know. Hopefully not too long.

[redacted] - Highly Confidential

MR. SYLVESTER: You let me know if you're flagging and need a break.

THE WITNESS: I could use a break.

MR. SYLVESTER: Can we just take one now, Lisa? He's saying he needs a break.

MS. ZORNBERG: That's fine.

MR. SYLVESTER: Thanks.

THE VIDEOGRAPHER: The time is 2:41 p.m. We're going off the record.

(Recess from 2:41 to 2:59.)

THE VIDEOGRAPHER: It is 2:59 p.m. We are back on the record.

Q. Dr. [redacted] I've handed you Exhibit [redacted] 10, which I'm going to represent to you has -- shows two slides, from the video presentation that Balaji Srinivasan gave called quantifying decentralization that you cite in your report.

Page 1 of the --

MR. SYLVESTER: Counsel, do you have all the slides for context? Or just two from the presentation?

MS. ZORNBERG: We have these two.

MR. SYLVESTER: Okay.

[redacted] - Highly Confidential

MS. ZORNBERG: I can't say for sure whether they're the only two or not.

MR. SYLVESTER: Okay.

("Quantifying Decentralization," Blockstack Summit 2017, was marked [redacted] Exhibit 10 for identification, as of this date.)

Q. Page -- the slide on page 1 of Exhibit 10 is from four minutes in, and the slide on page 2 of Exhibit 10 is from Minute 12 of the presentation.

So directing your attention to page 1 of Exhibit 10, the slide that Mr. Srinivasan titled "Six Subsystems of the Bitcoin Decentralized System."

Do you agree that those are subsystems of the bitcoin blockchain system?

A. I do not.

Q. Okay. Why don't you agree?

A. Exchange is not a subsystem or a bitcoin decentralized system.

It has nothing to do -- bitcoin doesn't care if there is an exchange or not.

Q. Okay. Mr. Srinivasan also includes a

[redacted] - Highly Confidential

subsystem for nodes by country.

Do you agree that's a subsystem of the bitcoin network?

A. I don't know necessarily what "nodes by country" means here.

Q. Okay. Your report did not analyze nodes by country for bitcoin Ethereum or XRP Ledger, correct?

A. No. I'm referring to Srinivasan to get a handle on the name of this concept.

Q. Okay. So you don't contend that you're using Nakamoto coefficient in the same way, necessarily, as Mr. Srinivasan.

A. I would say one of the users of Nakamoto coefficient he has is the one that I'm using it for. I'm not necessarily saying that I'm using it in the -- all the -- I didn't go -- I didn't talk to the guy. I don't know the guy personally. I don't know how he thinks about it.

I saw the mapping. And I think it's fair to say that this concept that I call Nakamoto coefficient is sometimes called Nakamoto coefficient because I'm pretty sure he

does it in that aspect. And that's where the handle comes.

Q. Mr. Srinivasan roughly defined Nakamoto coefficient during his presentation as, quote, How many folks do you need to compromise to get to 51 percent?

Closed quote.

Do you agree with that formulation? Is that -- let me put it this way: Is that formulation similar or different than the one you use in your report?

A. You said how many guys.

Q. I'm quoting from him. How many folks do you --

A. Folks.

Q. -- need to compromise to get to 51 percent?

A. I'm using it in a different way. So I'm trying to make more -- to specify folks more precisely. So we are talking about the authorities that are contributing to the system in some -- in some way, right? So they control certain components of the system.

Q. What's an authority, as you use it, in

talking about Nakamoto coefficient?

A. I use it -- so authorities would be, in the XRP Ledger, the organizations that run the validator nodes.

Q. I'm sorry. Say it again.

A. The XRP Ledger, the organizations that run the validator nodes. In the bitcoin blockchain, the entities that run, we can say full nodes or miner nodes. It depends. But you can extend to full node.

If we say, for XRP Ledger, validators, it would be only fair to talk about bitcoin full nodes, so yes.

Q. Okay. So did I understand that if you are going to do an apples-to-apples comparison of XRP Ledger to bitcoin, the -- the right comparison would be running a validator node on XRP Ledger to running a full node on bitcoin or Ethereum?

A. We need to define apples to apples, but it's not the same. It's -- no. I didn't say that. That's absolutely -- I didn't say that.

I didn't mean that.

[redacted] - Highly Confidential

Q. So I'm just going to read back your answer, make sure I understand what you are saying.

What you previously said is, quote, I'm sorry. Say it again. The XRP Company, the organizations that run the validator nodes, in the bitcoin blockchain, entities that run, we can say full nodes or miner nodes. It depends. But you can extend to full nodes. If we say for XRP Ledger validators, it would only be fair to talk about bitcoin full nodes. So yes.

Closed quote.

Explain -- it seems like you, as a matter of fairness, were saying you should compare XRP Ledger validators to bitcoin full nodes.

Is that -- is that accurate?

MR. SYLVESTER: Objection.

A. I don't think it's accurate. We would need to define "fairness."

Q. Well, what did you mean by that statement? And if you want to correct it, please do.

A. Yes.

[redacted] - Highly Confidential

There are certain similarities among the -- but there is also deference, so it's not apples-to-apples comparison. One would relate, to a certain extent. And we can define precisely how, XRP Ledger validators to bitcoin full nodes.

It's not necessarily fair to call them miners, miners, to relay them to miners, because the miners get rewards for their engagement in the bitcoin blockchain. Where actually, validators on the XRP Ledger, they do not.

But then, again, it's not fully correct to say that XRP Ledger validators are to be thought of as full nodes on the bitcoin blockchain. Because there is a certain security aspect that, for example, if I'm running the bitcoin full node validator and I'm running a -- a XRP Ledger validator which is not in the main -- which is not in the dUNLs that we discussed, there is a certain difference. So the difference is mainly because in the XRP Ledger -- shall I carry on?

Q. Not necessarily. No.

A. Okay --

Q. We can --

A. If you're happy --

Q. If you feel your answer is complete, then --

A. No. If you -- you were unhappy with my phrasing, so I'm trying to phrase. So if you're happy, I can stop. If you're not happy, I can continue.

Q. So my happiness is irrelevant as long as you feel that you're giving accurate and complete testimony.

A. I -- I -- you know, I am certainly. I can continue discussing this. It's an interesting point.

Q. Let me ask you a follow-up question.

A. Yes.

Q. And we'll go from there.

You mentioned that -- that miners get rewards. Do -- do bitcoin participants who operate nodes get rewards who are not miners?

A. Can you rephrase, please?

Q. Are there rewards in the bitcoin system for validation?

A. There are no monetary rewards, like

there is monetary meaning in bitcoin token. There are no rewards for that.

There are certain rewards. If you think about contributing to the security of the system, it's actually relevant. And there -- individually, I may get as a user who is running -- not I. Whoever runs the bitcoin validator node may get more privacy if he does so in certain cases, which we can discuss.

Q. Okay.

A. So rewards in the terms of bitcoin tokens, there are not.

Q. Okay. Let me direct your -- hold on.

You run a bitcoin node presently, right?

A. I run a bitcoin full node presently.

Q. Do you receive any in-protocol incentives for doing that?

A. In-protocol incentives? The way I -- the way I consider them in the -- in the report.

Q. Yeah.

A. No. So, no, no bitcoin is awarded for running the validator.

Q. Okay. Let me direct you to the second

page of Exhibit 10, which, again, is a slide that Mr. Srinivasan displayed during his presentation, which you referred to in your report.

According to this slide, Mr. Srinivasan determined that both bitcoin and Ethereum had a Nakamoto coefficient of 1.

Do you see that?

A. I see that.

Q. Do you know how he determined that the Nakamoto coefficient for bitcoin was 1?

A. Looking at his columns, what he did is that -- what I assume he did -- I cannot know for sure -- what I'm assuming here that he did is he took the minimum of the bitcoin column, so basically mining says 5. Client says 1. Developer says 5. Exchange says 5. Nodes says 171. Owner says 3. And similar for Ethereum, this looks like taking the minimum out of these columns.

Q. Okay. According to your report, if the Nakamoto coefficient is 1, a system cannot be deemed decentralized. Right?

A. Yes. I'm not saying what he did is

correct.

Q. Are you saying that what he did is incorrect?

A. I would -- I would argue with him that this is incorrect, yes.

Q. Why did you cite his YouTube video in support -- as one of the 22 references your report relies on if you thought his analysis of Nakamoto coefficient was incorrect?

MR. SYLVESTER: Objection.

A. I'm using it in the way I cited it.

Q. Okay.

A. This notion is sometimes called Nakamoto coefficient.

Q. Okay. Can I direct you to page 9 of your report.

A. Yes.

Q. Besides Mr. Srinivasan's YouTube video, do you cite any other authorities for the term "Nakamoto coefficient" in your report?

A. I refer to the scientific literature and engineering practice, which is -- I'm reading this out verbatim again.

It's typically interested. And

herein, typically interested and scientific engineering and literature engineering practice, I am referring to my experience working on these protocols for 18 years.

Q. Okay.

A. They're interested in the minimum number of authorities that the adversary needs to compromise to subvert the key property of the system.

Again, we are getting into names.

Q. Okay. Understood. But my question was really just a simple one. For your use of the term "Nakamoto coefficient," does your report cite to any authority other than Mr. Srinivasan's YouTube video?

A. It refers to scientific literature, engineering practice. If you want a citation in the form that something concretely appears, it does not.

Q. Okay.

A. But there is a reference to how people approach these things.

Q. Okay. So Mr. Srinivasan's YouTube video is the only citation for your use of the

term "Nakamoto coefficient," and Mr. Srinivasan found Nakamoto coefficient of 1 for both bitcoin and Ethereum?

MR. SYLVESTER: Objection.

Q. Correct?

A. It is not correct. So I'm saying that this concept is sometimes referred to as the Nakamoto coefficient. Implicitly, I'm referring to scientific literature engineering practice without explicitly pointing out to what I mean here.

Q. Okay.

A. But there is a clear indication that I'm referring to the larger body of literature, which is not explicitly cited.

Q. What scientific literature are you referring to?

A. This is a virtually all -- all protocols that I have been working on for -- looking at it 18 years. So I have these assumptions in my Ph.D. thesis. Leslie Lamport has this notion that can relate to this in his 1980s paper. Miguel Castro and Barbara Liskov, Turing Award winners, researchers at that time

at MIT who invented the PBFT protocol, have a similar concept.

THE COURT REPORTER: Slow down, please.

THE WITNESS: Yes.

A. So one can relate to these notions in multiple scientific papers.

And these are called the threshold of Byzantine nodes, threshold -- adversarial threshold or similar names. We discussed this a few hours ago.

Q. Okay.

A. I'm giving it a name, and it's just a name.

Q. You talked about mining pools a little while ago.

A. I did.

Q. In the bitcoin -- I have a clarifying question.

In the bitcoin system, let's say that Jeff controls Alice and Bob.

Does that count as one for the Nakamoto coefficient as you're using it or as three?

[redacted] - Highly Confidential

MR. SYLVESTER: Objection.

A. Can you repeat the question? How many participants are there?

Q. Well, I -- there are three in my hypothetical. So my hypothetical is Jeff controls Alice and Bob in the mining pool.

A. Who is --

Q. Does that count as one or as three?

MR. SYLVESTER: Objection.

A. Who is Jeff?

Alice and Bob are running validator nodes, but Jeff controls them. Jeff, mining pool operator? Or --

Q. Yeah, let's assume he's a mining pool operator.

A. What does it mean, controls? So whatever Jeff decides, Alice and Bob implement?

Q. Yes.

A. It would be one.

Q. Okay.

Okay. Now, your report evaluates bitcoin's resilience to the double-spend issue and to the censorship-of-transactions issue.

Correct?

[redacted] - Highly Confidential

A. Correct.

Q. Are there any other elements to resilience besides the double-spend and censorship resistance that you're offering an opinion about?

A. These are not elements of resilience. Resilience applies to different -- to ensuring different properties of the system. You just mentioned the different properties of the system.

Resilience would be, despite how many Byzantine components of the system, do we still reserve safety and liveness? So these are not -- we discussed safety -- I think we discussed this before. In safety, a measure of resilience -- I'm -- I'm paraphrasing this, but -- yeah.

Q. Okay.

So let's focus on double-spend. Why is -- why is the issue of double-spend relevant to decentralization?

A. I didn't write that it's relevant to decentralization.

Q. Okay.

[redacted] - Highly Confidential

A. I wrote something else.

Q. Okay. Is it -- is it your opinion that the double-spend issue is -- is a separate -- separate and apart from whether a system is decentralized?

A. Double-spend, the -- I'm giving it as an example. If you read page 9, it says, Informally, a safety property of a system stipulates that bad things do not happen.

An example of a safety property, in the context of blockchains, is double-spend resistance.

Q. I understood. So double-spend and censorship resistance are examples that you're giving that relate to safety?

A. That is not fully correct. So double-spend relates to safety. Censorship resistance relates to liveness.

Q. Okay. So let's talk about double-spend resistance.

What do you conclude with regard to bitcoin's resilience to double-spend?

A. Just to find in the --

Q. I think it's on page 15 of your report

if you're looking for a reference.

A. Yes. Shall I read it out? I found it.

Q. No. I don't need to you read it out.

Can you summarize, or can you just point out --

A. Yes.

Q. -- where your conclusion is stated?

A. Let me -- let me read -- these two paragraphs, and then I will summarize it if you don't want me to read it out.

(Witness reviewing document.)

A. So I'm giving an example of how an adversary which controls more than 50 percent of the mining power, I'm giving high-level examples what the adversary would need to do in order to mount double-spending attacks and transaction-censoring attacks. This is what I'm doing in this paragraph.

Q. Okay. So -- so it's your opinion, as expressed here, that more than 50 percent of bitcoin mining power is controlled by four mining pools. Correct? As of the date of your report.

[redacted] - Highly Confidential

A. I'm not saying that. I'm saying that, if we assume that the mining pool operator controls -- and that's a big assumption. It's not necessarily realistic.

If a mining pool controls all the nodes in the mining pool, then four mining pools control together 51 percent of the whole mining power. Why is this not the case?

Q. Okay. Did you answer --

A. Yes.

Q. Let me direct you -- let me direct you to the sentence on page 15, three-quarters down, where you wrote, With this in mind, at the time of writing this report, more than 50 percent of bitcoin mining power is controlled by four mining pools.

Do you see that?

A. I see that.

Q. You did not offer a citation in support of that figure in your report. Right?

A. I did not. This is correct.

Q. Where did you derive your assertion that as of October 4, 2021, more than 50 percent of bitcoin mining power was controlled by four

mining pools?

A. I do not recall, unfortunately, the sources precisely. I saw that number in -- I verified it myself on certain websites that -- that indicate how much mining power is controlled by which mining pool. Mining pool often -- often identify themselves. When they mine a block, they have -- some of them identify themselves. It's possible to identify them.

Q. What websites did you rely on, in -- for that factual statement in your report?

A. I'm not saying this here. And I don't -- I cannot quote from top of my head the exact website. I also read, just to finish my -- I didn't finish my response.

So there are also other scientific papers that actually come to this number. So that's -- it's not -- the moment that I looked at it, at the moment I looked at it, I'm pretty sure I looked at certain websites that track the mining power, because the miners tend to, again, identify themselves, some of them.

Q. Okay. But you don't remember -- you make a statement that as of the writing of this

report, more than 50 percent of bitcoin mining power is controlled by four mining pools. Is it your testimony that for that figure, as of when you wrote this report, you looked at websites that you can no longer recall?

A. That I cannot recall from my head? If I start searching, if I would be starting searching it, I could probably tell you how got it and why do I think this is -- this is reliable.

Q. Why did you not identify those websites, in your report, among the information that you considered?

A. It was not my intention to hide any information. You can call it an omission, if you want, or oversight.

You can call it however you want. But it was not my intention to note, Aha, I want to give this information and hide this source.

I didn't think like that.

Q. How can we know if the websites that you relied on for that factual statement are reliable?

A. I -- did my best and honest work to at

think at that moment that they're reliable. So they're not hidden websites. So reliable in a sense that somebody could go, estimating, you could probably get a historical -- you know, you could go back and try to understand what I was doing in July and August. So that would be repeatable in a sense that we did find reliable.

And I think this is doable by an independent researcher, to verify these claims.

Q. You agree that the percentage of mining power that's controlled by mining pools can change over time, correct?

A. I agree with that.

Q. It can change day to day, right?

A. It can change minute by minute if you want, yes.

Q. Sitting here today, do you have any basis to assert that the websites you recall looking at, for that sentence of your report, were reliable?

A. I have -- and this is not -- again this is not the -- this is not the only source. So there are scientific papers -- some of them we -- I think we brought up today -- that

[redacted] - Highly Confidential

actually look at the same metrics, and they come with the similar numbers.

So --

Q. And were those papers -- were there any papers that you looked at that gave a factual statement of the percentage of mining power, controlled by mining pools, as of October 4, 2021?

A. I would say, at that moment when I was writing this, I had these papers in mind. And -- but I was verifying this on these websites, this information from these websites that I was referring to.

Q. And you -- you agree it's an omission in your report that you did not cite the websites?

A. I --

MR. SYLVESTER: Objection.

A. -- said you can call it an omission. I didn't say I agree. Yes. So it's something that I didn't measure this for the first time myself.

And like I didn't cite -- explicitly, when I introduced the Nakamoto coefficient, I

didn't cite the body of literature. This is not because I'm hiding references or something.

When I do this, it's mostly because I think this is so easily verifiable that I almost don't need to do it. This is my line of work, rather than hiding information from anyone who could be reading this report.

Q. Will you agree that if one mining pool was in control of more than 50 percent of bitcoin mining power, the -- the Nakamoto coefficient for bitcoin would be 1?

A. I would agree that the very conservative estimate as I write it in report, under the assumption that a mining pool operator authority controls all the nodes inside the mining pool and only -- and under that assumption, yes. Then yes.

Q. Okay. Has that occurred at any time if bitcoin's history, to your knowledge? And by that occurring, are you aware of any time in bitcoin's history when one mining pool controlled more than 50 percent of bitcoin mining power?

A. I'm aware of certain -- certain --

[redacted] - Highly Confidential

I'll just point to -- not necessarily scientific authors, maybe -- maybe even -- yes, I'm aware that -- I suspect that in 2014, this occurred.

And, you know, you could arguably make a statement in the very early days. We don't know -- Satoshi Nakamoto is a group of independent people or a single people, but you could probably go back at the very beginning of bitcoin blockchain and said -- make such a claim.

So I'm aware of people making such a claim. Again, one should be very careful. There a big assumption about -- when we talk about mining pools, so fast-forward to 2014 and present days, there is this -- this is a very conservative assumption in which you really assume that the mining pool operator controls all the nodes. This is normally not -- not true.

Q. Okay.

MS. ZORNBERG: Can you show Exhibit [redacted] 11.

(Article Dated June 16, 2014, "Bitcoin Currency Could Have Been Destroyed by 51

[redacted] - Highly Confidential

Percent Attack," was marked [redacted] Exhibit 11 for identification, as of this date.)

MS. ZORNBERG: For the record, Exhibit [redacted] 11 is an article dated June 16, 2014, called "Bitcoin Currency Could Have Been Destroyed by 51 Percent Attack."

Q. Please take a moment to look at it. But my question is, when you mentioned a moment ago that you believed there was a time in 2014 when there was more than 50 percent concentration of bitcoin's mining power, were you referring to the incident that's described in this article?

MR. SYLVESTER: Take a minute to read the article if you haven't seen it before.

(Witness reviewing document.)

Q. Dr. [redacted] have you had a chance to look at it?

A. I didn't finish, but I guess, you know, we could -- just maybe just 30 seconds more.

Q. Okay.

(Witness reviewing document.)

A. Yes, I had a chance to look at it.

Thank you.

Q. So is the 2014 incident described in this article, when a mining pool called GHash.io, spelled G-H-A-S-H.I-O, mining pool, controlled more than 51 percent of the mining power of bitcoin?

A. GHash.io, yeah.

Q. So let me just rephrase it cleanly. When you talked about, earlier, a 2014 incident when the mining pool concentration of bitcoin exceeded 50 percent, were you referring to the -- the GHash.io incident?

A. GHash.io. I believe this is the same thing because I was talking about 2014. I'm pretty sure that the -- it's very probable or I'm pretty sure that I'm -- I was not looking at the guardian document that you presented, but, you know, different sources might have referred to the same incident.

Q. Okay.

A. So, I believe it is fair to say I was thinking of that. Yeah.

Q. So at the point of this 2014 incident, would the Nakamoto coefficient of bitcoin have

been 1, according to your analysis?

A. According to my analysis, a very conservative estimate of the Nakamoto coefficient would be 1.

Q. Did it require human intervention to avoid a threat in 2014 to bitcoin's safety and liveness?

MR. SYLVESTER: Objection.

A. I couldn't know if it -- required human intervention. It would be speculating for me to understand if, you know, you could write a software which immediately leaves the pool if, you know, you are looking at something and you says, Oh -- you could do it both ways.

Q. Okay. On page 2 of the article, the writer of the article writes, quote, For the brief period when GHash had 51 percent of the network, the security of bitcoin wasn't a result of its impressive mathematical background but merely the trust that the users of GHash would notice and respond if the pool's administrators decided to try and abuse their position, close quote.

Do you see that?

[redacted] - Highly Confidential

A. I lost you. Sorry. I apologize. I lost you.

Q. It's the middle of page 2.

A. Middle of page 2.

For the brief period when GHash had 51 percent of the network, that paragraph?

Q. Yes.

And my question is, do you agree that that's a fair statement?

MR. SYLVESTER: Objection. Foundation.

A. This is a -- this is an article for newspaper.

And I don't agree that the security of bitcoin wasn't a result of its impressive mathematical background, but merely the trust that the users would notice and respond.

There is a -- there is an incentive once you start playing this game, and I'm referring to this in -- in my report. Once you start playing this game of bitcoin, now assume this happens -- let -- let's suppose that this actually happened, and it happens today.

So now currently, you're controlling

51 percent of the mining power. Normally what this means is that you are mining to get some bitcoin rewards, and now you're facing the dilemma, even if you could do it, is it good for you.

If you are selfish, rational, economic player, is it good for you to do it or not, because you might -- you know, by mounting an attack, you might be devaluing the trust in the network, and that's actually integral part of bitcoin, if you see what I mean.

So that dilemma that you are having, even if you could somehow theoretically mount the attack -- I don't know, U.S. governments engages few nuclear power plants, starts mining bitcoin, it gets to 51 percent. Now, does it want to attack the network or does it want to continue mining bitcoin because it's -- because other -- you see what I mean.

So there is this part of the game which is very difficult to say -- for example, if the author says, The security of bitcoin wasn't a result of its impressive mathematical background. If I add game theory, game theory

[redacted] - Highly Confidential

is part of mathematics. That's a part of bitcoin's background.

MR. SYLVESTER: You asked him if he agreed. Let him finish.

A. Yes. So I could not agree with this. It's a sensational article, and there are certain challenges, of course, if you have 51 percent of the network, but there are hidden -- not hidden aspects, there are actually aspects of the whole game, theoretical background of bitcoin, which is part of its mathematical background, which actually puts you in a dilemma of, when you're an attacker, Do I want to do this or not.

Q. So are -- are you saying that someone with 51 percent control might have incentives to act in a trustworthy manner?

A. Yes.

Q. Okay.

Are you aware of any human activity, in connection with the -- with the bitcoin network, to prevent specific mining pools from reaching 51 percent control?

A. I cannot comment on that. I don't

have any firsthand experience with it.

Q. Okay.

While we're on the topic of double-spend, are you familiar with bitcoin CVE-2018-17144?

A. I think this is -- I think I'm aware of what you're discussing, yes.

Q. Okay.

What is a CVE?

A. I don't know exactly what CVE stands for.

Q. Okay.

If I told you it stood for a common vulnerabilities and exposure report, does that sound familiar?

A. Fair enough.

Q. Okay. What do you recall of the -- of the vulnerability that was at issue in CVE-2018-17144?

A. To give you an objective precise statement, I would need to refer to certain documents.

What I recall from top of my head is that there was a change in the bitcoin software

introduced in bitcoin core Version 0.14 to optimize certain performance of the bitcoin software.

Inadvertently or not, this change we're introducing a vulnerability that -- that a user could double -- to attempt to double-spend the same inputs.

Because of the way bitcoin works, you're spending certain outputs of a transaction, so if you use the same input twice, you're spending the -- if you're using the same output of a previous transaction twice as the input to your transaction, you're basically kind of attempting to double-spend in some sense.

So like I have one bitcoin, but I actually use it twice. So I'm kind of trying to spend two bitcoins, and the vulnerability, actually, was -- when it was first disclosed, it was the -- that basically this would crash a bitcoin 0.14, bitcoin core.

Q. Was a -- was a fix required to the bitcoin software to resolve that issue?

A. Depends. So if you are running the software before bitcoin Version 0.14, it was

not.

If you use -- because, you know, this bug didn't exist -- if you call it a bug, this didn't exist before 0.14. So if you ran a node on 0. -- prior version to 0.14, you wouldn't be required to change software, and it wouldn't crash your machine.

Q. But if you were running the 0.4 version of bitcoin so that you had the bug in your system, then you needed to download a -- a fix to the bitcoin software.

A. You would need either to revert, as you would not necessarily need to download. There is a world in which you are reverting back to a prior version of the code. Let's say you have 0.13. On your machine you can install that one.

Normally, this would -- so it's reasonable to expect that more often than not, this would -- for an operator of the node, this would take some manual intervention. I could imagine that you could write scripts if your bitcoin machine starts failing, that it reverts back to some previous item of the software, so

we cannot vouch that it would require human intervention.

But it's possible that it would require intervention of a human operator of a node if it was running 0.14.

Q. Okay. So now I want to talk about your analysis of censorship resistance in the bitcoin system.

Are nodes required to accept all proposed transactions into their block on the bitcoin system?

A. What is a node?

Q. Do you know what a bitcoin node is?

A. I know, but like what are we talking about here? So is it the bitcoin miner who gets the transactions from the mempool. Is it the validator node who gets the mine block and validates transactions? What are we talking about?

Q. Okay. I'm talking about a miner node. Is a miner -- is a mining node required to accept all proposed transactions into their block?

A. A miner is free to decide on its own

which transactions it wants to include in the block. It is incentivized by the bitcoin in protocol incentives to essentially -- if it's a rational economic player, it's incentivized to select the transactions that carry the most transaction fees.

Q. So, a miner can refuse to accept transactions on the bitcoin network?

MR. SYLVESTER: Objection.

A. The miner could not opt to selectively include certain transactions or not in the blocks that it is mining.

Q. And -- and the miner can do that unilaterally?

A. The miner can do that unilaterally -- it depends. If it joins the mining pool, then somehow, sometimes the answer is no.

If the miner is independent miner, it's fair to say that it can do it unilaterally.

Q. So if a mining pool can censor transactions unilaterally, shouldn't that make the bitcoins Nakamoto coefficient 1, under your analysis?

MR. SYLVESTER: Objection.

A. No.

Q. Why not?

A. Because that's not correct.

Q. Why is it not correct?

A. It's not correct that if a mining pool can opt which transactions to include, there are other mining pools that can opt to include the transaction.

So that wouldn't be censoring the transaction, so if you want -- if the -- so what you would get, effectively, is that the smaller fraction, the smaller mining -- the complete mining power that actually tries to include this transaction in the blockchain is smaller than 100 percent.

And in principle, what it could do is it could delay -- effectively it might delay a transaction for a certain time.

In order to exclude the transaction, as I write my report, to completely exclude the transaction, or the longer period of time and to mount the censorship attacks, we need to have 51 percent of the computing power of the cash power in the network dedicated and really

committed to excluding this transaction, and yes, they can do it; I mentioned it in my report.

Q. So if a mining node on bitcoin can unilaterally refuse to accept a transaction, are you saying that transaction might have to be resubmitted?

A. This is -- this is what's happening, yes.

It depends, so I mean, you know, it might never reach the -- yeah. I think --

Q. Okay.

A. -- I think it's clear.

Q. Let me direct you to page 9-- page 18 of your report.

Okay. And I'm turning now to your analysis of Ethereum resilience.

So, on the -- that paragraph on page 18, you make the statement, quote, At the time of writing of this report, more than 50 percent of Ethereum mining power is controlled by three mining pools, making the conservative estimate of the Nakamoto coefficient for Ethereum equal to 3, period,

[redacted] - Highly Confidential

close quote.

Do you see that?

A. I see that.

Q. You do not offer any citation for that factual statement in your report, correct?

A. This is correct. And to explain that, if I can expect your next question. Or you want to pose it?

Q. I'd rather pose my questions --

A. Please.

Q. -- just since we're getting late in the day.

A. Yes.

Q. Thank you, Doctor.

From where did you derive your assertion that more than 50 percent of Ethereum mining power is controlled by three mining pools as of the writing of your report?

A. That would be the same approach that I meant -- that I mentioned for bitcoin.

Q. Same websites?

A. It might be different websites. I -- I, unfortunately, cannot recall from top of my head. It might be the same website which

[redacted] - Highly Confidential

aggregate information across different blockchains.

Again, this is something -- so these -- these websites usually -- you know, I think this is verifiable because --

Q. Okay.

A. Yeah, I think this is verifiable.

Q. But --

A. Even -- even if I didn't give the -- that -- there are just many websites that do it. There -- there are many researchers that --

Q. Okay.

A. -- came to similar conclusions, so they use -- apparently science -- scientists use this different information, and this information is accessible.

I did my honest work to present this honestly at the time of writing.

Q. Okay.

Let's turn -- by the way, would you agree that it's -- as with bitcoin, for Ethereum, it's possible for one mining pool to control more than 50 percent of Ethereum's mining power?

[redacted] - Highly Confidential

MR. SYLVESTER: Objection.

A. I would say we can relate to what we discussed with bitcoin -- for bitcoin, and since the consensus protocols are similar, I think it would be fair to say that it's possible that a single mining pool, on the Ethereum network, controls more than 50 percent of the hash power.

Q. All right. Let's -- let's turn now to your evaluation of the resilience of the XRP Ledger, which you analyze on page 22 of your report.

We looked at this earlier today. Is the -- is the main conclusion or opinion offered that the -- the existence of the dUNL, or a dUNL, impairs the resilience of the XRP Ledger?

MR. SYLVESTER: Objection.

A. Can you repeat the question?

Q. Well, how would you state it? How would you state -- what is your opinion about the resilience of the XRP Ledger?

A. My opinion is -- of the XRP Ledger resilience is that it doesn't tolerate single -- basically a single authority, being Byzantine, and the single authority is the one that serves

in the release, 1.7.3, the dUNL.

I'm giving a simple example, but there are other examples. I would like to point out that this is not the only example of the attack that could happen.

So, I'm describing later the other possible -- some other possible attacks that may happen from the untrusted validator list sites that serves the d-- dUNL to the node.

Q. When you say "other examples," are you referring to other examples in your report?

A. Yes.

Q. Okay. In your analysis of resilience for the XRP Ledger, why did you not evaluate the ledger's double-spend resistance in the way that you did for bitcoin and Ethereum?

A. In a sense, I did.

So the -- the entire Section 4 of the report.

Q. Okay. So please identify where -- where in your report you specifically evaluated the double-spend resistance of the XRP Ledger.

A. For instance, and I will read -- I will need to read in more details this section

to point you out to possible other examples.

But the double-spending is stated as a challenge on page 20, in the first paragraph, where I'm quoting the Chase/MacBrough paper, and actually, when I say, Faces the same challenges as other digital assets in preventing double-spending and insuring network-wide consensus, this is the citation from the Brad Chase and Ethan MacBrough paper.

Q. So I --

A. -- I notice --

Q. I -- that -- that -- just to pause there. So you're identifying that the XRP Ledger, like other blockchain systems, have to deal with double-spend and have to deal with insuring network wide consensus. Right?

A. So, yeah, if you read this section, I'm really putting my words in the brackets. So I was trying to be careful here what are my words and what I get from the sources that are given by Ripple employees.

So whenever something is not in brackets prefaced by my initials, this is what I'm getting from one of the four sources that I

[redacted] - Highly Confidential

cite in Section 4.1.

Q. So my question is, where in your report -- other than identifying that the XRP Ledger has to face the double-spend issue, where do you address how it does so?

A. For example, if you go to page 21.

And the second paragraph in Section 4.1.2, "Consensus and Validation," the second paragraph talks about the goal of the XRP Ledger consensus protocol.

And then the third sentence --

Q. Well, where -- yeah.

A. -- or the second sentence, I say, Roughly speaking, these properties are related to double-spending prevention and censorship resistance.

The following sentence, the third sentence of the second paragraph of the Section 4.1.2 says that, Formally, safety properties relevant to XRP Ledger consensus protocol are agreement in linearizability.

Q. Okay.

A. Quoting Chase/MacBrough paper, which essentially mandates that correct validators

fully validate transactions in the same global order, in the brackets, hence, preventing double-spending.

From that moment on, when I talk about safety properties of XRP Ledger, they are, at this moment, tied to double-spending. And this is the moment I establish the connection.

Q. Do you have an opinion that you're offering in this case on the effectiveness of the XRP Ledger in preventing double-spend?

A. I am offering the opinions of which requirements -- what is necessary for XRP Ledger to actually prevent double-spends.

I relied on the Chase/MacBrough paper. I relied on my inspection of the critical parts of the safety part of the consensus protocol.

I was also investigating whether this part of the protocol changed since Chase/MacBrough publish their paper, until the point I was submitting my report. And this was suggesting that -- this is -- basically this is a valid understanding of -- of the protocol.

So --

Q. So --

[redacted] - Highly Confidential

A. -- if -- if the protocol -- if the protocol prevents double-spending, there are certain conditions under which it does so.

Q. Are you aware of a mechanism by which a malicious actor can accomplish a double-spend on the XRP Ledger?

A. I'm aware of certain mechanisms in which this can happen, yes.

Q. What are those?

A. So, for example, if you look at my report, page 21, this is fifth paragraph in Section 4.1.2.

For two validators to agree on the same global order of transactions, their UNLs must intersect or overlap. Chase/MacBrough may provide, in Section 4 of their paper, analysis of the required UNL intersection across different validators in order to guarantee safety and liveness.

I read this, and I understood this analysis, and I looked at the code to see their changes with respect to this that would affect the validity of the statement, because the paper was in 2018, and then I looked at the key, for

example, quorum properties, et cetera. They were unchanged from Chase/MacBrough.

And I support their conclusions. And their conclusions say that the analysis in that paper shows that to ensure safety of the XRP Ledger consensus protocols, this requires the intersection between any two UNLs to be over 60 percent.

Q. Okay.

A. Page 15 of that paper.

Q. Did you --

A. So there is a link to double-spending, via safety.

Q. So what -- so -- did you say that you reviewed what changes had been made to the XRP Ledger protocol after the Chase/MacBrough paper?

A. I did review. I was focusing on the changes to the consensus protocol and trying to see whether they would impact the analysis of Chase and MacBrough.

I didn't -- I didn't find -- I found, for example, that after the paper, the paper assumes that -- for example, for liveness, it

[redacted] - Highly Confidential

assumes 80 percent quorums.

And there was a -- after the paper was published in 2018, there was a change to the XRP Ledger consensus protocol because, to my recollection, the assumed size of the core was 67 percent of two-third majority in the code, and it was supposed to be 80.

So there was -- there were codes changes that were going towards fulfilling the assumptions of operations that Chase and MacBrough had in their paper; this -- this occurred, but there were none that would affect the analysis.

I'm pointing out, we discussed negative UNL briefly. Negative UNL would affect their analysis. It would not necessarily undermine my conclusions, but it would affect Chase and MacBrough analysis, but this change was not effective at the time I was writing the report and at the time -- for the release that I looked at.

Q. Okay.

MS. ZORNBERG: I'd like to take a break. I need a break, actually. So can

[redacted] - Highly Confidential

we go off the record.

THE VIDEOGRAPHER: The time is 3:53 p.m. We're going off the record.

(Recess from 3:53 to 4:13.)

THE VIDEOGRAPHER: It is 4:13 p.m. We are back on the record.

Q. Okay. Dr. [redacted] can I direct you, please, to page 16 of your report.

And this is part of your discussion of governance for bitcoin.

I want to direct you to the first two lines under "Governance," where you wrote, Concerning code improvement proposals, anyone can propose a change to the bitcoin open source software via a bitcoin improvement proposals. In practice, relatively few core developers, developers of the bitcoin core reference node software, propose and implement changes.

Do you see that?

A. I see that.

Q. In your view, is the fact of -- that there are relatively few core developers on the bitcoin system -- hold on, I have to rephrase.

Does the fact that rel-- that there

are relatively few core developers on the bitcoin system mean that the bitcoin network is centralized?

A. This is not what I mean, no. I wouldn't support that claim.

Q. So in your view, bitcoin is decentralized, notwithstanding the fact that it has relatively few core developers?

MR. SYLVESTER: Objection.

Q. You can answer.

A. I'm writing, In practice, relatively few core developers propose and implement changes.

I stand by the opinion expressed in my report that bitcoin is decentralized, so we can say that this doesn't make -- the relatively few core developers proposing and implementing changes to bitcoin is not preventing me to -- under my methodology, to say that bitcoin is decentralized.

Q. Okay.

Do you believe that bitcoin is the only digital asset that will be needed in the future?

[redacted] - Highly Confidential

MR. SYLVESTER: Objection. Beyond the scope.

A. I don't necessarily have that belief.

Q. Do you believe that other digital assets are inferior to bitcoin?

MR. SYLVESTER: Objection. Beyond the scope.

A. Can we define "inferior"?

So I can answer the question.

Q. Have you publicly expressed the view that bitcoin is superior to other digital currencies?

A. I don't believe that I expressed my view that it's superior to other digital currencies.

If I did, please point me to the place where I have -- did that. I don't believe I did.

Q. Do you believe that bitcoin will become the dominant form of money on earth?

MR. SYLVESTER: Objection. Beyond the scope.

A. I believe that there would be good things that would happen if this is so.

[redacted] - Highly Confidential

One cannot necessarily predict the future.

Q. So would you want bitcoin to become the dominant form of money on earth?

MR. SYLVESTER: Objection.

A. I think it would be -- it has good connotations, so I think it would be better for -- I -- I think it would be good for all of us, as a humankind, to have common money that is sound and that cannot be necessarily -- that would have better properties than the money that we have today.

To my understanding, bitcoin fulfills this, and it's a very good candidate, if it becomes dominant money, that it brings good to all of us, regardless of the current understanding of each and every one of us about bitcoin.

Q. You -- you argued in your position paper, in [redacted], that bitcoin's power consumption is not wasteful or excessive. Correct?

A. I argued in the paper that you submitted that -- as Exhibit --

[redacted] - Highly Confidential

Q. Exhibit 5.

A. -- [redacted] 5?

Q. Yes.

A. [redacted] 5. I argued for that, yes.

Q. Are you concerned about the -- the impact that bitcoin's energy consumption has on the environment?

MR. SYLVESTER: Objection. Beyond the scope.

A. Let me put it this way, so when I think about it, as I mentioned in my paper, the data I was able to obtain suggested that bitcoin has zero -- consumes 0.1 percent of the total world's energy production.

At that stage, to blame, currently, bitcoin for climate change and other things is a far-fetched thing. Like what happens to other 99.9 energy? So to blame it at this moment is not -- is, to my understanding, not justified.

Q. Do you -- do you think that energy consumption contributes to climate change?

MR. SYLVESTER: Objection. Beyond the scope.

A. I don't have understanding to that. I

[redacted] - Highly Confidential

don't have deep understanding to that, yeah.

Q. Let me direct your attention to page [redacted] of [redacted] Exhibit 5.

And I'll -- I'm just going to read into the record the paragraph in the middle of that page, where you wrote, quote, [redacted]

Did you write that paragraph?

[redacted] - Highly Confidential

A. I wrote this paragraph.

Q. Okay. And as you sit here today, does that express a view that you hold?

A. I am here so the paragraph that you read is the closing paragraph of [redacted]

And it -- for the record, because we are taking this out of the context, is the -- argument tries to -- so I'm trying to argue that if you have an inflationary money, that people are not incentivized to save, they're incentivized to spend. This is the part that we skipped.

As people are incentivized to spend, and they either spend money, they consume things, they consume products, et cetera, or they invest money into businesses and different sort of things, as we know, so I'm just summarizing other parts of --

Q. I don't -- I want you to complete your answer --

A. Yes.

Q. -- but I don't need you to do extensive summaries. My -- my question was just

[redacted] - Highly Confidential

whether that paragraph expresses your view as you sit here today.

A. I --

MR. SYLVESTER: Objection.

A. Yes, so I think it's important to say the view on what, essentially? The view on?

Q. Have you retracted anything in the paragraph that I read on page [redacted] since publishing it?

A. Rereading it, I don't find anything that I would retract.

Q. Okay. Can I -- can I ask you to turn to page [redacted] of Exhibit 5.

And in the -- you state that in this position paper, quote, [redacted]

Do you see that?

A. I see that.

Q. Okay. And "we" means you.

A. I, yes.

Q. Okay.

On page [redacted] of the article -- of your position paper, you -- you write, and this is

part of the last sentence on the top half, that, [redacted]

Is -- is that [redacted] project one that you're working on currently?

A. I'm referring to the [redacted] project that I'm contributing to in some sense --

Q. Okay.

A. -- today, yeah.

Q. Do you -- do you receive compensation for contributing to that project? For [redacted]

A. I do. Yes.

Q. Okay. On page [redacted] of your position paper, in the middle of the page, you -- you talk about tokens that have a genuine use case. Is the only example that you cite there, bitcoin?

A. I'm doing e.g., so this is example.

Q. Okay.

A. There might be others, so the example that I'm giving is bitcoin.

[redacted] - Highly Confidential

Q. And that's the only example you specifically give there?

A. That's the only example I specifically gave in that sentence.

Q. Okay. Let me ask you to turn to page [redacted] of Exhibit 5. About three-quarters of the way down, I want to read a sentence that you wrote, quote, Author's -- wait, I want to -- okay, I'll read the quote now that you're there.

[redacted]

Can you describe what you mean by [redacted]?

MR. SYLVESTER: Objection.

Go ahead.

A. Yes. So I mean, something that -- I was looking into bitcoin for 11 years. I understood it well, to my understanding, as a computer science system.

And I understood that it gives people control over money and everything, but this is not necessarily changing the whole behavior of

us as -- as human beings, as a species, to which I'm referring in the -- in the paragraph that -- that you -- that you read previously.

So that -- to go to that understanding, you're -- you need -- one needs to -- in my opinion, one needs to step out from looking at bitcoin as a computer science system, as a transaction processing system.

So one would actually need to, in my opinion again, look at bitcoin like implications, what is it use case. In this paper I'm discussing what is the use case.

I'm saying if it's a payment system, well, spending 0.1 percent of world energy on a payment system hardly is justified, but let's try to understand what it does.

And as we are trying to understand what it's doing, let's imagine -- so, okay, this idea, it seems that its goal is to become the money that we all use on this planet. So now you are saying, But it spends that much energy.

So, now you need to understand, Okay, but what do I get? If this is the money of the future, what would I get in such a world.

[redacted] - Highly Confidential

And now you're starting to think, and I realize, I explained to myself, that essentially incentives of humankind change, and it will make -- it will bring us, and this is what I'm arguing in the paper, to save resources.

To save. It just orients, instead of spending, and as I say, I -- I don't think it's -- I just think it's a technological evolution. It's not -- even if one had an idea such as to implement such a monetary policy, this was practically impossible. The technology was missing.

So, you know, in the history money, there are like -- everybody -- always somebody would come and be able to inflate the money regardless of how we did it.

And now we have a tool which we could use to actually promote savings and not overconsumption of resources. I'm trying --

Q. And that's bitcoin?

A. I'm trying to convey this message, and bitcoin, with its security and with the predictable monetary policy, which basically

[redacted] - Highly Confidential

incentivizes savings, it's going in the direction.

Q. Okay.

A. So once I realized that -- you asked me about [redacted] Once I realized that, I realized, Okay, this is -- as a computer science system, this is -- this is a nice protocol. I mean, it's interesting. It's consensus. It's interesting because I was looking into that from my professional standpoint.

But, you know, in -- in terms of my talks, I would say, bitcoin spends lot of energy. And usually when you do that, it's because of the number of transactions per second it processes, relatively high latency, and you consider it is a transaction processing system, as a payment system.

But once you understand that this is not necessarily the use cases -- actually, use case could be something else -- then you go back and say, Okay, do -- is it reasonable to devote energy of humankind towards that?

Q. Okay.

Did your enlightenment about bitcoin

[redacted] - Highly Confidential

come around the same time as [redacted]

[redacted]

MR. SYLVESTER: Objection.

A. Is that really relevant? So, I -- I spent before -- let's put it this way. [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Q. Okay. Now, in your -- both in your report and in your position paper, you talk about the fact that if Ethereum moves from proof of work to proof of stake, that will affect its level of decentralization. Correct?

A. This is correct. It might affect the level of decentralization.

So, I can elaborate on that if you wish.

Q. Well, my question is, in your view, is there any way for a proof-of-stake system to be decentralized?

A. There is a way. We discussed one

idea. There is a way, so if we take a snapshot of time, we apply Troncoso definition. We cannot find a single authority that controls the system.

And it is possible that this is the case. There just -- I would say, in our spectrum of the systems which pass from causal definition, and if you apply inclusiveness or if you value more permissionless system than permissioned or -- or inclusive as opposed to noninclusive, then it would put proof of stake on a -- less decentralized than bitcoin.

Plus there is this danger, which I don't elaborate in the report -- is that whenever you have the -- I think one example is, for example, you know, in any -- in any industry, how bigger players, over the time, do mergers and acquisitions of smaller players, et cetera. Right?

So there is this danger that the power in the system concentrates. For example, if I'm controlling 30 percent of the stake, depending on how the stake game is set, how the incentives are set, I might get more and more and more

tokens, and if you're not careful when you design this system, you know, as the power of such a stake grows, you could go over 50 percent.

So, you know, it's -- it's more -- in my opinion, there is more tendency for a system based on proof of stake, more challenges to keep it decentralized than it's -- it is for proof of work.

Q. Okay.

Let me direct you to page 25 of your report. I'm moving to another topic.

And -- and this is a page of your report where you are responding to Question E2.

Do you see that?

A. I see.

Q. And we -- we talked about Question E2 this morning. And you noted that you might have to rethink this section of your opinion, based on recent changes to Ripple D. Correct?

A. In the context of --

MR. SYLVESTER: Objection.

Go ahead.

A. Yes. In the context of my report, if

it's fixed in time and it looks at one point, 7.3, the answer would be no.

If someone -- if the Court, SEC, whoever, asks me to opine and I accept to do that on one -- if you -- so if one would allow it 1.8.1, we would need to revise this section. Yes.

Q. Okay. So I want to direct your attention to Number 1 in your -- in -- in your answer to Question E2, where you talk about things Ripple does or has done. And you -- you quote a Ripple employee named Nick Bougalis.

Do you see that in the second paragraph?

A. I see.

Q. Do you know Nick Bougalis?

A. I don't know him.

Q. Okay. And you -- you state that in an XRP chat online, in October 2020, from a user who appears to be Ripple's employee Nick Bougalis, following a November 2018 incident, he, quote, personally restarted several validators, close quote.

Do you see that?

[redacted] - Highly Confidential

A. I see that.

Q. Okay. I want to show you Exhibit [redacted] 16.

(XRP chat was marked [redacted] Exhibit 16 for identification, as of this date.)

Q. You're welcome to take a look, of course, through the whole document. I will point out that, you know, this is -- this is the XRP chat you appear to quote, and the section you appear to quote is on the third page of the document. And that's the only page I'm going to ask you about.

A. Yes.

Q. Do you agree that Exhibit 16 is the XRP chat you were referring to on page 25 of your report?

A. I believe I can agree with that.

Q. Okay. Can you look about midway down Exhibit -- page 3 of Exhibit 16, and starting with the place in the chat where Mr. Bougalis wrote, I personally restarted, and compare it to the quote that you excerpted in your report, and tell me if you think that you've accurately quoted the chat.

[redacted] - Highly Confidential

MR. SYLVESTER: Objection.

(Witness reviewing document.)

A. So under "Quotations" in my report, I attributed that Nick Bougalis, following the November 2018 incident, he personally restarted several validators.

If I look at the document, it says I personally started several of Ripple's validators.

Q. That's a difference. Right?

A. There is a --

MR. SYLVESTER: Objection.

Go ahead.

A. There is a difference in a sense that I skipped that he restart, so in the quotation marks, I skipped that he restarted Ripple's validators.

Q. Okay. And -- and do you agree that the actual sentence in the XRP chat in Exhibit 16 reads, quote, I personally started several of Ripple's validators, and other validator operators restarted theirs, period, close quote?

MR. SYLVESTER: Objection.

[redacted] - Highly Confidential

A. I believe I -- you said I personally started where it's written I personally restarted, several of Ripple's validators.

Q. Okay. Dr. [redacted] have I -- do you agree that I've correctly read from M 16 that the statement in the chat was, quote, I personally restarted several of Ripple's validators, comma, and other validator operators restarted theirs, period, close quote?

Did I read that correctly?

A. You read that correctly. I just corrected you because I heard that you said I personally started.

Q. Okay.

A. Yeah.

Q. In your report you -- you left out, Of Ripple's validators. You -- you wrote, quote, He personally started several validators, close quote.

So you left out two things. Right? You left out that he actually stated that he had restarted several of Ripple's validators, and you also omitted the part of the sentence stating that other validators restarted theirs.

[redacted] - Highly Confidential

MR. SYLVESTER: Objection.

Q. Correct?

MR. SYLVESTER: Objection.

A. I did not -- I did not omit. I was taking the part of the sentence on the quotation marks since what we could agree is that I didn't put -- attribute that validators are Ripple's validators.

Q. Okay. So do you agree that your report inaccurately quotes Mr. Bougalis in -- in that XRP chat?

MR. SYLVESTER: Objection.

A. I would say that it's -- apparently doesn't quote it word for word. If you restarted several validators, you -- if you restarted several Ripple's validators, you restarted several validators, so it's not incorrect.

As for use of quotation marks, if they are meant to mean exactly what was written, there is missing "of Ripple's validators." So there should be "several of Ripple's validators."

I -- I can explain the -- the context

if you wish.

Q. No.

A. No? Okay. No.

Q. Given the accurate quote from Mr. Bougalis, what is your basis for saying that in particular, Ripple's -- Ripple employees' effort was needed?

A. So, we didn't focus on the second -- so you basically added -- I was asked, so let's -- let's roll back to the question, E2; to what extent have Ripple's efforts been needed to support the proper function of XRP Ledger.

I'm trying to answer that question. This doesn't mean that there are no other's efforts involved in this. I'm trying to answer whether the Ripple's efforts be needed to support the proper functioning of XRP Ledger.

When I'm jumping to -- when -- when you're jumping, illustrating, in particular, Ripple's employees, we should also focus on the second sentence, which I believe is quoted, Without differences.

So the team at Ripple invested a significant amount of time troubleshooting the

[redacted] - Highly Confidential

issue and proposed several improvements.

This looks word for word.

Now, illustrating the amount of human and, in particular, Ripple, so the quotations that I'm giving are, in particular, illustrating the amount of effort of Ripple's employees.

Q. Dr. [redacted] I'm not questioning the second quotation, just so you know.

It's only the first quotation where I -- I wanted to point out, and you've acknowledged, that there are missing words from within the quotation marks.

A. Yes, I believe, if I'm not mistaken, that you asked me about the conclusion that, in particular, Ripple's employees' efforts are needed, so this is why I'm pointing out the second.

For the first one, I think we are in agreement.

Q. Okay. Let's turn to Question E3 in your report where you were asked, on the bottom of page 25, quote, What risks to the XRP Ledger would or might materialize if Ripple walked away or disappeared? Do you see that?

[redacted] - Highly Confidential

A. I see that.

Q. Was that a hypothetical question given to you?

A. That was a question giving -- given to me for an opinion as -- as it was phrased here, so I didn't come up with a question. I was given that question to answer it.

Q. Okay.

And you answer it at the bottom of page 25 by saying that, Serious risks may arise. Correct?

A. They may arise. We don't -- yes. This is what I said.

Q. So "may" means maybe they would, maybe they wouldn't?

MR. SYLVESTER: Objection.

A. May arise, it's -- there is a possibility that they may arise.

Q. Is it fair to say you're not providing an opinion in response to Question E3 about what will happen to the XRP Ledger if Ripple disappeared?

A. I'm not providing answer to that question, because it was not a question.

Q. Okay. In answering the question in E3, does your report cite to any scientific literature?

A. No, it does not. I'm answering my question to the best of my understanding of the protocol.

Q. Okay. So, it looks like you -- you -- in answering the question, you posited two possible cases, Case A and Case B.

Do you see that on page 26?

A. I see.

Q. So in Case A, you considered what might happen if Ripple disappears and the network is still able to agree on the contents of the dUNL as currently published on VL.Ripple.com. Correct?

A. This is correct.

Q. And -- and you conclude that in the case where more than 20 percent of the validators in the dUNL disappear, the network would not be operational. Right?

A. I agree.

Q. Okay. And you -- given the -- you do a calculation that because there are -- you

calculate 41 total entities on the dUNL, as of October 4, 2021, you say that, hence, the network would cease to be operational if nine validators disappeared, right?

A. 20 percent of 4.1 being 8.2, rounded up, so this means that the network would continue to provide liveness, and be operational in that sense, with 8 disappearing validators, it would take 9 to halt the network.

Q. Does your conclusion assume that the XRP Ledger network consists solely of validators using the unmodified dUNL?

MR. SYLVESTER: Objection.

Go ahead.

A. So, we considered two cases as I write on page 26. Ripple disappears, and the assumption for the analysis is that the network is still able to agree on the contents of the dUNL as nan currently published on https://VL.Ripple.com.

So that happens, we are dealing with the network in this imaginary example, right, what might materialize? I'm assuming that the dUNL is the same.

[redacted] - Highly Confidential

Q. So my question was, does your scenario or Case A also assume that the XRP Ledger network consists solely of validators using the unmodified dUNL?

MR. SYLVESTER: Objection.

A. As I mentioned, it assumes that the network is able to agree on the contents of the dUNL as currently published there, so what I'm discussing is the case -- what I'm considering is the case where the dUNL is the same as currently published on VL.Ripple.com.

Q. Do you know, as of October 4, 2021, how many validators on the system use the unmodified dUNL?

A. I don't know.

Q. You don't know by percentage or by total?

A. I don't know.

Q. Did you do any work in this case to try to determine how many validators use the unmodified dUNL?

A. That would probably necessitate that there is a disclosure of that by natural cooperators, the answer would probably be no.

[redacted] - Highly Confidential

Q. So you're not even sure it's knowable?

A. It's know--

MR. SYLVESTER: Objection.

A. It's knowable -- it's knowable in a sense that -- from the God's perspective it's knowable. If we interview all the node -- all the node operators and they're honest, they tell us the truth, it's knowable.

Q. Okay. You didn't do that?

A. I didn't do that.

Q. Okay. How many validators were active in the XRP Ledger system as of October 4, 2012?

A. How many validators have been active in the XRP Ledger? So, I don't know an exact number. I suspect that the number of validators on the XRP Ledger is between 100 and 200 validators.

That's a rough ballpark.

And on that day, there were 41 validators in the dUNL published at VL.Ripple.com.

Q. Do you know how many dUNLs -- I'm sorry, rephrase.

As of October 4, 2021, do you know how

many UNLs existed, besides the one that Ripple published?

A. I don't know how many UNLs existed beside the one that Ripple published.

Q. How can a validator on the ledger change their UNL?

A. The validator on the ledger can change the D -- UNL by changing its local state.

Q. Have you ever done it yourself?

A. I have not done it myself, no.

Q. Do you know how easy it is to do?

MR. SYLVESTER: Objection.

A. I don't know how easy or difficult it is to do.

Q. Do you know if it can be done in the space of a couple minutes?

A. I don't think it's relevant. I would accept that it can be done quickly.

It poses certain challenges to the system. If you're doing your -- if you're just specifying your UNL, I think it's important, so I'm agreeing with you that it's easy to change.

What should go on record, in my opinion, is that this affects safety and live--

this may affect safety and liveness. So if --

Q. Okay.

A. -- if we as a network, we just specify UNLs on our own and we don't get into sufficient agreement, this sufficient overlap that I'm describing in other parts of my report, it may happen that we just don't play the same game, so we'll get different views of the system and we don't get to consensus.

Basically, you and me as honest nodes, as honest validator operator nodes, as an example, we are -- just don't have enough UNL because we are not getting the same source of it or we are not talking to each other to agree on it.

There is the chance that if we do it independently, as you're just describing it, that we don't get -- that we can get consensus priorities violated.

Q. Okay.

On page 26 of your report, in answering E3, you wrote that, quote, If Ripple disappears, there's a risk that universities might cease to operate validators in the absence

of further funding.

And you're referring to universities that participate in the University Blockchain Research Institute?

A. University Blockchain Research Initiative, yes. I do.

Q. Okay. Also for short, sometimes called UBRI?

A. U-B-R-I, I call it, maybe UBRI, fair enough.

Q. Are you making any assumptions in that statement?

A. I'm making assumptions that, from my experience as a university professor, is that universities usually seek external funding, and there are certain expenses, for manpower, for computing power to ran validator nodes.

And to my understanding, the funding of universities came -- of University Blockchain Research Initiative came through Ripple.

And then, if Ripple disappears, I'm saying there is a risk. I'm not quantifying the risk. I am not sure even I am an expert to quantify -- to quantify that risk. But I think

it's fair and assemble that there is a risk --

Q. Okay.

A. -- that the universities stop operating their nodes.

Q. In citing that risk, did you assume that the nine universities were receiving funding from Ripple as of October 4, 2021?

MR. SYLVESTER: Objection.

A. I said Ripple has funded these universities.

You know, what does it mean receiving funding? Does -- is there -- was there a payment on October 4, 2021? I didn't say that.

Q. Okay. Do you know if that's true or not?

A. I don't know if that's true or not.

Q. Okay. Did you assume, in this part of your report, that the nine universities have an expectation of continued funding from UBRI beyond October 4, 2021?

A. The implicit assumption here is that it costs something to run the node. There are no incentives from the protocol itself that would fund this. For example, there are no

mining rewards or something similar.

So, it's -- cost certain money to have the manpower or -- and the equipment to operate this node. And, you know, if I am going to say that there is no risk that these universities eventually -- again, the word "eventually" where we don't specify when this happens -- that they stop because the funding stops. There is a risk that this happens.

Q. Do you know how much it costs to run a validator on the XRP Ledger?

A. I have some idea. So I think I saw different numbers, like few -- there are numbers of the cost of the -- of the node, which is in thousands -- to my understanding, in thousands of euros.

And if you run the fully -- full -- the validator with a full history, then the storage can go to over 15 terabytes, so maybe 20 terabytes, roughly speaking, and this blows -- this blows up the cost for running the validator node.

Q. As part of your work on this case, what communications have you had with anyone

[redacted] - Highly Confidential

from those nine UBRI universities?

A. I didn't have communications with anyone from these nine UBRI universities.

Q. Okay. Do you have a factual basis to state that those universities would cease running a node if Ripple disappeared?

MR. SYLVESTER: Objection.

A. This is not what I stated. I stated that there is a risk, and I tried to justify why this risk exists.

Because universities usually rely on external funding, there are no incentives in the Ripple protocol to make -- to incentivize nodes to -- to run the nodes, and this is the risk that may happen. I'm not saying that it will happen.

Q. I understand.

Other than in-protocol incentives, did you do any work to consider what out-of-protocol incentives UBRI universities might have to run a validator node?

A. Out-of-protocol incentives for you -- UBRI, right, to run a validator node, could be the funding that they got from Ripple and other

companies. This could be one incentive.

Q. Could it be anything else?

A. It could. It's -- you could have an incentive to do research, to publish papers on that. I didn't see -- I'm not saying these don't exist. I never saw one.

Q. Okay.

A. I'm not saying these don't exist.

Q. In answering Question E3, you also refer to four companies on the dUNL, Bitso, COIL, Towo Labs and XRP Labs. And you state that there's a risk that they could stop running a validator, too. Correct?

A. Yes.

Q. Again, you're not saying it will happen, you're saying that it's just -- it may be a risk.

A. It may be risk. I think it relates to Jeff, Alice and Bob example that you gave before. So if -- if there is a -- there is a risk that -- because of the connection -- business connections, that there is a -- there is a risk that -- that if those companies depend on funding by Ripple and it stops, it might be

going in the similar direction as we discussed for university.

So I would say there is a risk. I'm not saying it will happen, I'm saying it might happen.

Q. Is it possible that those four companies have independent business reasons to support the XRP Ledger?

A. There is a possibility. Again, there are no in-protocol incentives. It would be considerably more transparent to reason about independent economic and rational -- independent economic players if you have in-protocol incentives, if -- if there is something intrinsic to the property -- to the protocol that motivates you to continue what you're doing.

Q. Did you speak with anyone at Bitso, COIL, Towo Labs or XRPL Labs about their incentives to run a validator?

A. I did not.

Q. Do you have -- as part of your work on this case, did you investigate what products and services those companies offer?

[redacted] - Highly Confidential

MR. SYLVESTER: Objection.

A. This was not a part of the questions that I was asked to opine on.

Q. Were you curious to know if they offered products or services that used the XRP Ledger?

MR. SYLVESTER: Objection.

A. I was not curious to find out that. I was answering to the questions I was asked.

Q. Let me direct you to your Appendix B and B2. Briefly, in B2, you -- you present a scenario in which you say that the XRP Ledger could fail to guarantee liveness. Correct?

A. This is correct.

Q. Okay. And without going into detail or reading what you wrote in B2, but I'm referring here to your discussion in B2 and that scenario, are you aware of whether the XRP Ledger has any countermeasures to address such a situation as the scenario you lay out in B2?

MR. SYLVESTER: Objection.

Go ahead.

A. The scenario that I am laying out in B2 is the liveness analysis by Chase and

MacBrough. So this is the liveness analysis done by Ripple employees.

So I didn't invent this. I'm basically copying it from the paper that is -- if you look at the Ripple documentation and the Ripple original white paper, it says it's deprecated, in computer science terms, towards this paper. And an external reader could assume that this is an authoritative paper.

Q. Okay.

A. I did -- I did checks in the code to understand whether this understanding that Chase and MacBrough had when they published in 2018, still matches, despite the software changes in the last three years, at the moment I analyzed the protocol, whether this is the case.

To best of my understanding, this is still the case. So we can apply the analysis of Chase and MacBrough.

Q. Okay. I'd like to show you --

A. I would like to finish my answer.

Q. Please do.

A. Yes. Because you're asking me to say, like, this is my opinion. This is not my

opinion, this is the liveness analysis by Chase and MacBrough.

So, I agree with that analysis.

You asked me whether there are certain changes in the code, or actually, features in the code that prevent this from happening.

So there are some features that are doubled, detection of Byzantine validators in the code. And these changes actually don't do anything automatically.

So what they would do is, they would alert the operator of human nodes.

Q. They would avert the --

A. Avert, if something happens, to the best of my understanding, because they look at they changes, they don't automatically try to evict, potentially, Byzantine nodes from the -- from the system, from their UNL, for example, but they would avert -- they would alert the operator of the node. That's my best understanding of what happens.

And then what it means for the -- in the Chase/MacBrough analysis, it means that the analysis stands. It's just that some human

[redacted] - Highly Confidential

operators, of which action would be required later on, they would need to act on this information.

The software, you know, maybe if it detects, it raises a flag, but it doesn't do more than that.

Q. Based on your understanding of the Ledger's Byzantine validator detection measures, do those measures make it less likely that Scenario 2 -- that B2 in your report would actually occur?

MR. SYLVESTER: Objection.

A. I'm not sure I can opine on that.

We would need to measure whether it's less likely or not, whether they deter certain participants from doing this.

I don't think we can come to that conclusion.

There is no penalty to these nodes, so I would say we cannot -- I -- I couldn't take that standpoint, honestly.

MS. ZORNBERG: Okay. Let's go off the record, just for efficiency's sake. And we're still on time to get you out of here

[redacted] - Highly Confidential

by 6:00 o'clock. I want to take another ten-minute break.

THE VIDEOGRAPHER: It is 5:00 o'clock p.m. We're going off the record.

(Recess from 5:00 to 5:12.)

THE VIDEOGRAPHER: It is 5:12 p.m. We are back on the record.

Q. Okay. Earlier today, you mentioned having a close collaboration with an individual named [redacted]

A. [redacted]

Q. [redacted] Correct?

A. Correct.

Q. Okay. Did you discuss your report with him in this -- your report in this case with him?

A. No.

Q. Are you aware of an article that [redacted] co-authored in November 2020, titled "Security Analysis of Ripple Consensus"?

A. I am.

Q. Have you read that article?

A. I did.

[redacted] - Highly Confidential

Q. Did you -- did you and [redacted] ever discuss that article as he was writing it?

A. No.

Q. When did you read his article -- that article?

A. I read the article, I believe the first time he made it public. And I reread it during the -- when I accepted the case, I reread it to understand what -- in more details what he's writing about. So I read it at least twice.

Q. Okay. And one of the times you read it was in connection with your work on this case?

A. It is -- yeah, it was, yes.

Q. Okay. And the first time, do you -- do you also -- rephrase.

Do you recall that you also retweeted [redacted] tweet of his -- of his article in 2020?

A. In November 2020?

Q. Actually, the tweet -- or retweet was in December 2020.

A. I don't recall. I could trust you that I did that.

[redacted] - Highly Confidential

Q. Okay. Let me show you [redacted] 17.

(2020 [redacted] article was marked [redacted] Exhibit 17 for identification, as of this date.)

Q. Okay. Dr. [redacted] is this the [redacted] article from 2020 that you've just discussed having read and then reread in connection with your work on this case?

A. [redacted] yes, it is. It appears to be, yes.

Q. Okay. Did you cite this among the references of your report in this case?

A. I did not.

Q. Why not?

A. This paper shows an attack, which is pointed out by [redacted] And then there was a discussion -- in a sense, there was a -- an unofficial rebuttal by -- I believe it was Brad Chase, I'm not sure. Definitely, somebody closely connected to the -- to Ripple and to XRP Ledger consensus protocol.

But they basically questioned the attack. The attack is rather similar, if you look at the -- if you look at the -- Figure 5 on

[redacted] - Highly Confidential

page 15.

The attack is somewhat similar to the attack that I'm describing in Appendix B3, but it actually applies to the different phase in the protocol.

So I thought that Ripple's rebuttal in this case that was offered in the discussion -- I think I'm referring to Twitter discussion and some -- some -- basically comments of Ripple's employees that could be fine with respect to this report, I think they were grounded.

I don't think that the attack works. My best understanding of Ripple system is that this attack doesn't work as it's specified here.

So that that needs -- so it's just that it doesn't work as it's described here. So in that sense, I read it, and I didn't find it -- because of this incorrection that I perceived from my understanding of the protocol, I didn't find it relevant to include it. Because I don't think necessarily what's written here is true.

Q. Okay.

Can I direct you to page 36 of your

report?

A. Yes.

Q. And -- and you mentioned page 15, Figure 5 on page 15 of [redacted] 17?

A. Page 15, yes.

Q. Okay. So can you just -- you have a Figure 5 also in your report. Are there similarities between Figure 5 in your report and Figure 5 in [redacted] report?

A. I report there are similarities, yes. Here, it's similar in the sense that the setup looks like, but the message is centered different.

So Christian, basically mounts this type of an attack at the different stage of the protocol than what I did. So if you ask me, you know, with this -- what is inspirational for my attack maybe, was this -- I definitely read it before I came up with the attack, but it's different.

So it applies to -- there are similarities, as I pointed out immediately, but this applies to the different phase of the protocol.

So my attack applies at a very different phase of the protocol than Christian's attack.

Q. Okay. Let me turn your attention now to page 5 of your report, under "Governance."

So, in your report, you -- you note, that Ethereum's development was funded using proceeds of an ICO. Correct?

A. Correct.

Q. What was the ICO of Ethereum?

A. What?

MR. SYLVESTER: Objection.

A. What what?

Q. What was the ICO of Ethereum?

A. What was the ICO?

Let's see how I refer it to the -- in order not to diverge from -- from what I wrote, let's -- let's find when I mentioned the ICO and just make sure that we are talking about the same thing.

Q. So I'll -- I'll help you there. I can direct you to page 18 --

A. 18.

Q. -- of your report.

[redacted] - Highly Confidential

Where, at the very bottom of 18, top of 19, you reference 72 million ETH being preallocated in the Genesis block?

A. I definitely agree with you, I'm just trying to pinpoint the -- the line so --

Q. That line is at the very bottom of 18, top of 19.

A. Yes, okay, I'm with you.

Q. Okay. So turning now to your chart on page 5 of your report, under "Governance for Ethereum," you write that Ethereum was 61 -- 61.5 percent, about 10 percent owner controlled, of today's supply.

I just want you to explain, please, how did -- I want you to explain your math. How did you come up with 61.5 percent?

A. It says 61.5 percent. If you, for a moment, ignore what's in the brackets, we can come back to that. It says 61.5 percent of today's supply.

So today's supply can be estimated by different means. It's actually -- for Ethereum, it's difficult to pinpoint the exact supply, but there are estimations, including on many

[redacted] - Highly Confidential

comparison sites, such as CoinMarketCap and others, which would indicate roughly where the supply stands.

And that number, 72 million, would be 61 percent -- 61.5 percent, roughly speaking --

Q. Okay.

A. -- of supply on that day.

Q. So how did you calculate 10 percent owner controlled?

A. 10 percent owner controlled would be -- let's go back.

What I think is 10 percent owner control of today's supply. So you will take today's supply. 10 percent of that should be matching the 12 million Ether that I nominally --

Q. Are you -- are you expressing --

A. -- referred to.

Q. Is it your belief that the -- the launchers of Ethereum, the owners, initially controlled a hundred percent and then sold some of theirs -- percentage for money?

MR. SYLVESTER: Objection.

A. Could you restate, please?

[redacted] - Highly Confidential

Q. Do you have a view as to whether the owners, as you're using that term to talk about Ethereum blockchain, at any point owned a hundred percent?

MR. SYLVESTER: Objection.

A. There is a moment on the Genesis block. And the token 72 million Ether at the moment of the Genesis block were 100 percent of the supply at that time.

We can say that the game starts by -- at that moment where the allocation happened, you could say that the development team essentially may decide whatever it wants to decide, right?

But it respects the informal contractor, like from the ICO, that essentially the bitcoin that were sent to their address, in the procedure of the ICO, should be exchanged for 72 million Ether. So that moment, there is a genesis bulk -- bulk creation with the initial distribution of coins.

Q. Why -- why, if your assignment in the case was to compare the decentralization of bitcoin, Ethereum and XRP Ledger, as of

October 4, 2021, why are you even talking about owner control over -- you know, years ago, in your chart on page 5?

A. So --

MR. SYLVESTER: Objection.

Go ahead.

A. Yes.

So owner control, in my review of the literature, in one of the paper that we discussed, which is the Sai paper, and Exhibit [redacted] 4, where we discussed different layers, and -- so I would refer you to page 12, and Table 2 of the Sai paper, in the governance layer, you asked me also about the centralization factors Sai mentions in -- in that paper.

So, I'm before, page 12. Table 2 at the top of the page.

Q. Yeah, but in the methodology in your report --

A. I didn't -- may I finish?

Q. Oh. Go ahead.

A. So, Sai has the owner control as a centralization factor, and it's -- you know,

again, we are establishing here -- I was trying to establish the methodology that would be applicable, hopefully, beyond the three.

This is the way I approach things, right? So if you call it the methodology should be applicable to blockchains other than these three.

Maybe if you switch to proof of stake in any of the three, you know, you should be still able to understand the dynamics and to infer something about -- about the system, right? So for that is --

Q. So was your --

A. Yeah, for that is -- owner control is important because Sai mentions, he says once and like layer, I call this facet. And because it was part of the established methodology that we discussed in details before, I'm evaluating this owner control, and actually this owner control, I took that from Sai.

Q. So, for purposes of owner control, are you saying your methodology was not restricted to looking at ledgers as of the date of your report?

[redacted] - Highly Confidential

A. Owner control defines -- is defined in Sai, and I think I repeat that -- let -- let's -- let's -- not because I know my report better.

There is a point in which I cite Sai in the methodology, and that should be --

Q. I'd like to restate my question --

A. Okay.

Q. -- rather than going into Sai.

My question is about the chart that you wrote on page 5, and about your assignment in this case.

Were you -- was your -- did your methodology intend to compare bitcoin, Ethereum and XRP Ledger as of the date of your report?

A. Yes. But this -- so, yes, but there is this -- so if you look at page 11 of my report, so in governance, which is introduced at the very bottom of page 10, so there is this governance aspect or -- or layer in Sai's terminology.

Point C, owner control is defined as measured by examining the total tokens accumulated by the stakeholders in the early

adoption period. So since we discussed the Sai, so you see that there is a time reference to the early adoption period.

And since Sai as one of the peer-reviewed papers which we discussed before, which introduces the taxonomy of public blockchain systems of this -- their centralization, basically he defines it at that point in time. I'm including that in my methodology.

I also -- so -- so one other justification is there -- there like -- informally people would -- you know, if there is a fair distribution of tokens, if you have a blockchain which didn't -- one who create the blockchain didn't reserve the tokens for himself, that's, in some sense, more equal or in a sense -- so I see why Sai is doing that, why he points out that you should not, as they call it pre-mine the blockchain.

And -- and taking that as a centralization measure, I see why this -- so I agree with accepting that. But I'm not the only one who proposes that, so at least Sai does.

[redacted] - Highly Confidential

And he refers -- so they refer to the point -- so they really refer to the early adoption period. If you just look through the paper, they -- this is what owner control means.

Q. So, is it your view that even if Ripple control -- let me rephrase.

Even if Ripple owned zero XRP today, in deciding whether the XRP Ledger was centralized or decentralized, you would still look back to 2012 or 2013 to evaluate owner control?

MR. SYLVESTER: Objection.

Go ahead.

A. Again, owner control as it was defined, I'm accepting this as defined by other scientific researchers. If we accept that this is relevant, we would need to take it into account.

It's also --

Q. Can you answer my question, though? My question was --

A. Yes.

Q. -- if Ripple owned zero XRP today in 2021, would it be your view that to determine

the decentralization of the XRP Ledger, you would still, under your methodology, need to consider how much XRP Ripple owned back in 2013?

MR. SYLVESTER: Objection.

Go ahead.

A. Yes. I think what are you asking me requires deeper understanding, but it's relevant.

So I -- I don't know if you recall that I described the attack on proof-of-stake system where the old stakeholders can mount. I didn't mention that it's called long-range attack, but can go back in history to the point where they control a lot of tokens.

So that's important, because if you don't consider that in a proof-of-stake system, which may be not relevant for three blockchain systems we analyze here, but since this methodology should be applicable to other blockchains as well, this -- you would still want to look at that, because the attacker could go back in time to the point where it controlled enough tokens to mount the attack and present you with alternative history if the system

doesn't prevent this kind of attack.

Q. In the proof-of-stake system.

A. For example. We need to understand if these are the only ones. So that's the part of the methodology. As it's part of the methodology, I'm putting all the -- all the analyzed blockchains through that filter.

Q. Okay. Let me turn -- turn to a question about bitcoin miners. Is there a point when bitcoin miners will no longer be able to receive mining awards?

A. So depends on how you define the mining rewards. There are two rewards for mining. One is the block reward, which halves every 210,000 blocks, as I explain in my report.

There is another reward, which are transaction fees. So whenever you submit a transaction, you need to put some transaction fee. And bitcoin miners will always be collect -- assuming, again, no protocol changes, simplify our life and to talk about the current state of bitcoin software, is just runs after 2140, year 2140, where the block reward disappears, but the mining reward is still there

because there are transaction fees.

If you see the distinction between the mining reward and the block reward.

Q. So the mining rewards will run out eventually for bitcoin?

A. No. They will -- mining -- miners are rewarded by transaction fees and block reward. They would run out from block reward, but they would keep the transaction fees, which is part of the mining reward.

Q. Okay. Is it -- I want to talk about in-protocol incentives, which you define in your report.

Is it your opinion that in-protocol incentives are necessary to whether a blockchain can be decentralized?

MR. SYLVESTER: Objection.

Go ahead.

A. Yes. So I think we made it clear that the -- under the methodology that I'm presenting here, we couldn't call them necessary.

But we would call a system that has in-protocol incentives, in this -- so if there are incentives to participants in the protocol

which are in -- in-protocol, we could claim, under my methodology and under the standing of researchers that I cited, that the system is more decentralized than another one which doesn't have this.

Q. So in your view, in-protocol incentives are not necessary to decentralization, but an in-protocol decentralized system -- let me -- let me rephrase.

So in your view, in-protocol incentives are not necessary to whether a blockchain is decentralized, but a blockchain system with in-protocol incentives may be more decentralized than others?

A. I think that fairly summarizes my standpoint, yes.

Q. Okay.

In your definition of equal opportunities, which is found on pages 15 through 16 of your report, do you assume that there's a free market for computing power?

A. I do assume that there is a free market for computing power.

[redacted] - Highly Confidential

Q. Does your application of equal opportunities to bitcoin and Ethereum also assume a free market for electricity?

A. It does.

Q. And does your application of equal opportunities to bitcoin and Ethereum assume a free market for Internet bandwidth?

A. We could say that it does, but that -- that aspect is considerably less of a challenge with respect to two. If there is no free market, for example, for computing power, and that would be less of a challenge because the -- especially for bitcoin, the bandwidth is not that big, but I -- I could agree, yes.

Q. Okay. So I think you just said it, but would you agree that there actually is not a free market throughout the globe for computing power?

MR. SYLVESTER: Objection.

A. I did not say that.

Q. Is it your opinion that there is a free market for computing power, in actuality?

A. I think --

MR. SYLVESTER: Objection. Beyond the

scope.

Go ahead.

A. Yes. So I didn't opine on this, and I'm just saying assuming free market, there are certainly properties.

Honestly, it's -- it's at which level you zoom out and look at the game that we are playing here. So, anyone can -- there is no constraint that any, for example, nation or any individual, that any organization could start their own chip-producing facilities. It takes a lot of knowledge.

It takes a lot of know-how, but normally you're not prevented from doing that. If you have that know-how, if you have the resources, if you can produce your own chips, you could do it.

You could do your own research independently of others to advance the computing power, and actually, we are doing that. I mean, as a society, we are doing that. And nobody can stop you, in that sense, from joining the game, as I am discussing here.

Whether there is an ideal free market,

[redacted] - Highly Confidential

I guess, if -- you know, that in practice, that's another thing that, you know, I don't necessarily have an opinion on currently. I'm assuming if there is, what are the rules of the game?

Q. Your market assumes a free market for computing power?

MR. SYLVESTER: Objection.

A. My --

Q. I misspoke. Your -- your definition and application of equal opportunities to bitcoin and Ethereum assumed a free market for computing power?

A. This is what I said. So, because you're trying maybe to -- to guide me to say something that I don't necessarily plan to say --

Q. You know what? I'll just point it out in your report where -- a statement, see if you still agree, and then -- and we'll stop it at that.

On the top of page 16, you -- do you acknowledge that for proof-of-work consensus, assuming a free market for computing power,

[redacted] - Highly Confidential

existing participants cannot prevent new participants from entering the system?

A. This is what I'm saying, if we assume a free market for computing power, then existing participants cannot prevent new participants from entering the system.

MS. ZORNBERG: Okay. I think we're at the 7-hour mark, so we're going to -- we're going to stop here.

I'd like to put on the record that on behalf of all three defendants in the case, that we're going to request that a -- a proper list that complies with the -- with the Federal Rules of Procedure with Rule 26 be provided, of the materials considered by Dr. [redacted] in preparing his report, and we're going to reserve our right to re-depose him once we get a proper exhibit that complies with the rules.

MR. SYLVESTER: Well, we'll review his testimony, and we reserve our rights as well.

I have a few questions before we wrap up for the day, which I'm happy to start

now.

EXAMINATION BY MR. SYLVESTER:

Q. Dr. [redacted] do you remember earlier today, counsel asked you, Are you offering any opinion in this case as to whether Ethereum is a decentralized system?

A. I remember we discussed it.

Q. And throughout the day today, you've testified as to methodology for the relative -- for assessing the relative decentralization of bitcoin, Ethereum and the XRP Ledger, as you were assigned to do in this case?

A. I did that. This is correct.

Q. Okay. And as part of your opinions set forth in your expert report, you did apply that methodology -- methodology to Ethereum. Correct?

A. This is correct.

(Continued on following page to include jurat.)

[redacted] - Highly Confidential

MR. SYLVESTER: Okay. That's all I have.

MS. ZORNBERG: Okay. We're off the record.

THE VIDEOGRAPHER: It is 5:37 p.m., we are going off the record.

(Time noted: 5:37 p.m.)

[redacted] Ph.D.

Subscribed and sworn to before me this day of 2021.

C E R T I F I C A T E

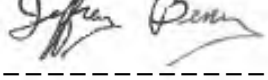
STATE OF NEW YORK)
) Ss.:
COUNTY OF NEW YORK)

I JEFFREY BENZ, a Certified Realtime Reporter, Registered Merit Reporter and Notary Public within and for the State of New York, do hereby certify:

That [redacted] Ph.D., the witness whose examination is hereinbefore set forth, was duly sworn by me and that this transcript of such examination is a true record of the testimony given by such witness.

I further certify that I am not related to any of the parties to this action by blood or marriage; and that I am in no way interested in the outcome of this matter.

IN WITNESS WHEREOF, I have hereunto set my hand this 20th of December, 2021.



JEFFREY BENZ, CRR, RMR

----------INDEX----------

----------EXHIBITS----------

NUMBER	DESCRIPTION	PG	LN
Exhibit 16	XRP chat	341	7
Exhibit 17	2020 [redacted] article	366	6

****

WITNESS DIRECTED NOT TO ANSWER:

Page 221

ERRATA SHEET

Case Name:

Deposition Date:

Deponent:

Pg.	No.	Now Reads	Should Read	Reason
___	___	_____	_____	_____
___	___	_____	_____	_____
___	___	_____	_____	_____
___	___	_____	_____	_____
___	___	_____	_____	_____
___	___	_____	_____	_____
___	___	_____	_____	_____
___	___	_____	_____	_____
___	___	_____	_____	_____
___	___	_____	_____	_____
___	___	_____	_____	_____

_____
Signature of Deponent

SUBSCRIBED AND SWORN BEFORE ME
THIS ____ DAY OF _____, 2021.

_____
(Notary Public) MY COMMISSION EXPIRES:_____

DEPOSITION ERRATA SHEET

Case Name: SEC V. RIPPLE LABS, INC. ET AL

CIVIL ACTION NO. 20-CV-10832 (AT) (SN)

Deposition Date: DECEMBER 17, 2021

Deponent: [redacted]

Page	Line	Now Reads	Should Read	Reason
11	23	Don't get me for the accusation	Don't cite me on the accusation.	Transcript error
13	11	with maybe one hour, initial	for maybe one hour, initially	Transcript error
14	6	case	cases	Transcript Error
14	13	correct	correctly	Transcript Error
15	7	I'm interested	I was interested	Transcript error
22	19	very much freedom	a lot of freedom	Transcript error
24	15	number of quorums	size of quorums	Clarification
25	4, 5, 8, 15, 22, 23	Blockchain Protocols in the Wild	Blockchain Consensus Protocols in the Wild	Clarification
34	11,15	permission	permissioned	Transcript Error
34	12	call	called	Transcript error
46	*Lines 20-24 are confusing.*	So Adriaens would take the definition, you know -- definition. Take the sentence. There is no definition. Even Troncoso admits that there is no definition, no -- that's the motivation of their work, and they actually propose the definition.	So Adriaens misuses a sentence from Troncoso to say that Troncoso admits there is no definition, to which I say no, that is not the correct interpretation of Troncoso -- that's the motivation of their work, and they actually propose the definition.	Clarification
48	13	by	and buy	Transcript Error
57	13	This is actually similar to accept the ledger.	This is actually similar to XRP Ledger	Transcript Error
58	16, 18, 24	Byzantine full tolerance	Byzantine fault tolerance	Transcript Error
59	14	is relate	is related	Transcript Error

60	24	forge	fork	Transcript Error
60?	25	in order for that work on your network	in order for that to work on your network	Transcript Error
64	18	Ripple D	rippled	Transcript Error
65	13	very	wary	Transcript Error
73	22	my opinion with rippled 1.7.3.	my opinion assumes rippled 1.7.3.	Transcript error
83	6	I am not sure Pat	I am not sure if Pat	Transcript Error
84	15-16	treat it as a fixed line	treat it as fixed	Transcript Error
85	15-16	of the paper	of the report	Transcript Error
91	15	2021	2001	Transcript Error
93	2	Go on	Go	Transcript Error
95	11	There is a degree in innovation and entrepreneurship	There is a degree in innovation and entrepreneurship?	Clarification
95	22	I did not	I do not	Transcript error
98	16	And what the program committee does then is, that it reviews the papers submitted by other researchers.	And what the program committee does then is, it reviews the papers submitted by other researchers.	Transcript Error
98	23	oversee	oversees	Transcript Error
98	24	It	He/she	Clarification
100	2	set	said	Transcript Error
100	7	poses	implements	Clarification
103	5,6	permission	permissioned	Transcript error
103	7	coin mentors	inventors	Clarification
103	13	some cases, it could be in decentralized	in some cases, it could be decentralized	Transcript Error
103	22	permissionness	permissiveness	Transcript Error
104	12-13	or like orientation if IBM did – didn't work	or, like, orientation of IBM – it didn't work	Transcript Error
105	5,11	permission	permissioned	Transcript Error
106	12	asked it's	sked if it's	Transcript Error
107	4	has	had	Transcript error
108	4	Zurich	ETH Zurich	Clarification
113	3	if we	that we	Transcript Error
113	20	motiving	motivating	Transcript Error
113	25	important for people	important to people	Transcript Error
121	23	permission	permissioned	Transcript Error
122	17	didn't write	until I actually wrote	Clarification
122	25	is decentralized	as decentralized	Transcript Error
123	14	honesty	honest	Transcript Error
132	23	permission	permissioned	Transcript Error

134	25	permission	permissioned	Transcript Error
135	20 9	proprietors	properties	Transcript Error
140		would admit a system is decentralized, if it follows Troncoso definition.	would admit a system as decentralized, if it contradicts the Troncoso definition	Clarification
140	17	To my understanding, there is no definition of decentralization	To my understanding, there is no such definition of decentralization	Clarification
144	21	It would be if Ripple was actually	If Ripple was actually	Clarification
145	4	series	service	Clarification
145	18	opinion, as I stated my report, because of the	opinion, as I stated in my report, because the	Transcript Error/Clarification
148	8	depending	depend	Transcript Error
148	10	Newark	network	Transcript Error
149	8	such part	such party	Transcript Error
152	18	what a UNL does in Ripple code	which UNL to use	Clarification
153	16	ledger means the block -- XRP Ledger should be added to the blockchain	ledger means the block in the XRP Ledger – which ledger should be added to the blockchain	Transcript Error
155	24	default Version Ripple dot -- this 1.7.3.	default Version rippled -- this 1.7.3.	Transcript Error
174	9	I tried this convey this is one possible test	I tried to convey this as one possible test	Transcript Error
181	23	permission	permissioned	Transcript Error
182	2	permission	permissioned	Transcript Error
182	4	inclusiveness	inclusiveness property	Clarification
182	22	report	paper	Clarification
187	7,8,11	permission	permissioned	Transcript Error
187	6	and we discuss this	and we discussed this	Transcript error
188	24	inclusing this	inclusiveness	Clarification
189	19	takes	take	Transcript Error
190	4	on EPFL	at EPFL	Transcript error
191	16-17	with [redacted]	by [redacted]	Transcript error
191	17	it my head	it in my head	Transcript error
195	3	of the case	in the context of the case	Transcript error

196	12	I talk to SEC	I talked to SEC	Transcript error
202	14,17	permission	permissioned	Transcript Error
228	4,8	permission	permissioned	Transcript Error
229	10	struggling	struggling with	Transcript error
231	10	colleague	colleague who	Transcript error
234	7	coming	coming up	Transcript error
242	13	proof of state	proof of stake	Transcript Error
242	14	weight	weigh	Transcript Error
246	11,13	End function	AND function	Transcript Error/Clarification
246	18	network layer would probably be centralized.	network layer.	Transcript Error
252	3	partition	partitioned	Transcript error
252	4	to say unreliable network	to say this is "unreliable network	Clarification
253	13	official Lynch-Patterson consultancy possibility	Fischer-Lynch-Patterson consensus impossibility	Clarification
259	23	that favor in the	that favor safety in the	Clarification
260	8	that was opted	that opted for liveness/availability	Clarification
261	21	it tends	tends	Transcript error
263	5	That	That would be	Transcript error
263	17	role	rule	Transcript Error
263	20	forward network	forward progress	Transcript Error/Clarification
267	8	bettering the ability	better readability	Clarification
272	8	my miners with some	my miners and with some	Clarification
273	15	faulty	faulty nodes	Clarification
273	22	that and proof of work	that for proof of work	Transcript error
277	21	or a	of a	Transcript Error
282	9	relay	relate	Transcript Error
291	14	reserve	satisfy	Clarification
300	8	single people	single person	Transcript error
302	18	the guardian	the Guardian	Transcript Error
305	15	U.S. governments	U.S. government	Transcript Error
309	8	0.4	0.14	Clarification
310	18	mine	mined	Transcript Error
311	3-4	in protocol	in-protocol	Transcript Error
311	11	could not opt to	could opt to	Clarification
312	6-9	It's not correct that if a mining pool can opt which transactions to include, there are	It's not correct that if a mining pool can opt which transactions to	Clarification

		other mining pools that can opt to include the transaction	include that the Nakamoto coefficient would be 1, because there are other mining pools that can opt to include the transaction	
312	24	cash	hash	Transcript Error
336	20	use cases	use case	Transcript Error
338	8	pass from causal definition	go from the basic definition	Clarification
338	11	inclusive	inclusive systems	Clarification
338	13	on a	as	Transcript Error
339	21	Ripple D	rippled	Transcript Error
349	6	4.1	41	Clarification/Transcript Error
350	24, 25	natural cooperators	operators of XRP Ledger nodes	Clarification
353	13	UNL	UNL overlap	Clarification
354	18	ran	run	Transcript Error
355	2	and assemble	to say	Clarification
362	15	avert	alert	Transcript Error

Date: 20.5.2022

[redacted]

[redacted]

[redacted]