GARY GENSLER: So this is the last use case day. And then Tuesday we'll wrap up. And I know that you all are preparing for finals and writing final projects. So it thins out at the end. So I thank you all for showing up, those of you that are still here.

I also want to compliment. I didn't get through all of the papers seriously. But I did my best to read them quickly last night and today, that were submitted for today. And just like the ones on trade finance, they're really good. And if there was anything that was kind of the learning objective of this-- don't get too happy, James.

AUDIENCE: I submitted mine just now.

GARY GENSLER: What's that? Yeah. I read it. It was like two hours ago, you put it in.

AUDIENCE: I've got a slightly improved version.

GARY GENSLER: Oh, I don't think Canvas let's that. That's going to be a double spend wouldn't it? Sure. Send it in. Send it in.

It's to show critical reasoning skills. What is this new technology? Why does blockchain technology make sense? And just like in trade finance and identity management, there's data that really matters. And we'll talk about this a bit. But the data really does matter, our identity and so forth.

But I wanted to turn back to trade finance, just for a minute, because James had challenged the whole group about supply chain management. And Lauren was a little quiet. But she knows I'm going to call on her. So this isn't a cold call. But Lauren, you want to give your view on this a little bit? Lauren who worked in supply chain management for four or five years.

AUDIENCE: Yeah. So the big thing, I worked in supply chain sustainability, and there's been a huge push. The De Beers thing touched on this. There's been a huge push over the past five to 10 years to just increase traceability and transparency through supply chains to make sure conflict

minerals going to make sure that things aren't using a lot of water in water stressed areas and things. There's been a huge push for transparency through the supply chain and trying to figure out how companies can basically like audit and assess their suppliers, can take it layers back.

And so one big thing now is it's all done through-- most companies do it through assessments. So annually, companies assess their suppliers and hope that they submit all this accurate information and hope that their suppliers are doing the same things throughout the supply chain. But there is very little transparency into it. It's very hard to verify.

And there's really asymmetrical information on all sides. So block chain would be, I think, for sustainability purposes. Because right now you're just like hoping that companies are allocating the proper time and resources to go through and track their raw materials and suppliers and things. But there's no real verifiable or transparent way for it to be done.

And so right now, a lot of customers are hoping that their suppliers, they're taking them at face value when they say things like, we don't use child labor, we don't source from these certain regions. But there's really no way to verify it.

So I think a big opportunity for blockchain and supply chain is helping increase that traceability so that you know you're not coming from places where child labor is OK. Ideally, you're coming from places with good safety standards and things like that.

GARY GENSLER: Have we gotten at least-- are you still on the rock bottom minimalist side of supply chain blockchain management, blockchain technology?

AUDIENCE: Marginally better.

GARY GENSLER: Marginally better. But that's what's wonderful about this class. And even the eight or 10 papers that I read about identity management, identity and access management systems and blockchain technology, ranged. I don't think I read any that were at a zero. There were no absolute minimalists. But there were some of your papers that veered towards that. And Alin, who's going to talk to us probably sometime during the day, I'd say your paper veered towards the most maximalist side I'd seen yet in 23 classes.

AUDIENCE: With respect to a certain definition of digital identity, which is probably different than what most people think about.

GARY GENSLER: All right. So we're going to hear from Alin maybe in 20 minutes or something. But mind you, that's the surprise of the class. He's moved to the maximalist side, at least on one application for blockchain technology, which is also, I think, the right place to be.

This is a technology that might have use cases that work and others that are just hype. There might even be some digital native tokens that will survive. And most, in my thought, won't. But there might be some that make sense, probably more blockchain technology applications than tokens. But we'll start going through identity.

Again, we'll talk a little bit about identity before we get into it, identity and access management systems. But what is identity? Then, the sort of management of them, particularly in a digital age. Some state projects in India and Estonia. And then some blockchain technology projects, private sector in essence. And then, of course, some of you might be graduating. And we'll talk about MITs. It is MIT, had to do that.

And the study questions were, what are the trade offs. What does it mean to be self-sovereign identity? And how might blockchain technology address that? And we'll see a show of hands later how many of you plan to get your MIT diploma on blockchain.

I hope, by the way, that all of you plan to get an MIT diploma. But there are some of you that are from Harvard here and from other schools. So maybe you'll come back to MIT. And then there was a handful of readings which, at least from the write ups, seem like they reasonably did its job.

So what is identity? This is an open question. Tom. What's identity?

AUDIENCE: I was going to defer to someone who wrote the paper today.

GARY GENSLER: You were going to defer to somebody. I see. I see. Who wants to say what identity is? James, you wrote a paper for today.

AUDIENCE: You have a birth certificate, identifies you as an individual.

GARY GENSLER: All right. So is a birth certificate identity?

AUDIENCE: No.

GARY GENSLER: Who's saying no?

AUDIENCE: I don't think that the birth certificate is an identity because you can also be identified, for example, biometrically or with your fingerprint. So it is not only for birth certificate.

AUDIENCE: But it is an identity. Like if you go to the DMV and you're going to get a license, you need a birth certificate to show.

GARY GENSLER: All right. But is the birth certificate identity?

AUDIENCE: It is not what identifies--

AUDIENCE: It is like an identifier for [INAUDIBLE]

GARY GENSLER: Identifier. It's a certificate. Right? Hugo?

AUDIENCE: Yeah. I mean, I feel like this is super philosophical question.

GARY GENSLER: Well, maybe. Do you feeling uncomfortable with that?

AUDIENCE: No.

GARY GENSLER: All right. Good.

AUDIENCE: Like identity is basically like who you are. And all of the things that prove your identity currently are government issued documents or like school issue documents that prove that somebody else has already done a background check to make sure that you are who you say you are.

GARY GENSLER: Brotish.

AUDIENCE: I think identity is kind of contextual. So sometimes it can be a date of birth. Sometimes it can be your nationality. Sometimes it can be your face. It depends on the context what identity is.

GARY GENSLER: Eric.

AUDIENCE: It should be identity is-- going back to the philosophical domain. Identity is what defines you as a unique individual and differentiates you from anybody else. Right? And use additional instruments to serve the purpose of identifying you as an individual to certain contexts, as Brotish mentioned, that the identity is inherent to a person, not an additional artifact, in my understanding.

GARY GENSLER: So how many people agree with Eric? It's something unique that identifies.

AUDIENCE: I agree.

GARY GENSLER: You agree.

AUDIENCE: I think it has to be something that you can verify in order to be identity. Otherwise it's just a piece of paper.

GARY GENSLER: Wait, you think you have to be able to verify it. But Eric was saying that it's unique. It's something about our humanity. It's about who we are.

AUDIENCE: I think, as Hugo said, I think it's very philosophical. I think it's who I am. So like my identity is like what my name, what date of birth, and my iris, and my finger, this is who I am. And I think what you're talking about is more like how can the society verify that you are the one who you claim to be. So I think there's different kind of layers that we're talking sense.

GARY GENSLER: Alexis.

AUDIENCE: I think it's like not unique in a sense that it's like characteristics that someone has. But like maybe someone else will have the same characteristics. But it's more, Jahib just said, like basically someone can verify that what you say is true. Like if you have these characteristics, that's part of your identity. But it's not like unique in the sense that it's just--

GARY GENSLER: So, Alexis, are you saying your identity is not unique? Or are you saying certain attributes [INAUDIBLE]

AUDIENCE: It's unique for me. But it's just like aggregation of characteristics.

GARY GENSLER: Aggregation of characteristics. We are going to get philosophical. This is good.

AUDIENCE: If you want to get philosophical, you can say that the identity is what the society imposes upon you, or what the society makes up of you. Because, for instance, a name itself is not [INAUDIBLE] itself. It's something that the society or common culture construct.

GARY GENSLER: So you're saying it's not just who you are, but how society accepts you. In a commercial sense, in an economic sense, identity is used for so many things. I do believe-- and maybe it is philosophical. I do believe that we are each unique souls. And so that's a belief system, maybe.

But in an economic sense, we have various attributes. So those attributes might be shared. I

know, in fact, yeah. Woo. So what is identity? There is a dude up there that I share DNA with, exact replicable genetic material.

But I, for one, think that I'm unique from him and I have a different identity. And you can be guessing, while you pull this down from Canvas, who's who. It's not a test. What's that, James?

AUDIENCE: You're on the left side.

GARY GENSLER: I don't know which side you're pointing to.

AUDIENCE: Technically, the left side of the photograph.

AUDIENCE: You're on the--

[INTERPOSING VOICES]

AUDIENCE: As we see it, on the left side of the photograph.

GARY GENSLER: I see. Yeah. Yeah. You're correct. But see, we're unique. Different identities. Same DNA. Who has an iPhone with face recognition? So on Thanksgiving, Rob hands me his iPhone. He says, what do you see? He says, just look at it.

And I look at it and I say, I see a bunch of text messages. Why? And he cursed. And he said, I handed you my locked phone. So whatever you think about biometrics and iPhones, it didn't work. Or it does work. I don't know.

So I handed him back my iPhone, which a little older. And I said, could you open it for me with your thumb print. And he couldn't. So just for now, we have a number of sets of identical twins in my father's family and so forth. So he tried it with two of our identical twin cousins, two women. And they, too, can open each other's phones.

AUDIENCE: With fingerprints?

GARY GENSLER: No, with their face recognition. Not with fingerprints but with face recognition. So it just is a little side story about identity. Eric.

AUDIENCE: Just a comment that there's a function in Facebook that shows you a list of photographs that you potentially can be identified and tag you. So I keep getting pictures of my twin brother, too. So, yeah. Very poor face recognition today.

GARY GENSLER: You're identical?

AUDIENCE: Yeah.

GARY GENSLER: OK. When I hear fraternal, then I have another thing about Facebook.

AUDIENCE: But there is actually a much simpler way to define identity. Philosophy aside, there is this physical human being, and there's billions of them on the planet. And one simple way to think about it is you want to hash each person.

GARY GENSLER: All right. We're back. We're back to the hash functions. This is good.

AUDIENCE: But that's actually what you want to do. You want to hash each person and get a number. And the property of that is that if you come to me and I hash you, I get some number. And if you come again, I get the same number. So I know I'm dealing with the same person.

GARY GENSLER: Even if I put weight?

AUDIENCE: Even if you put on weight. I can hash because I can use your iris, let's say. Then your twin brother presumably won't have the same iris. I'm actually not sure, but I don't think you will. So now a hash you, I get the same number, I know who I'm dealing with, and this solves a lot of the problems in the business world. Like KYC, getting a credit card at a bank, stuff like that.

And it also solves the problem, are you a new customer. Well, is your hash one of the new hashes that I-- is your hash a hash that I've seen in the past? So that's a very simple way to think of identity.

And you put philosophy aside and you assume that there is some physicality of human beings that you can distinguish between using a hash function of some sort. So the question is like, how do you implement this hash function.

GARY GENSLER: So you're not really putting philosophy to the side. You're saying, that may be all well and good, but you can also take a physical object, a human, apply a hash function, a cryptographic means, and get a unique identifier for that individual.

AUDIENCE: I have a counter question to that. So let's say you hash everything. I can have a counter feed of like five things that can essentially be the same thing. And you'll just have five different hashes for it. Right? It will still have to come from a non-blockchain source for you to be able

to--

AUDIENCE: Well, it's not things. It's human beings.

AUDIENCE: OK. But for you to be able to hash one person, you can still reproduce five other fake people and have five different fake identities with a different hash.

AUDIENCE: So that's the difficulty, right? You can't actually-- if I hash myself and I get a hash, you will have a lot of difficulty producing another human being. It's like finding the collision in the hash function. You have a lot of difficulty producing a human being that has the same hash as mine. Because the hash function is collision resistant. And it's hard to come up to clone me 100%.

For example, my retina, even if I give you all the data behind my retina and you have it, it's very hard to produce a retina in your own eye that you can scan and pretend to be me, for example. That's one way to think of hashing somebody. You just scan the retina. And even though you know the full retina, it's of no use to you because you have to put it in your eye and go there and get scanned. And it's like, OK, fine. Well, our medical technology is not there yet.

GARY GENSLER: [INAUDIBLE] And then we're going to move on.

AUDIENCE: I'm just going to say, if you want to take it-- it's not even your physical representation. Right? Because you can change what you are physically nowadays. And so it's like what you know, what you are, and what you have, the three things that you can put into this hash function.

AUDIENCE: Well, it should be-- it should be. You're right. It's not the whole of you. You have to do it very carefully. So the question is, how do you [INAUDIBLE] person. Because if you go by weight, let's say the hash function is your weight. Well, that's bad. Because you get collisions. So you have to do it very carefully, for sure.

GARY GENSLER: So, Eric, did you have something to add?

AUDIENCE: [INAUDIBLE] But actually, the main point of your elaboration is the biometrics behind the whole-- because it's not the hashing that's making this possible. It's the biometrics. Because you have to actually hash something.

When you come from the abstract construct of saying, hash somebody, you're actually saying, you're hashing some biometric attribute that has to be unique to get the hash.

AUDIENCE: I'm sure hashing a person is an abstraction for, let's say, take a biometric, it's actually collision

resistant.

AUDIENCE: The point, the really important point, it comes to biometrics.

AUDIENCE: That's right. That's right. And then the question is, well, biometrics get stolen. How do you deal with that? Then you have to be very careful with it. There's nowadays, you can actually, if you aren't careful, it can get stolen.

GARY GENSLER: [INAUDIBLE]

AUDIENCE: Yes. So to Eric's point, I think that's still an identifier. It's not really your identity. Because like you guys are saying, you can replicate somebody's retina, let's say, 1,000 years or 10 years down line, I don't know.

AUDIENCE: Perhaps. That's right. That's right.

AUDIENCE: Or they replicate somebody's fingertip. But that doesn't mean that you're replicating their entire identity. So I like the idea of hash somebody's identity, hashing a person. But I don't think it's just hashing their eye or just hashing their--

AUDIENCE: That's right. But I think you're getting philosophical. I'm looking through the perspective of a bank, a verifier. What does a bank actually need to do? It just needs to map everybody to some number. And when you come back, it needs to figure out which number you are or if you're a new number. That's all you need. And then, problem solved.

And then by the way, personal data attributes, you just link those to those numbers. It's not a difficult problem. It's an orthogonal problem. You solve that [INAUDIBLE]

GARY GENSLER: So let's agree that-- what Alin is saying is he's not talking about our soul or our unique identity. He's talking about something that a verifier or a bank might be able to do. And then you could say here's 7 billion people on the planet now. And there'll be 10 or 12 billion one day. But you could take each one of them and somehow have a unique identifier, a hash function, that has each of those.

Don't do it off of DNA though. Because Eric and I, you know, and hundreds of millions of others would-- so DNA is not a unique identifier for true identity. So the concepts of identity for things that I think about sometimes, some of the papers were about three. But there's attributes, a claim, a credential, an attestation.

What would be an attribute? Just any old attribute of a-- anybody?

AUDIENCE: Your retina.

GARY GENSLER: Your retina. Or it could be your age, address, citizenship, name. A claim is, my name is Gary. Or a claim might be, I am so old. Or I am a US citizen. Or a claim might even be, I have $5,000 in my bank account. There are other forms of claims. Or I do have a bank account at Bank of America. I don't think I have $5,000 in it right now. No.

A credential is what we started with. I think James mentioned it, a driver's license, an ID card, a utility bill sometimes. I mean there's hundreds of forms of credentials. We think of the governmental credentials.

The history of credentials is interesting. The first tens of thousands of years of human kind didn't have any. And we started to have them. Passports really aren't even that old of an invention. In the 16th century, the King of England had some pass boarding. But it was so that his citizens could be recognized in other countries. It was so that their rights would be respected and somebody would not be messed with. I'm under that sovereign, don't mess with me.

But in terms of a true permitting system, it was largely implemented about 100 years ago. Anywhere between 100 and 150 years ago. It's not that old a system. But it was all paperwork. And I don't know if any of you have ever asked to see a grandparent's or great grandparent's or an ancestor's passport or those documents, if you have them. But they're intensely paper.

In fact, if they're from the late 19th century, there's no photographs. They started to have photographs in the early 20th century. And so it's a big change. And the last 30 or 40 years of digitisation of this has actually made it a little harder, in some ways. I mean there's efficiencies. But it makes it harder.

And then attestation is that third party verifying it. And that's what Alin was talking about. If somebody can verify your identity, they're basically-- I make a claim. My name's Gary. I might give a credential, my passport to show it. The picture looks like me. A human looks at it. Lines it up. Says all right. You can enter the country of Germany or wherever I'm traveling. They don't actually know that I'm really-- but they do some verification.

So those are the big kind of pieces. Identity and access management systems, the functions--

and these are just taken from a bunch of readings-- authentication and then authorization. Authenticating that I have the bank account. Authorization, I can use it. Or authentication I'm a US citizen. Authorization, I can come into the country of Germany. So based upon some attribute, somebody authorizes me.

Or something that maybe some of you have dealt with at some stage of your life, that first time you went in and handed a driver's license in so you could take a drink at a bar. Let me make it tangible. That's like authenticating, do you look like that person.

And then who are the parties in this system? Users, service providers, identity providers. Anybody want to tell me about this ecosystem at all? Alfa, you didn't write. You wrote last time. Tom.

AUDIENCE: Again, I didn't write. But the idea of identity provider is interesting. It fits in our conversation, right? If we're talking about your identity being who you are, it's really identity verification provider. They're providing the documents.

GARY GENSLER: I think that's right. I mean, in a sense. Though identity, in a more philosophic way, is who you are. But yes, the identity provider can be somebody like the state of New York or the Commonwealth of Massachusetts, birth certificates, death certificates, marriage certificates.

Attribute authorities, like certificate authorities, are kind of a more recent invention. I don't know that they existed 100 or 200 years ago. But an attribute authority says, these attributes, we'll validate them. They're central authorities that say, yes, this is correct. And certificate authorities are particularly an invention of, what, 40 years maybe. The internet, 30 years.

AUDIENCE: I think the thesis was an MIT thesis in 1976.

GARY GENSLER: 1976 thesis at MIT.

AUDIENCE: If I remember correctly.

GARY GENSLER: Did anybody want to say what a certificate authority is? Because they're in the middle of all of that. By the way, every time that you go to the internet today, a certificate authority is involved in that transaction, probably 100 billion times a day around the globe. Yeah, that's probably the order of magnitude. Probably 100 billion times a day, a certificate authority is used. Alin, you want to--

AUDIENCE: Sure, yeah.

GARY GENSLER: Certificate authorities are how we access the internet all day long.

AUDIENCE: You want an explanation for what they are on the web?

GARY GENSLER: Yeah.

AUDIENCE: Right. So on the web, you have a bunch of websites. Let's say you have facebook.com and you want to visit it and give it your password. So if you have evil people like me, I might set up a fake server and pretend to be facebook.com, mess with the DNS records, get you to visit my server. When you type www.facebook.com, you visit my server. But you can't tell.

GARY GENSLER: DNS is Domain Name Server.

AUDIENCE: But anyway, the idea is that when you actually do a look up from facebook.com from an IP address, that's actually very insecure. And attackers can mess with that and redirect you to their servers. And they might completely replicate the Facebook page so you might think you're interacting with Facebook. But you're not. You're interacting with an attacker website. And you type in your password and your user name, and then the attacker steals it. And then he just redirects you to the real Facebook and you won't notice the attack at all. Does that make sense?

GARY GENSLER: And it all happens in nanoseconds.

AUDIENCE: Right. And it's called the man in the middle attack. So what you do is you use public key cryptography to solve that problem. You say, OK, let's give each website a key pair. So facebook.com will have a key pair, a secret key and a public key.

So now, the question is, well, there's a public key for facebook.com, but how do you know you have the right public key for facebook.com. Because an attacker could also give you their public key their fake facebook.com. So now, how do you distinguish between those two? That's where the certificate authority comes in.

So the certificate authority signs these public keys. And you have the public key of the certificate authority. You have a signature from the certificate authority on the public key of facebook.com. You're now ready to trust that you're dealing with the real facebook.com and you can encrypt your password to facebook.com using your public key. There's a lot of public

keys around. I know. I'm not sure if that made any sense.

GARY GENSLER: So we earlier learned about public key and private keys as part of blockchain technology. But know that when Satoshi Nakamoto wrote that paper, she was just using asymmetric cryptography, public-private key cryptography, that had been invented really in the 1970s. And then it adopted, as the internet came along, and took off and had a lot of use in the 1990s to secure the internet by 1996.

And the way that the internet's secured on TSL and SSL and these various ways it's secured was public key-private key cryptography, a full 12 years before Nakamoto wrote the paper, but used for a different case. But Facebook has a public key. And all those public keys of all the websites that you visit every day, there is a central authority called a certificate authority. There's actually a 100 plus certificate authorities.

But certificate authorities that say, this is the Facebook public key. So that when you go to your Facebook or you go to Google or you go to shop on Amazon, you know you're actually-- so that's a corporate or that's another form of identity. It's not one with soul, I would suggest. That's not a negative thing about Facebook. I just don't think websites-- but you all might have a different philosophy. I didn't think websites have soul. Brotish.

AUDIENCE: It's not clear to me how, as a user, I know that I'm going to the right website. I understand certification happens [INAUDIBLE] But how do I know that I have the right website.

GARY GENSLER: I'll try to do it in lay terms. And then you'll hit it. There's kind of a handoff that when you send that signal, you're trying to access-- is it Facebook? You're accessing Facebook. They send you some information, including their public key that you're-- in essence, a certificate authority is automatically checking. But Alin will give you the more technical.

AUDIENCE: Let's use a simpler example. Let's say you want to go to *New York Times* and you want to read a headline that says something about some important things, like tomorrow there's going to be a snow storm. Obviously you want to know if you're dealing with the authentic website. That seems to me the problem. So how do you deal with that?

Well, remember the *New York Times* will have a public key. It will have a corresponding secret key. So you visit their website. It turns out that when you download the website from the *New York Times* with that announcement about the snow storm, that's actually signed with their secret key to verify the website that you get. You verify it against their public key.

And you know that only they know the secret key. So only they could have offered that information and signed it. So then you know you're dealing with the right website. It's literally the *New York Times* sends you a signature over every piece of information they send you. And you verify it against their public key, which in turn you verified it from a certificate authority.

GARY GENSLER: If you remember the little bit of broccoli we did earlier this year, that asymmetric cryptography with a public key and a private key also has digital signatures. So you have, now, two things. Let's go back to Bitcoin.

In Bitcoin transactions, you have a public key. And then somebody signs a transaction. And the math behind it, the cryptography behind it, is a signature and a public key that come from the same private key. There's a way to do a function to check that they came from the same private key.

And the heart and soul of what was invented in the 1970s was not just that there's a public key and a private key, but also that you can digitally sign it. And then when the digital signature is compared to the public key, it's unique if they came from the same private key.

So going back to the *New York Times,* the *New York Times* you have both their public key and then each headline, each piece of information has a digital signature. And of course, you do have a centralization, a lot of centralization, on the internet related to these certificate authorities. Eric.

AUDIENCE: Just a point maybe to clarify, this is performed at a protocol level. That is not the user witnessing any of these interactions. It's done at the top of the TCP ICP stack, this TLS, which is the security protocol that works with HTTP, which is web.

And this is where you find that this little lock in the browser that's guaranteeing that that's the website you're visiting. Because the whole exchange of information that includes the public key from the website and the verification is done by the browser. You don't do anything interactive.

GARY GENSLER: We don't do anything. That little lock has that meaning. And you could actually see what certificate authority. I only pause on that to pause not only to tie back earlier conversations about public and private key, but the whole internet is reliant on these certificate authorities. And blockchain technology might be a way to step around and have a new paradigm. Kelly.

AUDIENCE: So for a contextual example, say I'm trying to access my brokerage account or whatever. And say I forgot my password. Or every month, they want you to replace this or that to protect your account. How does a person interact with these various parties going through that process when it's trying to verify that it's you gaining access? What are the points of contact for those?

GARY GENSLER: There is an initial layer, which we were just talking about, that you're actually dealing with you're-- I don't know. I'm going to make it up. DE Shaw. Or no, that's a hedge fund. With--

AUDIENCE: Bank of America.

GARY GENSLER: Bank of America. Fine. That you're really dealing-- so that's what we were talking about that. They are Bank of America. And you're really dealing with Bank of America. And you don't even participate in that.

But then there's another layer that if you've forgotten your password, they're going to ask you a bunch of questions, like the usual questions about who was your first pet and who was your first significant other and things like that. But at some point in time, they'll freeze you out.

AUDIENCE: That's the service provider that you registered with. That's Bank of America.

GARY GENSLER: That's Bank of America has their anti-fraud provisions. What we were just talking about is really at the internet browser. And in essence, Facebook is the one that's trying to be identified. 100 billion times a day, some human around the globe is trying to be protected, that they know they're dealing with the right identity on the other side.

We were talking about human identity. There's also the identity of the websites. And that's what we were just chatting about. Let me move on. And then if I've left you confused, because you were asking about what happens if you forgot your password--

AUDIENCE: Right. Like how do they verify you, not you verifying them.

GARY GENSLER: How did they verify you? I would contend it's still kind of a little archaic. I mean, it's a little bit like if you forgot your-- a couple of times you use a username and password, and of course if you have dual authentication, they might send you a notice to another text message or something. But if you've forgotten your password, then it's literally backdoor sort of saying, well, to remember your question.

I never remember the questions. I mean who is your first friend in elementary school? What

was the first car you drove? It's crude. And then they usually freeze you out for fraud protection after two or three times of trying that. And almost always, there's something where they can send it to you another place.

Identity management, some of the pain points. What are we trying to solve? And why would blockchain technology maybe help us out? Privacy and security is a big one. There are a lot of thefts, identity theft. How many people are in the room have had their credit card-- this year, in 2018, we're 11 months in-- have had their credit card have to be replaced because the bank got in touch and said it's compromised? Only about 20% of us. I would have thought it was going to be more. I feel like I get one of those calls every 18 to 24 months. Maybe I shop too much. Or my daughters are using my card too much.

AUDIENCE: [INAUDIBLE] big enough to be a target. Student banks tend to be negative.

GARY GENSLER: You think that's it? I just assume that some merchant has been hacked again. I mean, every time a merchant loses 1 million, or 100,000, or 50 million accounts, then the banking system needs to send out those notices.

I chair a commission, Financial Consumer Protection Commission of Maryland. And the credit union advocates in Maryland came to our commission and said, we need some help. We banks and credit unions have to protect a lot of data. But every time a merchant loses data, it's us credit unions and banks that have to replace all the credit cards.

And they feel there's an asymmetry, commercial asymmetry, that the banking sector is bearing the brunt of other merchant's, non-financial sectors, data breaches. And should the state of Maryland-- this is a live issue actually in front of our commission. Should the state of Maryland change its laws to put higher cybersecurity responsibilities on non-financial sector actors?

And the financial sector would say, yeah, that kind of feels you'd be leveling the playing field. And the merchants are saying, you can't do that on every grocery store and bar. It seems like it's a little out of sync.

AUDIENCE: Yeah, I was going to say that credit card theft like this is a perfect application public key cryptography. The [INAUDIBLE] don't give out your credit card number to these folks. Your credit card should have a key pair. It should have a secret key and a public key. And you give your public key to Amazon.

And then how do you pay Amazon? Well, you sign with your secret key that's on your credit

card. So nobody knows your secret key. It's on your damn card. Never lose that card. And problem solved. They can steal as many public keys as they want. Problem solved. Same thing with the SSN. Why would you share that--

GARY GENSLER: I disclosed to you. He became a maximalist, almost.

AUDIENCE: [INAUDIBLE] I'm talking about public crypto here, not without consensus. Although, consensus can be a very important part of all of this.

GARY GENSLER: Almost. Almost. All right. So let me just hit. So in terms of the big pain points-- privacy and security, a bunch of identity theft, forged credentials, back to the passport or the driver's license or the credit card, a forged credential, whatever that is. And of course, just how do we update our personal identity for any time we move?

And this term PII is three letters you'll learn in business. Because at some point in time you'll be running a business and somebody will be coming in, your chief of information officer, and say, we've had a breach. And unfortunately we broke some laws, too. Because in the US and in other countries GDPR, you have to protect certain data. And it's usually called PPI. It's usually the bucket of data you need to protect.

But every time you update your personal information, how do you how do you keep it updated? Ross, was there a question?

AUDIENCE: I just had a question back on your Maryland example. I make the assumption, maybe it's wrong, that if your commission allows the banks-- or passes that regulation--

GARY GENSLER: We're just an advisory. But if we recommend to the General Assembly.

AUDIENCE: That the banks are not going to lower their fee to the merchants. So what's the dollar number that they're trying to push? In other words, I'm trying to size the pain point. What's the amount of cost to those banks that they're trying to move to the merchants and thus drop from the bank's bottom line?

GARY GENSLER: I don't have a figure. It's a very good question. What we know is that the overall statistics on fraud and credit card is, I think, high teens basis points. I can't remember, 15 or 18 basis points but less than 20. And it's more than 10. So Visa Network charges 270 basis points or so. And the fraud part of it's 15 or 18 basis points.

AUDIENCE: And the issuing bank gets how much of the 275?

GARY GENSLER: 200 or so.

AUDIENCE: Yeah. So they want to [INAUDIBLE] whatever that is.

GARY GENSLER: But I don't know-- and this is particularly credit unions are coming to us and saying there's an externality, the merchants, the gas stations. All right. So you're saying, I know which way you would vote on our commission.

So what's going on a little bit about data breaches? I just tried to sort of list anything over 100 million customers. But then I had to put Facebook in because it was 50 million. But these are just like a dozen or so really big data breaches. There are so many data breaches in 2018 alone that you couldn't list them on a page like this. This is the last five years of 100 million people or more data breaches. So there's a problem here in cyber secure. And this is just the US. Brotish, didn't the Indian system--

AUDIENCE: [INAUDIBLE] more than a billion.

GARY GENSLER: 1.1 billion people's IDs were hacked in India. It was announced in January of this year. And so, it's a lot going on. And every once in a while, politically it captures the attention of particularly Equifax did, Facebook does. Wells Fargo, I think the breach was 3 million. It's not even on this. It wouldn't get to the 50th page by size. But Wells Fargo had other issues that was capturing the public attention. Kelly.

AUDIENCE: Just taking the Marriott one as an example, that's been the most recent one in the news, I think. It's so costly to these corporations. I think Marriott even said that they would pay the fee to replace passports for those affected. I mean, maybe it's a drop in the bucket for them. But in terms of the value in pain points, sort of like you were talking about, it's a lot.

GARY GENSLER: It is a lot. But one of the challenges that blockchain technology solutions is adoption. How do you get Marriott to contribute to a new system if you come up with a really clever, creative, new system? Because there are so many thousands of merchants that are trying to deal with their cybersecurity risk. And Marriott, all of a sudden, has all these costs.

But how you get them involved in your new blockchain technology solution, I think it's just an adoption issue, which somebody might solve. Or as Ross says, well, wait a minute. If the banks were to just [INAUDIBLE] right?

AUDIENCE: If they want to cut the fee and let everybody else-- then that's fine. But the merchants have no bargaining power.

GARY GENSLER: That's true.

AUDIENCE: So they cut the fee.

GARY GENSLER: So a couple of state identity projects. Estonia has e-identity. They started in 2002, well before blockchain technology. And it's run on a software called X-Road software. And while some folks might think of Estonia as a blockchain friendly nation, does anybody want to take a guess whether this software has blockchain technology? What's the consensus? No. It's not.

That doesn't mean it doesn't work. But they've sort of wrapped themselves in this sort of spirit of we're a blockchain nation. And they also have e-health records and many other records that are going online. And it may be, at some level, inspired by that. They have 1.3 million people in Estonia.

I think a bigger state actor in the challenge-- sorry, Brotish-- is Aadhaar. So there's a national identification system. And it was promoted really for inclusion, financial inclusion, and a way to get government assistance and welfare to hundreds of millions of poor.

India at the time that it was rolled out, well over half of India did not have a banking account at all. 12 digit ID and biometrics, being fingerprint and iris scan, I think they would deal with the identical twin issue. I think, from my little example that my twin brother Rob's finger didn't open my iPhone.

But there's been a lot of problems. And that's not a blockchain project either. But my read of it is Aadhaar-- and maybe Brotish has some views-- has done some very positive things in India. But it's also come with some very scary things. Brotish.

AUDIENCE: It's a quick nugget of information about Aadhaar. It was the fastest system in the world to reach 1 billion users, faster than Facebook or any other online platform. And [INAUDIBLE] optional, I mean it was not a mandatory system for people to get it. It was optional system. But it was the fastest one to reach 1 billion.

GARY GENSLER: But it's optional. But you can't get your government assistance any longer if you're not in it, right?

AUDIENCE: It's not like that. So actually, there has been some government efforts to make it that way. But then the court actually rejected those proposals. So they said that you cannot make it mandatory to make people receive benefits based on this. So whoever has that, they might have some ease of obtaining those benefits. But it's not like without it, you cannot get [INAUDIBLE].

GARY GENSLER: So Brotish is saying it accurately. But the court only ruled that this year during 2018 I think. And for a while, hundreds of millions of people thought that's the only way I can get my assistance. But the 12 digit ID and the biometrics has produced a system where, along with a payment system where you can do a QR code right on your iPhone and get goods and services, and it's pretty efficient. But it's one national system.

One national system and there's been a lot of challenges. Not just the hack, but also some mistakes sometimes. And based on those mistakes, people feel like they've lost their identity. I mean, they're still this human that they are. But they've lost it in a governmental sense. And thus they've stopped getting their assistance.

And there's occasionally reports of suicides, and reports of deaths, and things like that where people are no longer recognized in the system because of their Aadhaar ID. So there's a lot of public debate in India about the net benefit versus some of the costs.

Self-sovereign identity, four things I think about. People and entities control their identities more than we have now. This is a concept. We have direct access without some intermediary. Our identity is transportable. But not our human identity, but the attributes of our identity. So I use the term more loosely here. And then, it's widely usable or interoperable.

Self-sovereign identity-- what's that?

AUDIENCE: I was just thinking [INAUDIBLE]

GARY GENSLER: Yeah. I kind of remembered that back and forth. Self-sovereign identity does not rely on blockchain technology. It's a concept in a debate about should we go back to something that we, in a sense, had in the 19th century and even early 20th century that we could walk into any store and there might be other forms of censorship.

There are certainly many prejudices and racism and all sorts of challenges. But we could walk in without a document. We weren't walking in. We might have some gold, some money in our pocket. They would take the gold coin or the silver coin.

Self-sovereign identity is also thinking about can we have the individual hold their credentials as we held a physical passport but hold it in a wallet in some way. Ross.

AUDIENCE: Just your example of the 19th century ties into the question that I had, which is doesn't this only work if you also have a decentralized money system. Like go to your example. Only reason that works is because people could go in and pay with a completely anonymous form of money.

Unless you have a real broad, say, Bitcoin distributive system, your bank will require you to waive this. When you sign up for a bank account, you will have to waive this. And it's gone. They just will.

GARY GENSLER: So Ross is raising, well, will this even work unless you have a truly decentralized money system. I don't think it's reliant on a decentralized money system. I can see your point that it's benefited by a decentralized.

AUDIENCE: Any commercial transaction you have, the counterparty-- Facebook will make you waive. Because they want the information. And Google, that's right you could cut yourself off from all those things. But they'll just make it as part of the contract, part of the access, that you waive.

GARY GENSLER: So self-sovereign identity, concept that all of us humans could control our identity, not just our birth and our nationality, but maybe even our digital footprint, our spending patterns, and so forth. And Ross is raising, well, maybe Facebook and Google wouldn't transact with us as a commercial reality. You're saying their market power, they might cut us out. I think some might try. And that will be-- this hasn't been really adopted, self-sovereign identity.

AUDIENCE: Hell of a question for you Consumer Protection Commission.

GARY GENSLER: Yeah. Maryland probably won't be able to weigh into that too much. The benefits of taking identity access management systems onto the blockchain technology, and eight or 10 of you wrote papers on this. Does anybody want to comment on-- this is like, my summary, some of the benefits.

You can address verification costs and fraud. You could potentially lower some of the cost and fraud. I think you can trace provenance. You deal with censorship and so forth. And truly, I think you can help on privacy.

But the challenge is-- the real challenge is that if you're storing personal identifiable information on a blockchain, blockchain technology works by distributing the data to all the nodes. And so the initial write ups, three and four and five years ago, were, like, well, could you put self-sovereign identity in essence in a blockchain and store it? And everybody started to say, no. You really can't do that. Because you're not going to put all my personal stuff on 10,000 nodes.

AUDIENCE: So I mean, the first benefit there, I think, should be prevent identity theft. Because the main security goal of any identity scheme, including the one I described, is you want to prevent identity theft, to prevent impersonation--

GARY GENSLER: I'm sorry. I'm going back. I just chose not to read through this page. I'm agreeing with you. I mean, these are the pain points it would all address.

AUDIENCE: And in general, I think, when you think about identity, you have to look at it through that lens. Because what else is identity for if it's not for preventing people to claim they're someone else? That's what an identity scheme does. If your scheme doesn't address that fundamental problem-- like by the way, all of these startups don't. Because SSN numbers are still out there and require [INAUDIBLE]. So as long as that's--

GARY GENSLER: Social Security Numbers.

AUDIENCE: Yeah. Say goodbye to prevent identity theft. What are you doing then?

GARY GENSLER: I think, I'll go here and then Hugo.

AUDIENCE: Yeah. And something that was not very much addressed in the readings, I thought, was also the fact that if you used a blockchain technology, so evidently not. It's immutable. So it's often seen as a good thing. But here in this case, normally, like for example in Europe, normally in the internet, you can request to delete information you have if Google has a link which mentions you for instance. But here, you wouldn't be able to do it. Because the information is there. If someone steals or even if you want it deleted it, somehow you can't because it's immutable. So how can we deal with this?

GARY GENSLER: So you're raising a point that in Europe under the new privacy law, the GDPR, you have a right to be forgotten or right to be deleted. And so how can blockchain technology interact and work within that framework?

If your actual information is on the blockchain, I think you're right. I think it's very hard. But I do think there are solutions if it's just a hash of your information that's being stored on the blockchain.

AUDIENCE: Yes, but they were mentioning in the reading as well the fact that you can store all the data, basically, of the blockchain. And then when you transfer it, you just say like as a certification, oh, yeah, this is my information. And it is true. You can verify it is true. But you cannot have like--

GARY GENSLER: The actual information on a distributed network. Kelly.

AUDIENCE: I think that's a really interesting point. One of the sort of use cases I think of goes back to the original attributes you were talking about. So for example, what about citizenship? If in your digital identity it says you're a United States citizen and that changes, can that be changed if it's immutable, A. And then B, what about those privacy issues? For people that do not have, maybe it's not a fully verifiable citizenship, then we have a whole host of problems there as well.

GARY GENSLER: So I think you raise a good question. But this is one of the challenges of any identity database. But it's also a challenge of a money database called Bitcoin. You have ownership today. And tomorrow you might no longer have the coin. Today, you might live in Massachusetts. But a year from now when you get your fancy job and wherever you are, you might not live in the Commonwealth of Massachusetts.

So I don't think it's just citizenship. It's just the updating the records and the attributes, that you no longer can vote here, can no longer--

AUDIENCE: It just goes back to the trade offs that we were originally talking about. There's a lot of-- it certainly helps a lot of things like preventing identity theft. But there's also a lot of other [INAUDIBLE].

GARY GENSLER: They're challenges. But I think that challenges is surmountable.

AUDIENCE: But even though it's immutable, you can append new information. So isn't that the whole purpose of blockchain. Your citizenship may change, but then you append new information saying that your citizenship has been updated. And that becomes the source of truth now.

GARY GENSLER: I'm agreeing with that. I think that's correct. I think that's a solvable challenge. Hugo had his

hand up. And then we're going to go on just to--

AUDIENCE: So I'm going to question the idea that having a blockchain means identity theft is no longer an issue. I think it makes it a bigger issue. What happens if you lose your private key or if somebody finds a private key or somebody cuts your eye out or whatever? But really, if somebody steals your identity, then it's gone. You're not getting it back.

GARY GENSLER: Oh, steals your private key. Your identity identity is stolen.

AUDIENCE: Steals your private key. If you don't protect that with your life, then your life is gone.

GARY GENSLER: Right. I think Hugo's raising the right question. But that just means that's not the right solution. You can't pin it all on just one private key that's lost.

AUDIENCE: Well, the answer is also use multiple biometrics. And yes, sure, if you lose your hand, your eye, your retina and you go to the DMV, maybe they'll make an exception for you. Hopefully like 10 people ever show up that way.

GARY GENSLER: Let me try this-- plow in for a second of what are the projects. And this is a short representation. I could have made three more pages of representation. I'm going to hit three or four of these just for fun.

There's three or four that are ICOs. I'm going to choose to skip all of those. But there are, I want to mention that Civic Secure Identity, Existence IC, Sovrin which gets-- S-O-V-R-I-N-- but Sovrin that gets a lot of write ups in other papers were all ICOs, Initial Coin Offerings, to use a token to incentivize a system of, usually, self-sovereign identity at some point.

None are up and running yet. And I have my doubts about some initial coin offerings. But there are three or four. And there were probably six or 10 others that I didn't quickly find.

Bitnation's an interesting project that literally you can voluntarily get a citizenship in Bitnation. It is a decentralized borderless voluntary nation. But the keyword is voluntary. They don't have a UN membership. They're not part of the World Trade Organization. They have no geography. But the concept is, you can get a Bitnation passport. And you can get some authentication through that about some attributes about your birth and things like that.

There is a standard setting group, Distributed Identity Foundation that we're going to talk about in a minute, and I'm going to show a slide, which is just a whole bunch of efforts coming

together and saying, well, maybe we can do some standards around this. And then there's Rebooting Web-of-Trust that runs events. I think their only economic model is to make money on the events. But some of their research and some of their papers are very interesting, that you can read about this.

And not listed on this, one area that's spending a lot of time on self-sovereign identity is the World Wide Web Consortium, W3C. You can go and on GitHub you can read all sorts of information from W3C about self-sovereign identity. And they're promoting ways to do digital ID, and trying to form standards.

So I think W3C, which is not really a blockchain project, and this Distributed Identity Foundation, for any of you that are actually interested in pursuing some of this, you want to stay abreast of it. Because it's the standard setting also that I think will be relevant. But questions or thoughts for those who have done research on some of these? Other than Alin who we've heard from a bunch. All right. What's your question?

AUDIENCE: Well, my first thought is they don't solve identity theft in the United States.

GARY GENSLER: They don't solve identity theft in the United States.

AUDIENCE: Why? Because there's a certain policy by the US government that asks everyone to accept SSNs. And if James has my SSN, then James is me for all intents and purposes. So that is a policy issue. So these companies are basically a very inefficient way to change the policy. Hundreds of millions of dollars being invested in all of these guys. And by the way, all of them do public key crypto. It's not like something revolutionary here.

But at some point, some of them will get some market share, maybe convince a few banks. And maybe those banks will convince the government to start doing--

GARY GENSLER: So you're saying that an underlying challenge, at least in this country, is that we have an antiquated public policy related to a tax ID called social security number. And initially, social security numbers were not even a tax ID. Initially, they were to participate in a retirement program called social security. And you were not legally required to have a number in the 1930s or '40s when it first came about.

I didn't get my social security number until I was 14, I think. Now you pretty much get them at birth in this country. You can't use it for much. You're not working. But you're saying it's a public policy challenge, at least here. I would say in every country, there's some public policy

challenges that are very real around how attributes of identity are measured, whether it's off of taxes or birth records and so forth.

Can I hold? Because I want to just hit two other things. This Foundation, these are all the people in this Foundation doing all of this work. It's just a list that you can look at later. And they've set up-- and I apologize-- they set up sort of this whole idea about decentralized ID and server. So they have a whole program. It's not a small effort that they are investing in this.

And I only put it up to say, there is a lot of energy. And Alin might be right, it's all fraught with some risk because it's on the backs of government ID systems, not just in the US.

Public key infrastructure could change. And a lot of these concepts are on decentralized public key infrastructure. Basically, where are these public keys? Whether it's Facebook public key or any public key, where is it stored? I suspect, Alin, that you'd say this is at least going in a little better direction.

This is a key part of just saying, instead of the public key and having these certificate authorities, to have a secure way to store the public keys in a decentralized, hashed, using hash functions and blockchain technology. And I think all of them have this in the middle of it somewhere.

AUDIENCE: It's a consensus problem. You want to agree. Everybody needs to agree with Facebook's public keys otherwise we're in trouble. Because you might use my fake Facebook server. So it's really just a consensus problem. It's not about hashes, security. Forget about that. Everybody has to agree what Facebook public key is. And that's where the blockchain comes in.

GARY GENSLER: Sorry. Shawn.

AUDIENCE: I just wanted to answer Alin's question. I don't think that's a public policy problem. If you want to change the SSN system, you have to change the entire system of how the banks operate, how the insurance companies operate. And the cost, the social cost, is much greater than just changing the [INAUDIBLE] key itself. I think he's entirely coming from the point of view for the implementation of [INAUDIBLE] consideration of the hidden economic cost of such implementation.

AUDIENCE: But there is the Patriot Act, which says banks have to send your SSN to the government, which

basically means banks need to continue using SSNs. So in some sense, you're right. But also, government has to do something.

GARY GENSLER: So let's move on. I don't think it's just here in the US. What's happened is the attributes of our identity, or our credentials of identity-- whether it's for tax systems, for banking systems-- in the last 30-odd years, as we've digitized, and also post 9/11 and terrorists, we started to use all of these things for anti-money laundering, know your customer.

So the financial system, the tax system, and our identity systems have now all been kind of linked up, and not always with the best intent. I mean, maybe they were the good intentions. But with not with the best results.

And it's part of why I thought, if we were going to cover blockchain technology in the financial sector, identification systems were really important as well. Because it's so linked up with banking and finance. And that wouldn't have been the case before the digital revolution and the internet and so forth.

I think this is the last cover slide. But this is self-sovereign identity platforms. Basically right now, if we want to keep our identity, if we want to keep our identity and only give it up, a platform could create and enforce rules governing the workflow. This is a little thing called bitsonblocks.net.

But pretty much most of the startups are using an architecture around this. This happens to be Bits on Block's view of it. But it's basically, I'm going to keep my attributes of identity. And I choose when I can give it up and when it's used, authorities, and issuers.

So I think I have hopefully-- oh, yes. MIT. That's where I wanted to go. So what did you all think? You read the little article about your own-- you going to get in it? James, you going to get your blockchain blockchain diploma?

AUDIENCE: Yep. [INAUDIBLE] I have some experience. I started trying to get hold of my diploma back in 2012 for a degree that I got in 2007. My university was declared independent from the University of London. There was a whole record messup. I'm trying to get a copy of my transcript.

GARY GENSLER: And you can't get it?

AUDIENCE: I had to go through many different people, say, oh, can I get it? And they'd say, oh, we have to

contact the old university because we were part of them.

GARY GENSLER: I'm going to shorten your-- so how many of you are going to get a blockchain backed diploma when you graduate MIT? All right. A quarter of you. And those that aren't, who didn't raise their hand?

AUDIENCE: [INAUDIBLE]

GARY GENSLER: Oh, you will. Wait a minute. I didn't see any hands go up over here. So you're not? I don't care really.

AUDIENCE: [INAUDIBLE]

GARY GENSLER: Oh, you did? I want somebody who didn't raise their hand. Why aren't you going to get it?

AUDIENCE: For me, it's just pure lack of information about the process. How to get it, what I have to do. So I don't know yet if I will or not.

GARY GENSLER: So you're just saying there is an information curve you have to learn about it. The people that raised their hands and said you'd get it, how many of you will also get a paper diploma? You want something for the wall or for the significant other or for the children or the parents. Right? Right?

There's still something about that. I don't even know where my college diploma is, by the way. But you still want that piece of paper. Was there anybody who was only going to get a blockchain diploma? And any of you that go to a different university, do you wish your university had a blockchain diploma? Nobody's going to speak up. Maybe not.

All right. So it's a novelty. It's MIT. We're innovative. We have it.

I hope you all do come next Tuesday. It will be our last time together. I'm going to try to wrap up with some ground truth as to what I think the whole topic and this subject is. This was meant to be about the business of blockchain technology, getting through at least enough of the details, knowing those details, and then saying, well, how does that apply to the markets. Hopefully, you feel that you've gotten, and Tuesday we'll summarize it all, some critical reasoning skills that you can sort through the hype and the reality.

And those of you that came in maximalist, you're probably more in the middle. Some of you that were minimalist maybe came-- well, maybe you're still, but you came a little-- because I

thought that was the right place to teach. And you've all given me tremendous feedback. And I've learned a lot from you all. But let's keep it going. See you on Tuesday.