GARY GENSLER: Thank you again for all being here. We're going to talk a little bit about the challenges of blockchain technology. I'm apologizing in advance. I'm supposed to be, like, across campus for a 4 o'clock meeting. So I won't have much time right at the end to do the little wrap with students coming up.

I will note also that if you want to come see me I'm open to it. Next week's a great week, by the way, because I'm here all four or five days. But I don't have set office hours. Just email me.

Copy Dylan, who's the new course administrator. There was a swap out from Ryan. Or copy Talida or Sabrina or something. But just shoot me an email, and then I'll set something up with you if you want to follow up either on your projects, or it's a question about anything around blockchain.

I also want to thank-- we don't usually have people here with jackets on. But we have six or eight veterans who have served our country, and I thank you for your service.

[APPLAUSE]

They're here to observe us. I don't know whether we'll scare them away or not. But thank you for joining us.

So today's topics are going to be around-- of course, we're going to go through the readings a little bit. We don't have Larry Lessig, and it's a little bit more relaxed. So I might be doing some cold calling if that's all right.

I'm going to go back a little bit to the technical features in a quick wrap-- in two slides or three slides. But I just want to do that as the setup again. And, of course, because you all love hash functions so much, it's just a way to bring it back to some of the technical features to set up, really, what are some of the issues.

We have-- I think it's lecture 11 and 12, where it's just what I call act two as the economics. But I want to set up a little bit about the economics. You saw that in the reading-- the 21st Geneva report that Simon Johnson and Neha Narula and Mike Casey and Jonah and I wrote. So now you all-- I only assigned his seven pages out of it. So I hope that you read the seven pages.

But some of the costs and trade-offs, the challenges of blockchain technology that are very real. I'll give you my own perspective on where I think this will sort out over the next 3 to 10 years. So I'll do some predictions. Vitalik Buterin has also talked about a trilemma, and I want to chat about that. And that was one of the readings, if I recall.

He's such a leader in this community that when he writes and says something like this, it was relevant, I think, that everybody's understand what Vitalik Buterin's kind of "trilemma" is, even though that some people think he's mistaken.

Some possible solutions to this-- we have, who's attending today, Madars who is actually one of the developers on some of the solutions around zero-knowledge proofs. And he might get called on. He works over at the Digital Currency Initiative. I hope you're ready. And why I think governance is the most challenging piece.

So with that, the readings-- I have a list of everybody that hasn't spoken yet.

[LAUGHTER]

So the goal is to speak. That's what class participation is. I'm going to be lighthearted about it. I-- it's not that long ago I was a student, really. I remember all this, you know. You want to get your name off this list. I just want to say kind of encouraging.

So should I do it alphabetical from the list as to who wants to tell me? No. No. You look like you're ducking your head. What's your name?

[LAUGHTER]

AUDIENCE: Wendy

GARY GENSLER: What's that?

AUDIENCE: Wendy. Wendy.

GARY GENSLER: Wendy. Wendy. What did you take from the seven pages of the Geneva report? Did you read-

- did you do the readings? So what did you take from the great work of Simon Johnson-- and I helped him out, you know?

AUDIENCE: [INAUDIBLE]

GARY GENSLER: Anything about the business challenges of blockchain from the readings.

AUDIENCE: It takes a long time to do the [INAUDIBLE].

GARY GENSLER: So one challenge is time-- latency. It takes a long time to do. Wendy raises. Yes. If you could say your first name?

AUDIENCE: Catalina.

GARY GENSLER: Catalina. It really helps Sabrina out-- get you off the list. So it's self-motivation to say your name. So Catalina.

AUDIENCE: There is also a problem with performance and scalability.

GARY GENSLER: Right. So it's sort of related. They're not alone-- but performance, scalability, the time it takes to do a transaction. Other challenges? Yes?

AUDIENCE: There are issues

GARY GENSLER: First name?

AUDIENCE: Samir. There are issues with micro payments and how they're [INAUDIBLE] inconsistently confirmed.

GARY GENSLER: So how to do micro payments. You want to tease that out? Why is there a problem with micro payments?

AUDIENCE: I can't remember the exact details, but it was around just the fact that-- because they're so small, they were just essentially inconsistently [INAUDIBLE].

GARY GENSLER: All right. So how to do micro payments. And the small micro payments-- partly because they're so small-- may be relative to the fees and the cost of the network. Alexis?

AUDIENCE: Yeah, I just wanted to add, like on this point because basically the minors will try to add to the blockchain first the transaction with the highest fees. So a small transaction could take [INAUDIBLE].

GARY GENSLER: So there's economic incentives that are involved here. We're now moving a little bit away from all that stuff-- the broccoli that I said that we were all going to be eating about hash functions and so forth. Akira.

AUDIENCE: Yeah. Other challenges-- the privacy and security. [INAUDIBLE] those concerns identity of [INAUDIBLE]. And [INAUDIBLE] concern privacy protection of customers.

GARY GENSLER: OK. So Akira just raised a bunch of points about privacy and security-- about the individuals and the regulators. Does anybody want to tease that out a little bit more?

AUDIENCE: Well, the bank has more of an incentive to keep things on the privacy side, whereas regulators obviously will have pried into the details.

GARY GENSLER: OK. So you have that natural public policy tension that doesn't only exist around blockchain. Jihee?

AUDIENCE: I could hear anything back here. So if people can speak up a little bit.

GARY GENSLER: OK. Do you want to say it again?

AUDIENCE: So inherently, the regulators want to look into the details of the transaction, whereas banks have a high incentive to keep [INAUDIBLE] privacy side.

GARY GENSLER: So on the one side, there's a commercial interest to keep things private. On the other side, the official sector might want to peer in. And then interestingly, on top of it-- layered on it-- the official sector also wants privacy for everybody other than the official sector.

So like in Europe, there's a new requirement that wasn't in the readings. Don't worry. But is anybody familiar with the directive-- the privacy directive called GDPR? I don't remember your name. I'm sorry.

AUDIENCE: Erin.

GARY GENSLER: Erin. You want to tell the class a little bit about GDPR, or if you--

AUDIENCE: I'm not certain there. I just know that it's a big deal right now with going after [INAUDIBLE]

GARY GENSLER: Stephanie.

AUDIENCE: Yeah. So my understanding is that, especially when it comes to advertising to consumers, they have-- consumers in the EU have to really check certain boxes to agree to be advertised to as opposed to just automatically getting that.

GARY GENSLER: Right. So Joe Quinn?

AUDIENCE: It's a private deal. You have also the right to opt out of being tracked-- everything you do.

GARY GENSLER: Michael? This is Michael?

AUDIENCE: I was going to say we worked on this-- company I worked on at the summer. We had to put purging mechanisms into our databases.

GARY GENSLER: All right. So it's a remarkable new law. Europe is, in a sense-- if you wish to say-- either more privacy protection, or ahead of the US. You know, and each jurisdiction has their own cultural and political norms. But Europe as a whole has moved further, in a sense.

You have a right to be forgotten. You have a right to access the information as well. And so how to be forgotten in the context of an immutable blockchain is an interesting just technical set of issues. Yes?

AUDIENCE: There was a question I was going to ask-- Kyle is my name.

GARY GENSLER: What's your first name?

AUDIENCE: Kyle.

GARY GENSLER: Kyle. OK.

AUDIENCE: I worked for a company this summer that processes transactions. And it was our understanding-- speaking with lawyers in Europe-- that under GDPR, you're allowed to request your transactions because the transactions count as personal information. You're allowed to request your transactions to be erased from the ledger, which obviously opens the door to all kinds of fraudulent behaviors. I'm just curious to know if you've heard of any sort of resolution to that.

GARY GENSLER: I haven't. I was speaking at a conference earlier today here at MIT with a bunch of member companies to the Computer Science and AI lab. And one of the participants said they thought they had a technical set of solutions to it. So we're going to talk more about the privacy issues

and GDPR in the public policy session next week. So I'll try-- Kyle, remind me. And I will try to get more up to speed on that. Kelly.

AUDIENCE: I found the-- specifically in the GDPR chapter, there was something mentioned about what makes blockchain uniquely qualified to solve a lot of these solutions. And I found that it had coincided with what Professor Lessig said last class about-- there are significant trade offs that often come down to the cost of trust. But it still begs the question-- with so many technical challenges, why is it still such a-- something that's so sought after? So I'm hoping that we can clear that up a little.

GARY GENSLER: We'll give it a shot. Other thoughts or questions from the readings?

AUDIENCE: I [INAUDIBLE] third year with you about the layer 2.

GARY GENSLER: About the layer 2. Yes.

AUDIENCE: The layer 2. Yeah. And [INAUDIBLE] that is that it's OK about having a second layer to provide the efficiency and the high performance. But it's writing it off line. Yeah?

So we are starting to trust in a second layer that runs off line and then goes and put inside the blockchain. How feasible-- how can we trust?

GARY GENSLER: So the question is about possible solutions to address performance and scalability. And I have a few slides on that. But in essence, if the principal protocol-- the Bitcoin protocol, or the Ethereum protocol, or maybe tomorrow it'll be EOS or some other protocol-- has some performance issues, could some activity be moved to another channel?

That channel could be called a layer 2 in the Lightning network, which there was a reading about. That could be with a little bit different technology cord side chains or sharding, which I think was an optional-- yeah. I did that optionally. I didn't force you.

So there's a number of alternative channels. And though the technologies are, to technologists, importantly different-- sharding, and side chains, and layer 2-- for this purpose, for a moment, let me blur over the differences. The question that Leandro asks is, well, is that meaning that we have to trust?

I would contend we already have to trust the protocol that the Bitcoin core developers have written. It's open GitHub. It's open code. But very few people are actually going to investigate it

enough to be assured there's not a bug or an error.

But I agree with you that the core-- the Bitcoin core or the Ethereum core has been living in-- if I could call it-- the technological and commercial swamp. It's been attacked by so many viruses and bugs, you have some reason to trust it. But you should never be 100% sure.

The side chains are less tested. But I do agree with you. You have some trust, unless I misunderstand the question. I thought it was a trust in the underlying code.

AUDIENCE: My main point is working with secondary that's offline. You are not really transacting in the block chain. Yeah. It's off chain. Yeah. [INAUDIBLE]

GARY GENSLER: So the question is, if you're off chain, should you be more worried? I was addressing just a narrow part about the code. You're saying, should you be worried because it doesn't have the same validation models? So can I hold that question until we get to the slides? Because I think you do actually have some pretty good validation, but I think you're right that it's a valid question-- is the validation in these off chains still work? There was a question back here.

AUDIENCE: I was just sort of going to respond to the issue of sort of trusting these offline mechanisms. It's not in the same vein, but 90% of-- according to this-- daily trading volumes occurs in these crypto exchanges. So that's also sort of happening off the chain.

So I think that in this community of people who are currently participating, there is no reason that we're not going to trust third-party vendors.

GARY GENSLER: So you're raising the point-- and it's a sort of an irony of the whole ecosystem-- that the majority-- and, in some cryptocurrencies, over 90%-- of the actual daily transactions are happening in very centralized ways-- on exchanges, particularly the centralized crypto exchanges, where-- I can't remember. But it was about half of you have owned Bitcoin at some point in time.

But can I ask how many of you have actually operated a full node? So there's the two technologists at the middle table, and Hugo, who is also, if I remember right, an engineering PhD student? OK. So we have our 3 PhD students who have operate full nodes. Honors to you all.

But for most of you-- and it was half the class have owned some Bitcoin-- you've trusted some other authority to hold your private keys. I'm not saying you're wrong or right, but it's an

interesting and important point about this ecosystem.

So let me, unless there's other points, just go through some of how I thought about these things and laid it out. And I-- of course, the study questions we've been talking about. So I'll come back. But we will talk a little bit about hard forks. And we-- I didn't hear anybody talk about interoperability. So we'll come back to that as well. We've talked more about performance and privacy issues.

Just back to the technical features-- it's just repetition. Sorry. But I do think it's worthwhile.

There is, of course, the cryptography and timestamp logs-- so the bedrock of this technology that we did three or four lectures ago. You will find that in permissioned systems. You will find it in permissionless systems. That is a bedrock.

You will find in Ethereum Bitcoin and 1,600 others. There will be some shifts around-- the hash functions might be a little different. But that's kind of a bedrock of this technology.

The Network Consensus is not necessarily always the same, as we talked about. Sometimes, it's proof of work. Sometimes, it's proof of stake. Or in the permissioned systems, the consensus is really, are you amongst the club? And then there's kind of some form of a club deal.

If you're the Australian Stock Exchange, the only member of the club is the Australian Stock Exchange. But in other permissioned systems, it's 20 banks or 15 banks that are sharing that some delegated randomized authority to say, what's the next amendment to the--

And the transactions code and ledgers shifts largely dependent upon whether it's a transaction ledger or an account ledger. So transaction ledgers have to have some way to record transactions. Account ledgers have to have some way to record the change in accounts, which Ether calls state transitions.

But either you have to record a transaction, or you have to record a change in the state or a change in the account. An account would say, yeah, it would be like the income statement versus the balance sheet. But you kind of need to record that.

And basically, all of these technologies, as I understand it, have some way to keep those ledgers, though there's multiple ways to do it. And as we talked about last week, some have one Merkle tree, and some have four or five Merkle trees. And so forth. But it's embedded in

this, and they could have different scripting.

Questions? Just-- that's like the thumbnail just to remind you about the technology. It's the T in MIT.

AUDIENCE: Just a quick [INAUDIBLE] question on ledgers. So for a transaction versus account in an account-based ledger, does it say-- like, if you spend $5, does it say who you're spending that $5 to? Or does it just say, your account went down $5, and somebody's else went up $5, but it doesn't matter where it came from?

GARY GENSLER: So I'm going to take, as I understand Ether and Madars. You'll bail me out.

But you put a state transition-- instead of a transaction input, it's a state transition input. And that state transition input does have one account going down, another account going up.

AUDIENCE: So if you investigate that, you can see where it came from.

GARY GENSLER: You can see both sides of it, as I understand. And there is a receipt ledger. There's actually a receipt Merkle tree that then keeps this state transition happened. Did I did I roughly get that right, Madars?

AUDIENCE: [INAUDIBLE]

GARY GENSLER: Oh, wow. All right. Madars actually does this for a living. I mean, he's the one of the founding people of Zcash and a bunch of other wonderful things.

I'm not going to go through each of the details, but there was about 15 or 20 details in these slides about the differences between Bitcoin and Ether. And I just use it to remind-- because it's saying, OK, why did the professor-- why did the-- why did Gary put it up there? This professor Lessig-- that was nice for Larry. But for me, you don't need--

But in essence, the big difference is account-based versus transaction-based. The kind of big difference is Ether does seem to go faster, but it doesn't have a lot of throughput. They still both use proof of work. Even though Ether says they're going to move to proof of state, they're not there yet. When they get there, we'll all know together.

The economics are a bit different, of course, as well. But all of these details are part of the reason why there's problems. And so you read in the Geneva report a little bit about a professor-- an economist from the 1930s. Does anybody want to take a crack at it? Or should I

just do my slides?

Here we go.

AUDIENCE: It was [INAUDIBLE]

GARY GENSLER: Yes.

AUDIENCE: He had the fact that everything you should be analyzed on the cost-benefit analysis so that if one wants to use the blockchain decentralized network, you should take into account all the benefits in terms of various costs of trust-- enhancing security, but also the cost of switching to a decentralized system.

GARY GENSLER: Coase is an economist from the 1930s who wrote extensively about the cost and empirically about the corporation. Kelly?

AUDIENCE: Yeah. Basically trying to understand why transactions would aggregate into a firm. Why move all your activity into one?

GARY GENSLER: Right. So in a much earlier time-- way pre-Bitcoin, but a different-- why does economic activity cluster into a firm, rather than-- if it was truly market-based, I might just be selling my services. In essence, he was asking the question, why don't we have a fully gig economy in the 1930s, where everybody's free labor, and even capital and labor meets individually, and we collect up together? That was kind of the body of his question that he was-- so centralization versus decentralization 80 years ago studied by a great economist.

So just thinking about it here a little bit, I think that when you go from decentralization to centralization, you tend-- on the centralized side, you get capture. You get economic rents, and you do have a single point of failure. In some sense, the resiliency of the system, whether it's in finance, where you worry about systemic risk-- one clearinghouse, one central bank, one government. If it's knocked out, it's so relevant to the economy at large. It brings it down.

Or if it's one database-- you have a single point, in essence, of failure. Economic rents is an ability to collect excess profits. I assure you everybody in this class wants to collect economic rents.

We start out as venture capitalists and entrepreneurs, but we have a motivation and an incentive to be monopolists. But we don't want to do it illegal, of course. I mean, we just want

to get there by dominating the market. I'm sorry. Was there a question here? You're just-- you're shaking your head, and I didn't know.

But on the other side, there's the benefits. The y-scale is not written on here. The y-scale is how however you want to think of it, but I think of it as kind of costs. So the y-scale-- up the y-scale is greater costs.

Decentralization-- the big costs that come there is coordination. You have a lot of collective action issues. If the 100 or so people in this room were trying to do something together, you would have to figure out how to do it collectively in coordination. And that's true of every blockchain that you can think about.

Governance relates to coordination and collective action issues. And then security and scalability-- these two lines are not in any of the readings, but they try to capture what-- and depending upon the slope of the two lines, you might say that a market might tend towards more centralization. In theory, if I change the slope, it would be further to the decentralized side. Right?

If the cost of decentralization is a lower slope, and the cost of centralization is higher, we will tend more towards decentralization. So it's just a way to visualize-- here are the costs of centralization, which are basically capture rents and single point of failure, not that there aren't other costs of centralization. Here are the costs of decentralization.

I think in each one of the applications, when you're thinking of use cases, it's worthy-- this is kind of a core thing. Will this application lend itself to a low slope decentralization curve and a high slope centralization curve? Are there a lot of economic rents? Are there real problems with single points of failure or capture? And if it's a low slope decentralization curve, meaning there's not much cost to the governance of coordination and scalability issues, then you're going to be more towards decentralization.

This isn't any reading or book. It's just a shot at trying to visualize it. Sean? Any question?

AUDIENCE: [INAUDIBLE] One question I have-- it's slightly irrelevant from this area-- is that why are all the privacy coins are off the hard fork? What-- a lot of them are off the hard fork for the Bitcoin as a [INAUDIBLE].

GARY GENSLER: So Sean's question is why are the privacy coins forked-- not all of them, but many of them are forked off Bitcoin or one of the major coins. Madars, you want to say-- did you-- you have one

privacy coin.

AUDIENCE: So Bitcoin has a very robust and well-established code base. So there is a lot of high-quality code.

GARY GENSLER: Could you speak up?

AUDIENCE: Bitcoin has a lot of high-quality code so you can build up on it. So it's natural to add privacy on top of Bitcoin in your fork rather than write it from scratch.

GARY GENSLER: What Madars is answering is there's something that's freely available-- the Bitcoin Core code. It's actually under a copyright license here at MIT, which makes it free. That was Satoshi Nakamoto's decision. It wasn't that-- well, maybe Nakamoto does work here.

[LAUGHTER]

It's a clue. But it's been developed, and it's knocked around, as I call it, in the proverbial swamp-- I mean, with all these attack viruses and so forth. And so Madars is saying, build off of that and basically get that code for free. And then fork. Is that--

So the challenges-- we talked about it-- of performance, scalability, efficiency, privacy, security. What there was less talk about was interoperability, governance and collective action. And I'm going to dig into those two more because it feels like that's worthwhile.

I also believe that the first bucket-- performance and privacy bucket-- are more susceptible to fixes. Though that might take three or five or even eight or 10 years to happen, I think they're more susceptible to the bright men and women that are in these fields addressing themselves to the computer science and cryptography of the space, whereas governance and collective action might be solvable. But I think it's sort of inherent in the human element and the commercial arrangements that governance and collective action are the harder of these four buckets. That's just one person's read of it. But we'll go through some of the reasons as well why I kind of get to that view.

There's also commercial use case challenges. We're not going to dig into that much here. That's mostly the second half of the semester. But I just wanted to mention that's a real thing that a lot of folks are saying, well, would-- I have to make sure that this is the best commercial application, and so forth. And can I make money, I mean, ultimately on it?

And then we are, next week, going to talk about the public policy issues and challenges. And they all kind of intersect in a way, as well.

So Vitalik Buterin-- I think there was a *Medium* post I had you all read. Bo, do you want to tell us a little bit about what you think? Is Vitalik not only a brilliant computer scientist, but does he get the economics of this right? Or you think he's off?

You can be on-- there's no right answer. I know people that feel both ends of the spectrum about his trilemma. So I'm setting you up that--

AUDIENCE: Geneva [INAUDIBLE] it first. It seems like it makes sense. But his-- he's basically saying choose two. You can't have all three.

GARY GENSLER: Right. There's an old saying about-- how many of you have ever hired a contractor to fix something in your kitchen or renovate something? I mean, I have. I'm a little older, right? You know the old saw that it's good, quick, cheap, but you can't get all three? You can only get two out of three. That's sort of the contractor dilemma.

But what do you think? Do you think he's right? Or do you think you could maybe, over time, get all three-- good, cheap, quick, scalable, decentralized, and secure?

AUDIENCE: My very unsophisticated knowledge of the technicalities behind this-- I think he's right.

GARY GENSLER: You think he's right. Who wants to take the other side just to have some fun and some debate? Sure. Yeah. Go out at it, Leonardo.

AUDIENCE: So--

GARY GENSLER: There. You got it. We got the name.

[LAUGHTER]

AUDIENCE: I think one of the texts we're talking about-- the time that systems have had to develop. So the image, for example, Visa has had 60 years to develop a system that works. Some of those currencies have three, four, five, ten years. So they will, I think, even put a number. His personal opinion of [INAUDIBLE] was that less than 5% that will not overcome the hurdle.

I don't know if that is right or wrong, but I think the fact that it's so recent-- I think the jury's still out.

GARY GENSLER: All right. So Leonardo's point is it's recent. This is a new technology. Yes, maybe Vitalik is right that only 5%-- maybe only 1% will succeed. But to say that no one will deal with these three points in this simultaneous satisfactory way-- and ultimately, it has to be satisfactory in a commercial way-- taking the risk and trade offs. So Leonardo takes the other side.

Anybody want to say why Leonardo-- Hugo, were you-- which side are you taking? Leonardo's side, or Vitalik's side?

AUDIENCE: Somewhere in the middle.

GARY GENSLER: OK.

AUDIENCE: So I think that there is a trade off. But I agree that it might take time to improve all three simultaneously.

I mean, one thing that happened just this last week in Bitcoin was there was a vulnerability discovered. And as somebody who doesn't know how to check the code base, really-- I'm not a computer science person, so I've never checked for bugs or anything like that. I don't know how to do that.

I kind of just take the software as it stands and download it and install it. And when they say I need to update my software because there's a bug, I'll update the software because there's a bug. And that kind of feels like more of a centralized system, but you're getting that security. But then the decentralization comes from the fact that the network is still spread out over so many nodes.

So there are trade offs that I think you can kind of build on one and then climb another cliff and kind of build on each, but not the same time.

GARY GENSLER: So Hugo is somewhere in the middle. I'm probably an optimist enough on the human condition and that the technologists will solve more than Vitalik. So I'm not saying I'm all the way where Leonardo-- wherever yeah-- there would be. But I'm probably closer to Leonardo than to Vitalik. But that's just my point of view.

I also find it interesting, if it's all right if I say-- Hugo's an engineering doctoral student here. And yet, he's not checking the code. Not any-- right? Because-- right.

AUDIENCE: [INAUDIBLE]

GARY GENSLER: So there's a trust issue that-- in the marketplace, the trust of the code. We all also trust Facebook and Dropbox and, broadly speaking, the internet as well. Priya?

AUDIENCE: I was going to say that there are several examples throughout the evolution of human interaction where these three things have been sorted. So it might not be that any-- in some systems, at any one time, all these three nodes are working, right? Like for our current payment systems, there are moments of vulnerability. Yes, but then you catch it sooner or later. So I feel like it's maybe not-- it's about having it all perfect right now versus, will you get to a point where all three are mostly in place and working.

GARY GENSLER: And I think-- I like how Priya said working enough, right? It doesn't have to be scalable to the place where it's millions of transactions a second. But maybe it needs to be faster than seven or 10 transactions a second, or Ethereum 20 transactions a second.

We had-- I should also remind everybody Tuesday nights we have dinner. Simon Johnson treats every Tuesday night. It's not required to come, but it's 5:30 to 7:00 that we have an outside speaker around the blockchain space, and you're welcome to come. Michelle is here, who-- Michelle Fiorenza.

AUDIENCE: [INAUDIBLE] mailing list. So please-- I'll put my name on the board later.

GARY GENSLER: So Michelle will put her name on the board-- anybody that wants to come. But this past week, we had somebody speaking about the scalability issues. And when his company did a $25 million initial coin offering, the day of the offering, which only had 40,000 to 50,000 purchasers-- so 40,000 or 50,000 purchasers on that day-- that means a smart contract had to be triggered numerous times that day. Took over a third of the entire Ethereum network on that day.

And it's sluggish. And just to close and settle on its initial coin offering, it was saying, jeez. That's not the scalability we want. So we know that's where we are today.

Visa runs around 20,000 to 30,000 transactions a second. DTCC, which settles all the stock and equity trades here in the US, has to be available to transact at least 100,000 a second. Most seconds, it's 5,000, or 10,000. Or some seconds, it's 30,000. But the Securities and Exchange Commission says, no. You have to be rated for four times your average, roughly. So this gives you a sense of the scalability issues, just in the current environment.

If one layer is the Internet of Things on top of it-- there's somewhere that I've heard different estimates of 8 to 10 billion devices currently connected to the internet. And that's likely to grow as more refrigerators, and street lights, and traffic lights are tied into the internet in the next five or 10 years to 50 to 100 billion devices tied to the internet.

If they start communicating to each other, will it be a blockchain for Internet of Things? Can't do it at these types of scaling numbers. Or can you do it in some alternative method?

Proof of work is also has a bunch of energy consumption. We didn't have that a lot in the writing. We chose not to put a bunch of that in the Geneva report.

One estimate is that it's 200 million kilowatt hours per day. That's equivalent to about 7 million US homes, on average, just to give you a rough digicomonist estimate. That's 1/3 of 1% of all the world's electricity just scale it if you-- now you can have a nice dinner party conversation point.

It's the electricity of the country of Austria. Is anybody Austrian? No. I just was-- you know.

So that's one set of trade offs of proof of work as well. But it also costs a lot of money to run the banking system. So I think that when somebody says, well, it's terrible. It's challenging, all this electric costs. Yes, we always want to lower costs. But the US financial system is 7.5% percent of our economy and costs $1.5 trillion.

So the payment system around the globe costs a 0.5% to 1% of the global economy, which is more than 1/3 of 1% of the world electricity costs. So I'm just putting it in-- it's back to those questions of which costs of trust, which costs-- I'm neither a maximalist or a minimalist, as you recall.

So what are some of the alternatives? We're not going to dig into each of these-- side chains, sharding, layer 2, payment channels. Anybody want to take a crack? They're not all identical. It's-- Madars and I had a conversation earlier today and said I couldn't even get my head around because I get confused. But does anybody want to give the basic-- we were talking about it earlier-- the basic tenet because you had a reading about the Lightning network as to what's the economic thing and technical thing that's being attempted in all four of these types of thing?

James, was that a hand up? You're going to give it a shot? Give it a shot.

AUDIENCE: Most of these are on the chain-- sorry. Most of these are off the chain, but some is on the chain. And the idea is you transact off the chain that balances are traded, and the net of the results goes onto the chain. So you try and speed up by processing off the chain, where you have thousands and millions of transactions. And it's only the net amount that goes in the chain that is [INAUDIBLE]

GARY GENSLER: So James has summarized it as, it's like saying, there's this chain-- this channel, if you wish, that the water is running in, or the digital money is running in, that only has a certain speed. It can only take a certain amount of performance. Why not take a lot of activity and put it in a side channel, which is called a payment channel, actually-- but a side chain, or a payment channel, or a layer 2, all with slightly different technical features. And maybe do millions of things off here, and only put some here.

It is not new to blockchain and Bitcoin. We already have that in the world of finance for decades, in some way or another, where some activity can't go to a central settlement system. And recalling ledgers-- the central bank, whether it's the US central bank or any central bank, could have been set up that all of our deposit accounts were directly with the central bank.

And in a sense, the side chains in finance right now are 9,000 commercial banks. 9000 commercial banks are dealing with our money flows and then sort of net settling to the central banks ledger in what's called digital reserves. And in fact, even the banking system-- the 9,000 banks in the US-- have their side chains-- Visa, MasterCard, First Data, all the money processing. So there's already a layering. I look at layer 2 and side chains as kind of taking a similar economic approach and technical approach that's already been around, but in a new way.

I grabbed a chart from 2015. The details don't matter, but this was-- I did it because it was three years old. This was one person's truth coin. One person's view is what side chains-- basically what James says. Lots of activity over here, and only a few things go over to the main chain. The visual is what I wanted to get across. It was just that it's kind of-- think of it as loads of activity over here, and then we only settle at some times to the main chain.

Another visualization of a different is the Lightning network. Again, a lot of activity, then settle to the main chain. Questions?

AUDIENCE: Zack. There seems to be a good trade off. A lot of people are proponents of making the block size bigger. A lot of people say the side chains. I have trouble understanding the trade offs

between those two. So why not just a bigger block? What's the problem there?

GARY GENSLER: So there's a series of trade offs of economics and technology. The more you put inside the-- let's call it the main chain-- the blue boxes at the bottom, to speak. The more you're putting in there, you weighed it down. There's more processing, of course, and more storage, and so forth.

But also, there's some-- there's too much latency. In Bitcoin, it's every 10 minutes, and you're not really sure until 3, 4, 5, some would say 6 blocks to an hour go by. So economically, if you want high frequency, low latency-- short time periods-- you might say, I can't get that on the main chain because the main chain wants to have low latency. Every 10 minutes is low latency now. Low latency to be more secure to keep the mining cost and the proof of work up. So there's some economic and technological both crosscurrents with that.

Unrelated to what I just said, but overlapping, there's also a bunch of miner and mining poll operator economics as to whether they want big blocks, or small blocks. And part of the split last year was-- it was sort of more motivated around local politics rather than global politics.

As the former Speaker of the House, Tip O'Neill, said, all politics is local. I think some of the debates last year was about local economics and the economics of miners But I don't know-- Madars do you-- Madars was probably in the middle of some of those debates. But would you have a different view?

There was a big debate last year as to whether the Bitcoin block should go bigger or stay the size. It was not the only reason, but it was part of the reason we have now Bitcoin Cash and Bitcoin because Bitcoin Cash has a bigger block size and a shorter 2.5 minute processing time.

AUDIENCE: There's something that can be said about--

GARY GENSLER: Speak up.

AUDIENCE: --mining centralization. The bigger blocks you have, only the miners that can handle the enormous blocks will be able to stay in business. And less decentralization means less security. So there is incentive, both from decentralization and security, to keep the blocks smaller, not bigger.

GARY GENSLER: So what Madars is saying is there's also a bit of economics around centralization. The bigger

the blocks, the fewer miners can handle it. The fewer miners, the more centralization, and thus, less secure, and maybe even economic rents because every centralized system can collect economic rents. Yes. Alin.

AUDIENCE: Another problem is that if you have bigger blocks, they take longer to propagate to the network. And in sort of unintuitive ways, if that happens, you get more accidental forks to the blockchain. And people hate accidental forks, especially minus accidental forks because they lose coins when their blocks aren't--

GARY GENSLER: So Aleen is saying a technical feature is bigger blocks are more likely to take time to propagate through the network. And thus, you might end up inadvertently having more chains that are discredited, in a sense, because there was work being done until the first one gets propagated.

AUDIENCE: My question is about keeping track of the transactions.

GARY GENSLER: That's right. So Leandro-- did I-- no?

AUDIENCE: Yeah, yeah. That's right.

GARY GENSLER: Leandro-- OK-- was asking, how do we validate the Lightning network? And how do we assure that that is-- though-- though--

AUDIENCE: Yeah because we're working with net [INAUDIBLE] in the chain, how do we really keep record of everything that's--

GARY GENSLER: OK. So the side chains are not recorded gross on the main chain. They're, in essence, recorded net. And in Lightning network-- I said I wasn't going to get into the differences, but here I go. The Lightning network is more a bilateral network.

It can take on the feeling of multilateral because I could have a transaction with James. James could have a transaction with Kelly. And it feels like it's three of us, but it's bilateral James and Gary, bilateral James and Kelly, as I understand it.

And so those individual transactions, while they're recorded-- keep me going here-- recorded in the Lightning network, they're not on the main chain. We ultimately, then, net settle to the main chain. And we actually, in a sense, pre-fund or pre-- it's a form loosely of escrowing at the beginning.

So James and I might be messing with each other, but we're bilateral. And so we have another approach to the trust. In addition to the computer code, James and I might have other reasons to trust. Joe Quinn.

AUDIENCE: Sorry. What keeps me out of double spending-- once on the Lightning network, and another one on the blockchain main network at the same time?

GARY GENSLER: Because there's-- I want to be careful because I'm using the terms loosely. There's a form of prefunding. It's not that you actually fund onto the main chain, but there's a little bit of partitioning. Does that-- Madars? All right. I keep looking at Madars because he's actually coded this.

So that's what protects you, in essence, that James and I-- if I'm saying, well I'll send you a one bitcoin. And tomorrow, if the sun does come up tomorrow, you'll send me half, we're partitioning that one Bitcoin or his half Bitcoin until we then close out that-- it's written into the scripting code. And it's written almost like a smart contract-- but it's not called smart contracts-- to sort of partition, or you might loosely think of it as escrowing, even though technically it might be different.

But stop by, and we can-- and if not, some of our colleagues at the digital currency initiative like Taj Draga, who programmed the Lightning network. I mean, that's an MIT collaboration with others. And we don't promote it just because it's MIT. It's like one of the leading ways to do performance. It happens to be MIT.

So let me talk about other ways to do performance and move on. We already talked about alternative consensus protocols. You've seen this slide, I'm just bringing it back because it is a way to deal with scalability. It's a really critical, important ways. Proof of work is one of the issues about scalability.

And generally-- I'm summarizing. I'm simplifying, in a sense. But generally, all the alternatives have some way to randomize or delegate the node that will do the next block. It kind of all comes back-- how do you add another block?

And Stuart Haber in the 1990s, when he started with all this blockchain stuff and put it in the *New York Times,* had a central authority. And he set up that company Surety. And he put it in the New York Times.

And what Nakamoto consensus is, is he said, well, no. We're not going to have Haber and a central authority. It's going to be decentralized.

So these other consensus protocols generally have some randomized approach to delegate the selection of the next block. It's not always that way. But they may also have a mechanism to do a second thing-- a second touch.

Silvio Micali's algorand-- he's a professor over in the Computer Science and AI Lab and a Turing Award winner. He's got a company that has an interesting thing. It's like a jury selection. It's like picking somebody for the jury that's picking this short group of 12 nodes that might do something. And every block has that selection process. But then there's another broader group that then can check the work of the jury.

So often, there's kind of a second automated way, because trust isn't there, ensuring that there's a quick second check. Did they decide guilty or innocent correctly, so to speak. Again, I apologize if I'm a little oversimplifying Silvio's brilliant work.

So it could be proof of stake, proof of activity, proof of burn, as we talked about, proof of capacity. And as I mentioned last week, there's not large-scale uses, but DASH and NEO both have some form of this going on right now.

And Ethereum has a big project. I'm confusing their two projects. There's Plasma and there's Casper. Casper is their project to get to prove of stake, but they're not there.

Privacy and security. So I'm trying to remember who raised the contradictory tensions. The contradictory tensions is law enforcement and regulators want more transparency. Even though the FBI did, you know, sort of figure out some Russians were using Bitcoin to mess in our elections, they want some more transparency in financial institutions. Users and even some regulators want less transparency. So it's not-- it kind of goes both ways.

But these, I think, are also truly solvable. Well, for consumers, there's DASH and Monero and Zcash. And there's even mechanisms called mixing and tumbling, which I truthfully can't tell you the difference. But I can tell you regulators talk about mixers and tumblers and privacy coins.

When I go to some regulatory conferences-- because they sometimes invite me as a former-- that middle slide-- the privacy coins and the mixers and tumblers-- the finance ministries and the law enforcement stuff, that's where they kind of get worried.

Madars, you want to come up here and tell us anything about Zcash? Or you want to do it from there, as to what inspired you to do a privacy coin that a bunch of law enforcement folks don't like?

[LAUGHTER]

Oh, I don't mean-- I mean, but, you know.

AUDIENCE: Obviously.

GARY GENSLER: And it's legal. I mean, it's a coin. It's real.

AUDIENCE: So just like cash can be used for illicit purposes, also systems that provide strong privacy like Torque can be used for illicit purposes. So it's said privacy is a human right, and we shouldn't be giving up our financial independence just because I want to buy a coffee. I don't want to reveal all my other transactions. Well, I think that there are mechanisms how law enforcement can against our regulatory objectives, but privacy I think is fundamental right, so we should fight for it.

GARY GENSLER: And so when did you start working on the project?

AUDIENCE: I think it was 2014 when we started writing the paper.

GARY GENSLER: So you started with a paper.

AUDIENCE: [INAUDIBLE] like prototype, codebase, we put it open source. And then there were the companies that got formed to launch the project.

GARY GENSLER: And I think Zcash now is somewhere around a billion dollar market cap.

AUDIENCE: It fluctuates wildly.

GARY GENSLER: Fluctuates. So that's why you're here. It went down? No, no. You don't need to answer that. Sorry. Privacy. But in essence, what Madars is saying that he came to this-- what were you doing in 2014?

AUDIENCE: I was a grad student here at MIT. I was mostly working in zero knowledge groups.

GARY GENSLER: On zero knowledge groups.

AUDIENCE: It seemed to be like a natural application, like Bitcoin plus [INAUDIBLE] techniques. Maybe there's something there.

GARY GENSLER: So here, a talented graduate student at MIT with the collaboration of others said here's this cryptographic mechanism called zero knowledge proofs, which we'll chat about in 30 seconds. And here's something called Bitcoin. Why don't we bring them together, and we can promote in his own words some human rights? Just as you buy a cup of coffee and you don't have to say who you are, you could use this new Bitcoin enhanced zero knowledge proof, Zcash.

AUDIENCE: I have a question regarding how do you define illicit activity in a way [INAUDIBLE]. Living in a country that has capital control, and if I use, for instance, Monero or Zcash as a way to get the money out, does that count in these activities, or [INAUDIBLE]?

GARY GENSLER: So fortunately, I don't have to define illicit activity. But generally, societies come together through their reasonable mechanisms, whether they're democratic societies or not, but they come together through their legislative branches and their executive branches and their courts and define some things that are not allowed. But generally speaking, when I'm using the term in this class. I'm thinking about four or five buckets.

Most societies do not want to shrink their tax base. So they want economic activity be inside the tax envelope, rather than outside the tax envelope. And that's usually the words that finance ministers call that is a tax base, how much is outside versus inside. Secondly, most law enforcement and most societies do not want to have the money rails, the banking, and other ways you can move value to facilitate otherwise illegal activity.

So it's using money to facilitate otherwise illegal activity. So the otherwise illegal activity might be drug running. The otherwise illegal activity might be terrorism. It might be child slavery literally. So it's whatever the otherwise illegal activity is to use money, and that's generally called money laundering or other things.

So you're absolutely right. Another thing is that for some countries, less than a majority, but some countries have capital controls. They're trying to maintain the value of their Fiat currency relative to other Fiat currencies. And in an effort to maintain some either fixed or relationship, they have capital controls, and thus, in those countries, they might say illicit activity also is running around the capital controls.

But it's each country, each society. And Sean, you raise a good point as to what does it mean.

I mean it not to show any value. I'm saying there's a series of these things that each society comes together and says usually around the tax base, usually around trying to not use money to facilitate otherwise bad stuff and in some countries, the capital controls. I saw a hand here. Daniel, no. Was there-- and we're going to do more about illicit activity next week about guarding against illicit activity. Hope the correction got filmed, too.

So there's another set of security issues around private keys. And to most of us that have passwords, you know if you lose your password, they're usually in essence a back door that somehow the platform, whether it's Facebook or even at Bank of America, if you lose your password, There's a back door, and they can say, there is a way to validate with enough probability weighting that I'm Gary Gensler, and they'll give me a new password.

I mean, in some circumstances, it's a high bar, and there's some biometrics involved. But in most cases, it's a pretty low bar, and they'll give you another password if you can, like me, remember the answer to my high school girlfriend was or something. These questions, like I remember it's Irene, but then I've just given it up. I've just given it up. That's terrible. I have to change it.

But custodial private keys is a very real thing, and you've read about the hacking, and we'll read more about it when we get to crypto exchanges. It's a very dominant issue, not just for individuals, but for institutional actors. How does a hedge fund or more likely how does BlackRock or Fidelity, as an asset manager, secure custody in a way that works? And it's an asymmetric risk. It's a tricky risk.

For most of finance, they don't have custody any longer of the securities. When I started on Wall Street, they were still the cage. C-A-G-E. It was a physical cage where the remnants of paper stock certificates were still in the cage. I didn't start so long ago that it was before DTCC. Things were getting electric, you know, digital. But there was still a physical cage for some physical paper certificates.

If you lost the paper certificate, you could still go to the government or the company that issued it and back door and get a new paper certificate. It took time. It was hard. It was to authenticate it. But in this circumstance if you lose the private key, there's not the back door issuer to get the next one.

So it's a very interesting issue, not just a technological issue and a cybersecurity issue, but it's a whole set of financial custody issues, an asymmetric risk if you're a Goldman Sachs or

Fidelity, and you lost a key, or it got hacked, and it was billions of dollars. So it's just interesting-- I don't think it's unique to blockchain, but it's rather specific to blockchain and finance and how it overlaps.

So some of the solutions-- and I do think there are solutions here-- are some of the things that Madars and Neha Narula, who runs the Digital Currency Initiative, are working on. And they're working on using two cryptographic primitives we're not going to deeply go into. We did hash functions, and we did digital signatures. Those are algorithms, or they're called cryptographic primitives. Well, there's dozens of cryptographic primitives, math algorithms.

Well, the other two that are used a lot in this field are zero knowledge proofs and less often probably as Peterson commitments. And I put up there my words. I got Madars to help me write this one. But my words is zero knowledge proves let someone prove a statement is true without revealing the details of exactly why that statement is true. You might say, wait a minute, you can prove something's true.

It's sort of like if you walk into a bar and they need to know you're 21 to get a drink, let's make this tangible. What do you need to prove that you're 21? You need to prove that you were born before 1997, September 27. But you don't need a lot more details. And so there's some computer scientists here at MIT that actually did the foundational work on zero knowledge proofs 20 to 30 years ago, Silvio Micali and others, for which I think was part of why they won the Turing Award, amongst other work.

So zero knowledge proofs are very interesting cryptographic mathematical puzzle solving that Madars used for Zcash. Neha and Madars is using for something called ZK Ledger, which was an optional reading. My gut tells me there are ways that we can go forward that regulators and the official sector can get their transparency they want and the financial sector at the same time can get the privacy they want, that the two can actually coexist through the modern methods of technology.

Alexi, is that a hand up or just a waving-- no, all right. You want to add anything Madars since you're the co-author of this the ZK Ledger paper that was optional.

AUDIENCE: [INAUDIBLE] an influential [INAUDIBLE] called zero coin protocol developed at Johns Hopkins.

GARY GENSLER: So Johns Hopkins developed a middle coin--

AUDIENCE: Middle protocol called Zero Coin.

GARY GENSLER: Zero Coin.

AUDIENCE: Using Pedersen commitments and Zcash didn't use Pedersen commitments. There's a lot of very interesting history behind.

GARY GENSLER: And Pedersen commitments are yet another cryptographic primitive or algorithm, which interestingly, they're similar to hash functions, where you take a bunch of data, and you squish it together in a sense. You compress it and get a commitment. But you can actually add and subtract them. It's an interesting thing where you can commit to data like a hash, but you can also add and subtract commitments.

So it has some interesting features. If you're deeply interested, I will probably line up Sabrina to help you, or Madars might help because I'm at the edge. But what I'm saying from a business side is my hunch-- and this is that-- we're at the we're at the cutting edge here at MIT of some of the folks try to figure out how to do privacy and security at the same time. Questions on that? Because we're going to get to the tougher things.

Interoperability. Linking Blockchain applications to legacy databases or linking them to each other. So you might want to link Blockchain application-- if you're thinking about a payments protocol, how does that payments protocol and Blockchain world link to the fiat. Because ultimately, if you're doing, let's say, remittances, and you want to move money from here to Mexico, somebody wants Mexican peso, they might be starting in US dollars, how do you operate basically with three different systems in that case?

Your ingenious, innovative start-up, but the US dollar fiats system and the Mexican peso system. So that's a form of interoperability and the challenge around it, or Blockchain to Blockchain if we've got 1,600 of them, or even interoperability of the main chain and some of these layer two and side chains. That's an easier interoperability because it's kind of coded right in. But it's always-- and this is not a new thing.

Banking has had interoperability all the time. Take my example of the US to Mexico. To move US dollars and convert it to Mexican peso is in two entirely different banking systems and two entirely different ledger systems. So we have to have this question of interoperability even pre Blockchain. But it's just bringing it to this new technology.

It raises costs of trust in coordinating the transfer assets and information across chains, in

essence, or as we talk about, across ledgers. So it's an issue that it's been around. We just got to sort of see how we solve it here. One solution. It doesn't mean it's the right solution, it's the only solution, but one solution is to do through some decentralized mechanisms including side chains, or one of the favorites of the director of the Media Lab, Joey Ito, thanks maybe if we have layer 2, we should also have layer 0.

Underneath all of these coins, underneath Ethereum and Bitcoin, maybe there's a layer that we can technologically create. Nobody's done this yet, but Joey's a visionary. Joey had the first internet service provider in Japan at the age of 23 when he got $1,500 of computer equipment and put it in his bathroom. And that's how he started. Yes. Yes, his bathroom. It was the only real estate he had.

So which way does this go? You hadn't heard that about Joey? So it's a way to start a company. And I think far more work needs to be done. So it may be solvable. I'm not sure. And then consensus required for software updates. It's a tough one.

Open source software updates, which are not backward compatible. Like, can I update the software, but then you can't use it for the 500,000 blocks that are already out there in Bitcoin, or in some-- or the millions of blocks in the ether. So the problem often happens that the older versions won't validate all the new blocks. And if they won't validate all the new blocks, I'm simplifying again-- think of like Excel and you get that update on Excel or Word for Windows, and you can't open your old files.

I mean, it's a rough lay definition of what this issue is. And so it leads to something called hard forks. And this little visual on the right hand side is basically what happens is you can't validate all the old blocks, because the new software is kind of going beyond it. A hard fork would happen is if you took two megabyte blocks, if you made the block size bigger. The old software would not take that if I've got this right. That would be a hard fork.

And so that's an issue, and it's happened. The Ethereum network has Ethereum Classic and has Ethereum because of a hard fork that was encouraged by Vitalik Buterin, and the Bitcoin network has one from last year, where it was this debate about block sizes. So most software for decades has dealt with how do we update software, but they can push it to us. And we get it, and we hit a button and we get it, and after a while, we get annoyed and we don't update if you're like me.

But the consensus-- remember, this was a graph that we had. The consensus always supports the longest chain. If the consensus is to adopt this new technology, and only 80% or 90% adopt it, it's a question of whether the other 10% or 15% will keep maintaining the shorter chain. And in Bitcoin Cash, they have.

And so in essence, now you have two currencies. If, for some reason, it atrophied, and they stopped maintaining it, then the value, in a sense, in a commercial setting might go to zero. Was there a question? So broadly speaking, I think the toughest issue is about collective action and governance. How do you get a whole group of people to be moving in a similar direction?

Blockchain applications derive part of their value from participation of multiple parties on the network as well, that multiple people are involved. It's remarkable in hindsight that Satoshi Nakamoto, whomever he or she was, got this many people. There's nearly 100 people in this room studying this 10 years later. But somehow he solved a collective action issue because it was just software code back in 2009.

But it's still the example, how does Silvio Micali with a very clever Blockchain adaptation and Algorand, how does he get people to start using it? And until he starts to get people to use it, where's the value? Or if you have an application that's to be file sharing or for medical records, there is a medical records project here at MIT, but how do you start to get people to use it?

And these are solved every day in the internet space, but Blockchain has a little bit greater wrinkle. So there's a chicken and egg issue. Priya.

AUDIENCE: This is like heresy in this room, but is it because it isn't a real thing? Versus like a medical records, it's really a real thing. Because I wonder about that a lot. Does it proliferate because there's essentially not much effort, real cost to it--

GARY GENSLER: Priya's question is is there some perception-- can I use that word? There's some perception it's not a real thing, so it might not propagate, and there might not be as much consumer adoption. That may well be one of the commercial challenges. Eilon, did you have [INAUDIBLE]?

AUDIENCE: Yeah, I think the adoption of Bitcoin was because people were interested in the innovative solution. And then Ethereum and with Algorand leaving in a few months, it will happen in other blockchains, are basically pouring money into the ecosystem, giving money to developers to

develop solutions, because they are betting on the success of that network.

GARY GENSLER: Right. But for every one of you as you're thinking about your final projects, this collective action issue has multiple features. One, to me, is the governance of the Blockchain software updates, which we said is a little bit about hard forks and so forth and how do you have consensus and how centralized to the governance stay, which we'll come back to when we talk about the Securities and Exchange Commission and whether it's a token that's regulated as a security.

So there's that part of governance. But then there's the collective action issue that if you have a payments or medical records or trade finance, how do you get folks to adopt. And in the banking sector, the banks are the big sort of elephants in the room, the big dominant incumbents, how do you get them to adopt, or are you somehow competing away their profits and not having them adopt, which is more a commercial business issue about collective action.

So the financial sector, as we've talked about, favors permissioned blockchains that don't have as many-- they have some collective action issues, but they don't have as many collective action issues. They have far fewer scalability and performance issues, because they say, I'm not using proof of work. It might be 15, 20, or even 75 or 100 nodes, but they think that way, they can secure their privacy and security.

Now, Madars and Neha's paper on ZK Ledger might be a solution. And some of those banks might start using that. But I'm talking about 2018. I'm not talking about 2020 or 2025. Right now, they're favoring permissioned closed loop systems, rather than permission-less open loop systems.

So next week, we're going to be moving to public policy. Oh my god. You're going to get to read my testimony, all 28 pages of it. Yeah, look, I get it. But I was asked to testify in the House Agriculture Committee in July. It's a venue I'd been at a whole bunch of times. It was fun to be back in front of them, Chairman Conaway from Texas and Collin Peterson from Minnesota.

But yes, you'll get to read my-- I knew that there was no legislation that was going to happen this year. I want to just give you the feedback. But Republicans run the committee. They get to invite as many witnesses they want, and then they let the minority invite one, sometimes two witnesses. So I got the call to testify, because I'm like the old sea dog, and they're bringing me in or something.

But it was fun. But I was preparing for this class anyway. So I kind of wrote the testimony for you all. Congress thought it was for them. And it was. It was. But that's the main thing. Mark Carney, who runs the Bank of England, wrote this really beautifully written piece that he gave in the spring, about a little bit the history currency and so forth. But Mark also runs the Financial Stability Board, which has the finance ministers and central bank governors and securities regulators from 20 countries. So it's the G20's finance heavies.

I used to go to that, not as a finance heavy, but I used to go because they wanted me inside the tent, rather than outside the tent, because we were doing derivatives reform here in the US. And some of the foreign finance ministers had a different point of view. And when it got to the place when finance ministers-- and it was an interesting group, the Russian finance minister in the UK and the South African and four others wrote a joint letter to Secretary Geithner pointing out some-- shall we say observations on what we were doing. They had differences.

I got invited, so I used to go. I got to know Mark very well. But it's a good paper. And you'll get a sense really-- I would say, Mark is neither a Bitcoin maximalist or minimalist, but he does say don't use the word cryptocurrency. Use the term crypto asset. So it's kind of an interesting piece.

And then I don't know how many of you are Sloan Fellows that are here. I recognize some of the Sloan Fellows. I think about 20% or 25% of the class are Sloan Fellows. You're going to get to see Joe Stiglitz in New York in a few weeks, and I think-- yeah, this is the CNBC piece where Joe, who's a Nobel laureate at Columbia University, has a stark and distinct point of view about Bitcoin.

I've had two or three lively conversations with Joe about this. Later in the semester, you'll read Paul Krugman and Nouriel Roubini, and there's a little video of Bill Gates talking about Bitcoin. I want you all to be aware of the Bitcoin minimalist and understand what they're saying. And I would put Joe on a 1 to 10 scale, at maybe 1 and 1/2 or maybe 2.

Paul, you'll read Paul Krugman's piece a little later. He's kind of down there, too. I can't just-- they can't modulate between them. But I think it's really important to understand what some really great minds are thinking about this from that side as well. So that's what the three things are for next week.

And the conclusion, I think that it does provide the networking, but it comes with costs. As we said, there are a bunch of trade-offs. I think the scalability, the efficiency, the privacy they want are solvable. I can't prove it. But I think in a matter of years-- and it might be three or 10 years-- it won't be three to 10 months, though. I think a lot of that is susceptible to the bright minds of MIT and elsewhere as computer scientists.

I think the challenges that are tougher, it really relates to governance. I think governance and collective action and back to those two graphs, there really are places that are better to centralize than decentralize. And we're going to be exploring that for the rest of this semester together. So thank you. Thank you for the veterans who sat through all that.

[APPLAUSE]