GARY GENSLER: Welcome, welcome. If you have a desire to learn a little bit about blockchain and its intersection with the world of finance and money and you're looking for 15.S12, you're in the right place. If you're here to not do that and just hang out and have a good time, I guess you still hopefully are in the right place, because we're going to have a good time this semester. My name is Gary Gensler. I'm a Senior Lecturer here at MIT Sloan.

I'm also an advisor over at the MIT Media Lab. And I've spent a lifetime around the world of finance, and money, and public policy. And I've been at MIT this last eight months.

And we're going to learn a lot together about blockchain and money. We're going to have a little bit of fun here and see what we're going to do. So we're talking about blockchain and money. That's where we are.

By the way, I do cold call. I do call on you-- so if you want to leave now, I understand-- because I want to have an interaction a little bit about it. So my first question for the class, for everyone, whether registered or not, how many of you have ever owned a cryptocurrency? Wait, wait, let's see. It seems like it's about 45% of you or so. All right, so it gives me-- Alin you want to keep your hand up long?

And how many of you have ever worked on any blockchain-related projects, in an entrepreneurial setting, a corporate setting, anywhere? All right, good, so about a third in the room. All right, so you all know probably more than I do, but I'm going to give it a shot.

I'm going to always start every week with what are the study questions for the week. How many of you actually got the syllabus? This is not going to be graded assignment. I just have to have a sense of who actually got this syllabus-- so a good many of you.

And how many of you actually did the two readings? It's not graded. I've just got to gauge the class. Oh, thank you, thank you. Write those grades down, by the way--

[LAUGHTER]

- -

--no, no. All right, so the two main questions for this week's lecture really is, what is blockchain? And why might it be a catalyst? And I emphasize the word "might" it be a catalyst for change in the world of finance. We could talk a lot about things outside of the world of finance. And blockchain may indeed have a lot of applications outside of finance, but I've chosen to try to just narrow the scope a bit. So this semester is really about blockchain and money or blockchain and finance.

And secondly, you will see index cards on every one of these round tables. One assignment, by the end of the class-- you could do it now or later-- I would like each of you to anonymously write on the card what you want to achieve in this semester. It could be anything from this class, from learning about blockchain, from making money on Bitcoin, from-- I don't care if you tell me it's meeting your future spouse. Like, what do you want to achieve in this class? I can't help you on the third, but I will try to help you on the things I can help you on.

And Sabrina and Talida will collect them later. And next Tuesday, we'll tell you the results. What is it that you want to achieve in this class? And then we'll see at the end of the semester if we've done that. So it's just a way to help guide me help you. So that's what we're trying to do.

And so what were the two readings? One was a little thing I did. And one was a thing I did with some of my colleagues. And Tom, since I know you, what did you take out of the readings?

AUDIENCE: That blockchain is essential to improved profitability [INAUDIBLE].

GARY GENSLER: Did you have a good summer?

AUDIENCE: Mhm.

GARY GENSLER: Did you raise your hand? Did you own Bitcoin? No. Who in the class read the readings and took something different than Tom? He said there was potential. And your first name?

AUDIENCE: Alin.

GARY GENSLER: Alin.

AUDIENCE: Well, I'm coming from the technical side. So from the technical side, all I see is a bunch of hype. And 10 years have passed since the launch of Bitcoin with very little to show for it other

than hype. [INAUDIBLE]

GARY GENSLER: OK, how many agreed with Alin? This isn't a vote. No, just two or three. How many agreed with Tom? There is more. And how many of you are too shy on the first day to put your hands up? Most.

So I'm going to start and go back-- the internet. How do I sort of-- I've come about this and of thought about, well, what is blockchain? What is it really about? Well, the internet started many decades ago, before most of you were born, but 1974-ish. I mean, there is some predecessors even from the late '60s, the ethernet, which is really how two computers communicate.

And then you had TCP/IP, which was really the internet protocol of multiple computers compute-- talking to each other. And then later on in 1990, how do we move forward? Does anybody know what HTTP is? We're at MIT. Your first name would be helpful.

AUDIENCE: Eric.

GARY GENSLER: Eric.

AUDIENCE: It's a protocol for communicate web content.

GARY GENSLER: Web content.

AUDIENCE: It's Hypertext Transport Protocol.

GARY GENSLER: Right, do You know who is associated with the invention?

AUDIENCE: I don't remember right now.

GARY GENSLER: Anybody else? Anybody know who-- it's not in the readings, or anything, Tim Berners-Lee? Anybody know who is associated with TCP/IP?

AUDIENCE: Was the company initiated by MIT faculty, I think, [INAUDIBLE] or something?

GARY GENSLER: I don't know if it was a company associated with MIT, but Vint Cerf may have had some association with MIT. So these are the first three layers. And then there were companies, commercialization, 3Com and Cisco. And of course, Amazon is still around today.

But there was something else going on. How do we commercialize the internet? Does anybody

know what this scene is from?

AUDIENCE: This is the first pizza sold by Bitcoin.

GARY GENSLER: Good thought, good thought, first pizza sold by Bitcoin, but no.

AUDIENCE: Is it from that movie *Hackers* or something?

GARY GENSLER: All right, movie *Hackers.*

AUDIENCE: I think it's from *Net.*

GARY GENSLER: *The Net?* Have you ever seen the movie? It's not a good movie. So this is the opening scene of *The Net.* And yes, that's Sandra Bullock.

And the year is 1995. It's a cyber thriller. You know, a president's involved. The Defense Department's involved, and so forth.

But actually, Pizza Hut is associated with the very first sale, online sale anywhere in the world. They started something called PizzaNet. This was the screen, by the way. If you wanted to go on, you could order your pizza.

But there was one problem. Does anybody know what the problem was with PizzaNet? I mean, maybe there were multiple problems. No, Alin I've called on you.

AUDIENCE: You couldn't pay online.

GARY GENSLER: You couldn't pay online. Nobody had figured out how to move money online. You had to pay when you showed up with the pizza.

So now I'm going to talk a little bit about cryptography. We're going to spend a lot of time on cryptography. It's cryptocurrencies and the like. What's your name?

AUDIENCE: Jihee.

GARY GENSLER: Gigi?

AUDIENCE: Jihee.

GARY GENSLER: Jihee. Jihee, what's cryptography?

AUDIENCE: I would assume that that's something cryptic?

GARY GENSLER: Cryptic, all right, no, you got it. You've got a start there. Anybody want to help Jihee out? Does anybody want to help Jihee out? Yeah, tell me your first name. We're going to figure out how to have everybody have nameplates by next week, but we'll work with Ryan and do it that way.

AUDIENCE: Addy

GARY GENSLER: Addy

AUDIENCE: Yeah-- it's the technology or the science behind encryption and decryption for fortification, so how do you encrypt a particular text such that it's not readable by someone else without having the decryption code.

GARY GENSLER: OK, so it's how do you encrypt something so it's not detectable by others. Or in essence, it's communications in the presence of adversaries. You have an adversary who wants the communication. You want to communicate and not let your adversaries know that communication.

And this is true for ancient times. So in ancient times, there was something called the cipher. And this was a way that you'd take a piece of leather or a piece of cloth and have a lot of letters. And both sides, you'd encrypt and decrypt, because they were different measurements of the cylinder. Has anybody seen the movie *Imitation Games?*

AUDIENCE: Mhm.

GARY GENSLER: All, right the Enigma machine-- now the movie was wonderful, because it said Turing cracked it. And he did help crack it in an automated way, but actually, the Polish government had cracked it in the 1930s before they fell to the Germans. And Turing built on all of that and cracked it further. And then in the 1970s-- and this was here at MIT, to some extent-- there is private-key public-key cryptography, which I'm not going to dive into today, but it's the heart of Bitcoin and blockchain. It's at the heart of the internet.

But it's about-- the key thing is communications and the presence of adversaries. How do you keep a secret when everybody wants in and get that information? And there is a long history. And MIT is at the center of a lot of that.

A lot of early cryptography failed on the internet. In the early '90s and late '80s, David Chaum

and others tried to do things. And we're not going to debate these today, but you will have one reading-- I think it's either next week-- which will give you that history. And it's worthwhile knowing about the history of failure.

But cryptography is the reason why the internet works today. Does anybody want to tell me what SSL and TLS is? Do we have any computer scientists? And remind me your first name?

AUDIENCE: Eric.

GARY GENSLER: Eric.

AUDIENCE: That's the protocol that mounts on top of the TCP/IP stack to provide encryption using asymmetric case, which is public-infrastructure cryptography. It's secure socket layer [INAUDIBLE].

GARY GENSLER: Right, so it basically uses asymmetric cryptography, which we're going to talk about two lectures from now, but it secures the whole internet. So all of a sudden you could deliver the pizza and get a pass code. And I have to tell you, I never knew how this worked before I was at MIT.

So PayPal came along in 1998. I mentioned this. A whole bunch of other digital currencies then failed, but some of these people who we'll read later-- like, we'll read Nick Szabo's is a piece on smart contracts later, Adam Back who created Hashcash. Some of these innovations were what Satoshi Nakamoto later used. Some innovations which were really helpful and worked were Alipay and M-Pesa. Does anybody know what M-Pesa is?

AUDIENCE: I think it's used in Kenya as, like, mobile cellular-enabled cash.

GARY GENSLER: Right. In essence, they found out in Kenya-- this was 10, 12 years ago-- that people were trading mobile minutes. They were unbanked, but they had cellular phones. And they were trading their minutes as a form of currency. And Safaricom realized that and said, wait, we could help people be part of the digital economy, even if they're unbanked.

And in Africa today, a half of the adult population, according to World Bank figures, is still unbanked, but half of that half has mobile phones. M-Pesa has 20 million customers in Kenya right now. So it's a form of money that's kind of swapping mobile minutes.

But the riddle remained, how do you move money on the internet? Or in essence how, do you

move value peer to peer without a centralized intermediary? And that's the core of blockchain technology.

So who solved the riddle? Is anybody going to tell me who solved the riddle? Who solved this riddle? No, [INAUDIBLE]. You're wearing a t-shirt that says Quentin Tarantino. So I think Quentin Tarantino--

AUDIENCE: [INAUDIBLE]

GARY GENSLER: --should solve a riddle. What's that? What's your name?

AUDIENCE: Rufus.

GARY GENSLER: Rufus-- and who solved this riddle?

AUDIENCE: Satoshi Nakamoto.

GARY GENSLER: Yeah. So a peer-to-peer cash-- this is the actual doc top of an email that was sent out on Halloween 2008 by Satoshi Nakamoto. We don't actually know who Satoshi Nakamoto is, but it's a study question a few lectures from now to ask you to tell me who you think Satoshi Nakamoto is. So I won't ask that now.

And he started with a very simple sentence in his email. "I've been working on a new electronic cash system that's fully peer-to-peer with no trusted third party. It's kind of a modest statement. And so the question is, is this another internet layer? We're going to explore that this whole semester.

I don't really have the answer. I don't think the best minds at MIT could really yet tell you. There are some who are maximalist and say, yes, it will be. And there are others who will say, no, no, no.

And in this course, we're going to review the minimalist and the maximalist. We're not going to try to center it in one place. But that's the key kind of question.

So what is a blockchain? We're going to do this and a lot of lectures, but I'm going to try to do it in a short version. So it's time-stamped append logs, meaning you can add a little bit of information to this. And it's time-stamped. So these are these blocks being added.

Satoshi did not invent blockchain. It was way earlier. Does anybody want to guess when it

was? You're going to have a reading about this later, but early 1990s.

AUDIENCE: Stuart Haber.

GARY GENSLER: What's that, Madars?

AUDIENCE: Stuart Haber.

GARY GENSLER: Stuart Haber, Stuart Haber-- worked for Bell Labs, right? So one of your assignments-- it's not going to be a graded assignment. It's just going to be a fun assignment. Could any of you, I'm going to say by next Thursday, just because, have some fun, find the longest, and time wise, longest-running blockchain. It's not Bitcoin. And it's been running since the mid '90s. And your clue is *The New York Times.* And we'll discuss it next Thursday.

But this time-stamped block, block, block, block of data creates a database, an auditable database. And we'll talk about ledgers, particularly next week, but we'll talk about ledgers all throughout this course, and how it changes the world of finance. Now, it's secured by cryptography, because cryptography, remember, is communications and making sure adversaries can't pick you off.

We're going to learn about hash functions. And hash functions are a really important part of cryptography, and initially for databases, and how to search and store information in databases, but in this circumstance, hash functions were the way to not only append the next block to the prior blocks, but really importantly, to compress data, to make it more manipulable, and to verify it, and as I've written here, tamper resistance and the integrity.

Digital signatures, which has to do the public-key private-key cryptography-- there is no prerequisite to this course. You do not had to have taken computer science, cryptography, algorithms. If I can learn a little bit about hash functions and asymmetric cryptography, these are the two key important sides. And we have enough computer scientists in this room that can sort us out if I say the wrong thing. Right, Madars? Hopefully.

And then consensus-- so there is a really important part of blockchain is, how do you decide who appends that next block? Because when I went back here, there is block and block. Each of these blocks, somebody has to decide who appends, who gets to pick the next block.

And that's what's called consensus protocol. And there is wide debates about consensus protocol. And we'll talk a lot about consensus protocol. But in essence, it addresses

something, a term called the cost of trust.

And we'll talk about Byzantine Generals problems, which is another reading. The Byzantine Generals problem was laid out as a sort of mathematical game theory issue some 30-ish years ago. That's what Satoshi Nakamoto solved was this last part, the Byzantine Generals problem.

Pizza for Bitcoins-- a year and a half after Satoshi Nakamoto laid out blockchain and Bitcoin, somebody sent an email. And you'll get these slides. But this is the real, live email. I'll pay you 10,000 Bitcoins for a couple of pizzas. I just want some pizzas. The guy who sent this, he says, I like onions, peppers, sausage, mushrooms-- Laszlo.

Now, catch the date. This is May 18. And he's offering 10,000 Bitcoins of 2010. But the key line is, what I'm aiming for is getting food delivered in exchange for Bitcoins. Nobody had used Bitcoins as a medium of exchange. 16 months into its existence, nobody had used it to buy something.

And Laszlo is a computer scientist in Florida who was just kind of interested. And he put this ad on an email list. Three days later, he still doesn't have his two pizzas. So nobody wants to buy me a pizza? Is the Bitcoin amount I'm offering too low?

Another day goes by. He gets his pizzas. And he posts pictures. So here is a picture of his child reaching for those Papa John's pizzas. Anybody know what those 10,000 Bitcoins were worth back in-- back then? Chicago.

AUDIENCE: I know what they're worth now.

GARY GENSLER: Anybody want to say back then?

AUDIENCE: [INAUDIBLE]

GARY GENSLER: What's that?

AUDIENCE: [INAUDIBLE]

GARY GENSLER: $41. And Laszlo was saying, two pizzas are probably worth $25 to $30, because there was a whole email thread. He kept saying, why won't anybody get me my pizzas? You can make money on this. Today or earlier, late last night, $66 million. Yeah, so it's kind of a cute story. May 22 every year is called Pizza Day or Bitcoin Pizza Day or something.

So what is blockchain technology? These are my words but they're sort of picked from the literature and so forth. It verifiably moves data on a decentralized network. And the economics of blockchain technology are really around that, verification, and the economics of verification, and the economics of networking.

And in many ways, blockchain adds certain costs to the verification through this consensus protocol that we'll be studying, but it lowers some other costs of verification, because you're not relying on a centralized authority. So it's really a trade off of cost to verification. I don't think it's-- I'm not a purist that says it's better or worse, but it's a trade off of cost and verification through decentralized networks.

The data can be value. Like, Bitcoin was a money system. Or the data can be actually computer code. And we'll learn a lot about smart contracts. And you could have the data being verified computer code and algorithms.

My world, finance, this directly goes to the plumbing of finance, because finance is fundamentally about moving money and risk through a network. And that network is the 7 billion people that live in this world. It's moving money and risk.

And you've all taken finance courses. Or many of you have. And it's the intermediation of money and risk throughout our economy.

But there is a whole host of challenges. And over the course of this semester, we'll talk about those challenges, technical, commercial, and public policy hurdles. Will they be solved? Will they not be solved? But it could be a catalyst-- but we're not sure yet-- for a change in the world of money and finance.

So does anybody want to tell me that the role of money in society? And tell me your first name.

AUDIENCE: Thomas.

GARY GENSLER: Thomas.

AUDIENCE: Basically it's a way exchange things and services between people--

GARY GENSLER: All right, medium of exchange, got that one.

AUDIENCE: --without doing bartering, I mean. Exchange [INAUDIBLE].

GARY GENSLER: So a medium of exchange. Somebody give me a second-- yellow shirt.

AUDIENCE: Yeah, medium of savings.

GARY GENSLER: Savings, all right, so that would be a store of value.

AUDIENCE: Yeah.

GARY GENSLER: Third-- I'm sorry, the gentleman here.

AUDIENCE: Unit of account.

GARY GENSLER: Unit of account-- wow, all right, there we go. There we go. So we're going to spend some time next Tuesday talking more about money, and the role of money, in the history of money, which I think it sort of lays a foundational piece of this.

What about the role of finance? I've already sort of said a few things about that. And I'm sorry. I don't know your name, but right here, the woman, yeah-- role of finance? It's all right, I'm not going to tell any financial finance professor what your answer is.

AUDIENCE: To raise money.

GARY GENSLER: To raise money-- so keep going. Anybody else want to--

AUDIENCE: Connect savers and borrowers.

GARY GENSLER: Connect savers and borrowers-- so connecting is sort of moving money, moving.

AUDIENCE: The valuations.

GARY GENSLER: Valuations-- so that's the pieces of it. So there is moving, making valuations. I use the words, moving, allocating, and pricing. Pricing is the valuations of money.

But let's not forget, it's also about risk. When you buy insurance, that's a transference of risk. When you buy an equity stock, that's a transference of risk. If you enter into a complex credit default swap, that's a transference of risk. So finance is not just the movement of money. It's the movement of risk as well, throughout the economy.

And I always think, finance, I always-- I've thought this when I was at Goldman Sachs for 18 years-- that finance sits at the neck of an hourglass. And it's why it collects so much economic

rents from society, because when you sit at the neck of an hourglass and billions, literally trillions of grains of sand go by, if you collect some of those grains of sand, you get uber wealth. And that's-- those are for other classes. But finance can collect a lot of economic rents.

The financial sector, though, has a bunch of challenges. We'll have one lecture later in the semester about some of those challenges. And we have a reading. I think Sheila Bair wrote something recently that I asked you all to read later in the semester.

But we will talk about the financial crisis and some of the problems. But it's had a lot of crises. Fiat currencies have a lot of instabilities, of course. We have centralized intermediaries, as I laid out. And we'll talk about collect a lot of economic rents.

So there is opportunity. Blockchain has real opportunity to kind of come under this world of finance and maybe do some things better. Central banking, I also have a bunch of legacy payment systems. And those legacy payment systems are slowly adapting, but it's slow.

And why did Alipay do so well in China is part of this story, because there were so many unbanked, just like M-Pesa in Kenya. But here in the US, we still pay 2.5% to 3% for our interchange charges for Visa, MasterCard, and the like.

And a lot of clearing and settlement still has a lot of counterparty risk. And one that I care deeply about, financial inclusion-- there is still 1.7 billion people in this world who are unbanked. And so we don't think of it as much in the developed countries, but it's certainly true in many products even here in the US.

And these are, to me, the opportunities. Finance is 7.5% of the US economy. That's $1.5 trillion of revenues. So any of you that are thinking about entrepreneurial opportunities, the payment system just here in the US is a 0.5% to 1% of our economy.

That's $100 billion to $200 billion of revenues. I think Visa is about $18 billion. But you know, when you add up the whole payment system, that's $100 billion to $200 billion in payment revenues. So that's kind of the opportunity.

Can blockchain technology come in? It's got problems. It's slow. It has performance issues still. But can it compete with that?

Here are some of the problems, the financial sector would say, with blockchain. These are real, live things that we're going to study later in the semester. They say, it doesn't have the

performance, scalability.

A modern payment system, you need to be able to move about 100,000 payments a second. A modern securities clearing, the Depository Trust Corporation, the Securities and Exchange Commission says, you do about 30,000 transactions a second, but we need you to scale. And your computers and everything have to be resilient to 100,000 transactions a second.

Bitcoin, you can do about seven transactions a second. Visa currently-- it depends on the second-- does anywhere from 20,000 to 70,000 a second. So it's just a sense of scalability and performance. We might get there. It might be three to seven years away. I'm optimistic, but there is still a bunch of performance and scalability issues.

Privacy and security-- blockchains, by their nature, are public. So they're not fully censorship-resistant, but there is a lot of innovation about making them more private. But then that makes the public sector a little nervous. Interoperability-- they don't necessarily work yet with other legacy systems or with each other. The internet, one of the great innovations of the internet, it became interoperable, that all of these different websites could kind of speak with each other.

Governance is a very big issue we'll talk about. And one of the things about governance is, it's hard to update the software of a blockchain, because if you create a decentralized where no one's in control, no one can collect economic rents, you also don't have sort of somebody with the ability to necessarily update the software. And we'll talk later about how Bitcoin updates its software, and what Bitcoin core developers are, and so forth.

But Facebook, you do know one thing-- though they're a company that collects a lot of profits and economic rents off of their two billion members, they know how to update their software. It's a governance issue that's a real, live challenge. And that's why the financial sector says, I'm not sure this works, this is ready yet for me. And then thus, what are the commercial use cases? And what are the public policy issues?

So right now, the financial sector favors permissioned blockchains versus permissionless. About four weeks from now, we'll kind go through these two differences, but I want to just frame this briefly. Permissioned blockchains have a known group of people who actually participate.

The half of you that said you've owned Bitcoin, you know it to be something where anybody can update the ledger. Permissioned blockchains, you can't do that, in essence. You pick the 3

or 20.

The Australian Stock Exchange is updating their clearing and settling. They announced they're doing a blockchain project. They're doing it with digital assets. And they're using the Hyperledger blockchain, which is an IBM software, open-source software. But the Australian Stock Exchange is going to put it on three computers, which is called three nodes, that they control all three of them. The Depository Trust Corporation is looking at blockchain-inspired solutions for some of their data warehouses, but they, too, are going to control the nodes. I'm just giving you-- that's permissioned blockchain. So there is nothing wrong with that. That's just how they are looking at this.

Permissionless blockchains are like Bitcoin, unknown participants, securities based on incentives, a cryptocurrency, and crypto economics. Crypto finance is about $200 billion. But you know, you have to update these slides daily. Two days ago, it was $230 billion. And this little pie chart is-- a little over half is Bitcoin.

The next slice is something called Ethereum, and then Ripple, and down the line. We're not going to spend a lot of time in this semester-- if your goal is to how can you profit, and day trade Bitcoin, and day trade Ether, god bless. Go prosper.

You can stay in the class. I just won't give you much advice on it. This is not a crypto-investing-centered class. But I'm OK if that's what you're doing.

Does anybody know what the worldwide capital market size is? Does anybody want to guess? You know, this is $200 billion. What's it look like? I've already said it's modest.

AUDIENCE: Hundreds of trillions.

GARY GENSLER: Hundreds of trillions-- global equity, about $80 trillion, global bond and debt markets, $250 trillion, so it's still quite modest compared to that broad breadth of capital formation. And gold? If Bitcoin is digital gold, what's the value of gold? All the gold that's ever been-- Tom?

AUDIENCE: About $6 or $7 trillion.

GARY GENSLER: Yeah, $7 trillion-- so just to give you a sense of scale. So there is also something that's interesting about this space, is that it's outsized public attention, even as evidenced by the hundred of you in this room, versus the size it is relative to the capital markets today. There is a bunch of public policy issues. We'll have a lecture.

I'm a former regulator. I ran the Commodity Futures Trading Commission. But this course is not about regulation, though we have to always come back to regulation. We always have to infuse what we're doing with the regulation.

But let me just give you a little framework. And then you'll have to be bored in a handful of weeks and read-- I gave some congressional testimony on it. Yes, it will be required reading, sorry. But it's guarding against illicit activity.

A lot of Bitcoin and cryptocurrencies started out in the cyber punk sort of movement and libertarian movement, so forth. And it is true. You can use this for illicit activity, absolutely. But I would say, crime is not new, just the mechanisms and means are new. And so the criminals, yes, will use this and have used it for illicit activity.

Financial stability-- central bankers around the globe, sort of will this shake finance? Well, it's only $200 billion. The financial markets are $300 trillion plus-- not yet, is generally what they're saying. But for some countries, it's a way to get around capital controls. And so for those countries worried about capital controls, it's a very real and live set of issues.

And then protecting the investing public-- and when we do this in a few weeks, I'll go through each of these, the investor protection issues, and yes, the SEC, how we test, and the like. For those who wish to do their own initial coin offering, I'll give some broad sense of what the SEC is trying to accomplish. But it's a moving target.

So this is a very interesting thing. As opposed to many of your Sloan classes, or your C cell classes, or Media Lab classes, this is a very unsettled area of public policy. So it makes it interesting. And if you all go off and form companies, you will actually be helping sort of set the edge of that public policy debate.

I would always say, just remember poet Riley, the duck test. This is a poet, Indiana poet-- so those that aren't from the US might not know the duck test. But basically, if it quacks like a duck and it walks like a duck, it's a duck. So whenever you're thinking about public policy, folks like myself who once was a regulator, we think in the duck test.

And then we secondarily think about the actual words in the congressional act. Where is the common sense? And if it quacks and walks like a duck, it's probably a security. Or it's probably this or that.

The incumbents, like this lioness in the corner, are eyeing this space, because there is a lot of volatility. And Wall Street makes money on volatility. Volatility is the friend of Wall Street. It may not be the friend of investors, but it's a friend of Wall Street.

And they also like the trading volumes and the spreads. Coinbase, the largest crypto exchange here in the US, has 20 million accounts. They might not all be active, but that's the size of Fidelity's membership or account list and twice DE Shaw.

And Robin Hood-- how many of you have ever used Robinhood as a trading app? Wow, half of you. So you know, free trading, five million members-- for those who don't know, you can download Robinhood. And you can trade stocks for free, no commission. And if anybody is interested, show up and I'll do office hours on how Robinhood commercializes-- they commercialize your order flow. And they make money without charging you commissions.

But it's a sort of wonderful app. Millennials love it, 5 million members already. So you better believe DE Shaw and the incumbents are worried about things like that.

The startups are also more willing to beg for forgiveness from regulators. They're willing to sort of take risks and beg for forgiveness, whereas incumbents tend to have to ask for permission. So there is an unlevel field, that always, it's asymmetric business set of risk about regulatory risk-- not always.

I'm not crying for JP Morgan. I mean, the big incumbents have also-- they have their advantages. And Coinbase is becoming an incumbent rather than just a startup, in a sense.

And we'll talk during the semester about some of the incumbents. We're probably going to get Jeff Sprechers here in mid-November. He's going to talk to you about what Intercontinental Exchange and the New York Stock Exchange is doing with Starbucks, and Microsoft, and the like.

The financial sector use cases-- I'm not going to go through these, but this is the second half of the course, is going to go through each of these. And we'll do one to two sessions on each, payment systems, central bank digital currency, secondary market trading. The venture capital and initial coin offering space, we'll do two course on that, and move through.

So what are we going to do in this whole course? Basically, our goal is to learn the fundamentals-- that's about roughly the first half of the course-- pivot to two sessions on the economics. We're going to be talking about the economics throughout the whole course, but I

want to really just focus, drill down on the economics, on two of the discussions. And then riff through the financial space for the second half-- that's our journey together.

To me, it's for anybody who wants to gain critical reasoning skills. This is not just kind of a, hey, this is going to change the world and revolutionize everything class. And so I basically think of an old Defense Department term called ground truths. It's when the general doesn't really know what's going on but needs to figure it out and needs to talk to that corporal on the ground who has got dirt all over him and has been shot up and says, here is the real ground truth. We're going to try to talk about ground truths in this class and separate the mere assertion from the hype.

And some of your readings will be some real Bitcoin and blockchain minimalists, from Nouriel Roubini that uses words I'm not supposed to repeat on a recording about this stuff, to Paul Krugman who-- and Joe Stiglitz, and other Nobel laureates who say, no, it's not going to work, or Warren Buffett, to maximalists. We're going to try to cover both sides.

Larry Lessig is honoring me because he's in the back of the class-- who is an enormously esteemed professor from Harvard. I didn't know Larry was going to be here. And I did this slide before. But in 1999, I think, you wrote this book, Larry. Is that right?

AUDIENCE: [INAUDIBLE]

GARY GENSLER: *Code and Other Laws of Cyberspace,* I put you in the-- but I think it's worthwhile to think about Larry's four bits here. And I don't know, Larry, if you want to say anything, but I'm going to try to infuse this course in just how you think about this. The tech-- we're at MIT.

The technology-- and we're going to get you a lot of technology. If you want more than I can give you as a former finance sort of type my whole life, there is going to be a bunch of computer science people in the class. We're going to hook you up together with the folks from the Media Lab and C cell and try to connect you to the technology side if you want to swim deeper in that pond. But the technology really, really matters. And that's why we are going to go through hash functions, and go through asymmetric cryptography, and so forth.

From a business perspective, markets matter. Why is it that incumbents or startups are or are not doing this and that? Why is it 10 years in and nobody has got an enterprise-wide solution yet to payments that use blockchain? The law matters. The public policy side matters.

And the fourth of Larry's layout, social norms-- that's a little harder for me to teach. That's not what this class is about. But it is also a flex all this. It's not just the technology, and the markets, and the law.

So it's not just a three-legged stool. It's kind of a four-legged stool. How did I do Larry?

AUDIENCE: Excellent, all right.

GARY GENSLER: I really didn't know Larry was going to be here. But I wanted to give you a framework for how your faculty member thinks. And we'll be on this journey together. Range of perspectives-- we're not going to be a Bitcoin minimalist or maximalist. I'm probably, to be self-disclosed here, a little bit center minimalist on Bitcoin. Smart contract minimalist, maximalist, I'm probably pretty center. Larry is probably a little bit center maximalist, I'm guessing.

AUDIENCE: I'm hoping I can be, but you're going to teach me whether I can.

GARY GENSLER: Oh, so you're still center or center minimalist on smart contracts? And then blockchain maximalist or minimalist-- I'd say a few weeks ago, I was kind of center maximalist. And I'm sort of skipping back to the middle.

Permissioned blockchain, I'm a little bit more-- and there is some in here. Alin who is one of your Sloan cohort that you might know, six months ago when we met was working on a permissionless system. And now you're working on a permissioned system. You have a startup.

AUDIENCE: That is correct.

GARY GENSLER: Yeah, because you bounce up into the market realities. And we're going to talk a lot in this course about critical thinking, about when do you really need the advantage of a decentralized peer-to-peer system where the costs of trust are such that that's the right way to go. But I am one who thinks that there is also so much economic rents in the financial system that $1.5 of revenues, or 7.5% of our economy, or just $200 billion in the payment systems, for instance, that there may be times that you don't really need a decentralized system, but it just might be your opportunity to tuck in underneath all of those economic rents and all those revenues.

Now, incumbents will react. You poke an incumbent, commercially poke them, I mean, and they're going to react. And that's why I think blockchain may well be a catalyst for change, even if incumbents then adopt a lot of that inside.

The requirements of the course-- class participation is a hard thing to judge as a faculty member when I have this many people. But I always think class participation matters. We made it 30%, which if you have any advice on this next semester-- 30% two individual write ups, one in the first half, which is up to, I think, lecture 10, which is basically the blockchain fundamentals.

You pick a topic. I don't care which one, but you'll get a much better grade if it's about critical reasoning, if it's really taking whatever those sets of writings are and not just repeating that which is in the readings, but really going the next step and saying, here is what's going on.

And this isn't business school. You don't have to convince me that something about computer science. It's like critical reasoning about the economic opportunities, the strengths, the weaknesses, the opportunities, the threats, that old business school sort saying of swats with regard to that week's-- whether it's about hash functions early on, cryptography, or you sort of wait during the foundational period to permissioned versus permissionless.

You pick-- but to please hand it in before that class' lecture, because I might during the lecture say, who wrote today? Do you want to tell us what you think? And it might help spur the class participation-- and then a second write up in the second half when we're riffing through the use cases, again, critical reasoning.

And then lastly, the usual approach of teams of up to four-- no, I don't want teams of five, to handle that right now, three or four. And somewhere in the second half of this semester, we'll talk about more of the content. And there is a couple of you in here that worked with me last semester in a smaller group.

You know, I want you to do well so I'm going to sort of give you a sense of what do we want to do, but it's basically, the idea is, you're an entrepreneur or you're an incumbent. And what sort of use case are you going to pick? And whether it's permissioned or permissionless, sort of make a proposal.

Do a use case. Use your critical reasoning around this new technology somewhere in the broad world of finance. I mean, you know, and I'm glad to define finance really broad. You'll pick. So that's kind of the piece.

Act one are the fundamentals. I won't go through each of the pieces, but you know, that's in the syllabus, of course. Act two is the pivot of the economics, and act three, our financial

sector use cases. And hopefully throughout, we'll have a lot of fun.

So the study questions for next Tuesday, real quick, what are the roles and characteristics of money? So I really want to sort of dig behind money. Money is but a social construct or a social convention, medium of exchange, a store of value, unit of account.

There is some readings about the debate, whether money first came from the barter system, or a really good set of anthropologists and archaeologists and everything say, no, it actually came as a ledger system. And no one knows for sure 10,000 and 15,000 years ago whether money came from the-- out of the barter system or more as a unit of account, keeping account of credits and ledger. But I'd say, when you read through some of those readings, you start to think, well, this is just a societal construct. And so we'll get behind that.

What is fiat currency? Fiat currency, which is an invention, really, only of the last few hundreds years that we take for granted now. But how does that fit into that whole history? And importantly, how do ledgers-- accounting ledgers, I know, boring stuff, but it's probably why we came out of the dark ages about 500 or 600 years ago with double-entry bookkeeping. Sorry, I like ledgers. We'll talk a little bit about ledgers and how that fits into money, and securities, and so forth, and then layering in how Bitcoin fits on top of that history.

Next Tuesday is not deeply about Bitcoin. It's just a little dollop on that. There will be five or six readings. One of them is a three-minute video, the third one. It's fun. Watch. It's just a funny little video on what money is.

There is no need to read Nakamoto's full paper. When I said the email, I mean just the cover email. It's one paragraph.

My goal in the readings each week was not-- and each session was, by and large, try to keep less than 50 pages. You say, you're going to look sometimes and you'll go, it looks like it's more. And maybe it is. I figure you're all going to figure out for yourself how to sort through the depth of your knowledge.

But I will predict that some of you, maybe as much as a quarter or a third of you, are going to go down a rabbit hole one day. And you're going to be doing blockchain for the next 48 hours. And you won't know where the time went, because it is an addiction at some point that some of you will get, because there is this curious notion.

I'm not predicting that infirmity for all of you. I'm just saying some of you will have that happen to you. So occasionally I have readings just-- what, Alin it's happened to you?

AUDIENCE: I think so.

GARY GENSLER: Let me just conclude and then take any other questions and lay it up there. Blockchain I think does provide a peer-to-peer alternative. I hope, Larry, I'll be able to convince. It does provide-- and that peer-to-peer alternative addresses cost of trust. It doesn't mean it's the only way to address cost of trust, but it addresses cost of trust.

The financial sector does have challenges, not just that it has 7.5% of our economy in the US and similar ratios around the globe, but resilience, how it survives shocks. The financial crisis and things like that are real. And inclusion-- 1.7 billion people unbanked, but then if you look at other products, who has access to credit cards, and mortgages, and the like?

And then fiat currencies, Ken Rogoff and others have written a lot about the instabilities that come with fiat currencies. And we'll talk about some of the history, and why central banks exist, and how they came about. The next key point is, we already live in an electronic age. Satoshi Nakamoto and Bitcoin didn't create electronic cash. I mean, Sandra Bullock couldn't pay electronically. That was 1995. They did a sort of B-rated movie about it all.

But by today, you pay your tuition online. Those of you who work get paid online. You pay your auto loans online. Most of our lives are electronic cash, not 100%, but in some countries like Sweden, it's getting very close to 100%.

We'll learn together and discover that money is but a social and economic consensus. Blockchain technology along with crypto finance might be a catalyst for change. And then much masquerades as fact, but is only mere assertion. We're going to try to sort through that, those differences.

That doesn't mean that all of you are going to walk out agreeing with Paul Krugman, a Nobel laureate, or Nouriel Roubini, that this is just a bunch of nonsense. Some of you might, by the way. But I think you'll come out with real critical thinking skills.

And I hope that some of you will say, I've figured out actually where there is a real opportunity in the world of finance to use blockchain technology, and make it a better financial sector, democratizing finance, or somehow providing a service at a lower cost, a better service throughout. I hope throughout that we'll learn together and we'll have a bit of fun along the

way. So that's kind of my thoughts. Questions? We have exactly-- what?

AUDIENCE: 18.

GARY GENSLER: 18 minutes, there you go, but we can cut it short, too. I don't care. There we go. Could you tell me your name? And we're going to do placards. Ryan's going to work to figure out how to do placards, because--

AUDIENCE: It's [? Younghere. ?] I wonder how are the teams formed, the final project.

GARY GENSLER: How the teams form? Traditionally-- anybody at Sloan can speak to this too-- but students do it their own. So the faculty doesn't sort of try to insert themselves to help you, but we tend towards the latter half and say, well, who is formed up in groups?

If it's a smaller group, it's like, well anybody who is not yet formed in a team, why don't you move to the left-hand side of the room and just get together. But we could do that electronically too. And you know, whether Talida and Sabrina who could help in trying to basically have a social network to help form the teams, because this is a big group, you're right.

But that's traditionally, people-- students do it on their own. Other questions? Is anybody going to go out and sell their Bitcoin now?

Larry, why are you here? No, no, let--

AUDIENCE: Other than the payments you talked about or-- no, I am here because I think you're going to bring a critical skepticism to the whole field. And you're incredibly informed about the finance side. So I want to see the combination of those, and whether at the end I'm still there is a there there. I am convinced there is a there there. As we've spoken, because I really think it could radically change the cost of trust around the world.

That will benefit the developing nations substantially. But I think there is a lot of questions I still have. And I'm eager to see how this conversation helps it [INAUDIBLE].

GARY GENSLER: Well, I thank you for coming. And any week you could be here, any day, we benefit. And I hope it's really-- this is meant to be a conversation. I'm not that far ahead of you.

Simon Johnson approached me last October and said, what do you think about coming up to MIT? And Tom knows this story. And we were sitting down for lunch in DC. And it was a good

time in my life.

My three girls-- I have three daughters. And I'm a single dad. And they were-- two are in grad school and one are in undergrad. It was a good time in my life. I said, why not come up here and get engaged in this digital currency initiative over at the Media Lab?

And I've spent a life-- I was 18 years at Goldman Sachs on the investment banking side, helping people buy and sell companies. We call it mergers and acquisitions. And then I went to the trading side, fixed income, and went off to Asia, and did a bunch of-- I ran the fixed income, and currency, and swap trading in Asia.

And then my last job was the co-finance officer. So we were about a quarter of a trillion dollar balance sheet at that time-- Goldman Sachs, this is. We were still private, which meant if we lost money, we were personally-- I was a general partner-- was kaput. That's a technical word.

But we had 700 legal entities and 1,000 people who could commit the capital of the firm. Those are people we generally call traders. But you know, it was a fascinating period of time.

I then went on to public service, because Bob Rubin knew that I'd be a soft touch to service. He was the Treasury Secretary. I was a former partner at Goldman Sachs. And I went off to the US Treasury as a assistant secretary, an undersecretary in the late '90s-- a little different times than we have now for many reasons.

But we were paying down the debt. We were dealing with the Asian debt crisis, long-term capital management, the Russian debt crisis. It was sort of a fascinating period of time.

I worked on a bill with John McCain-- I didn't get to know Senator McCain that well, but he was just remarkable to work with even for a short period of time-- called E-Signature. It was a bill that basically said, you can sign everything electronically. And he was the Chair of the Senate Commerce Committee at the time. It was a wonderful little-- sometimes in government, you can work on small things.

I worked on the redesign of the currency. And I could tell you stories about why it looks the way it does, and how you can redesign paper currency. And for a future lecture, I'll tell you the one design feature that I-- is still in the currency. And you can visually see it.

And when I asked for it, the fellow that ran the Bureau of Engraving said, why? And I said, because it looks better. And I'm the guy that's approving it. And maybe can we get it done?

Can we work this out?

And it did look better. And he loved it. He was worried about the political risk of doing it. It was a better design. He just was-- I said, I'll cover you politically. Let's do it.

But then I worked with Paul Sarbanes in what became Sarbanes-Oxley. I was his senior advisor. I worked and kicked around some political campaigns. We lost two of them. That would be the '08 Hillary campaign and the '16 Hillary campaign. I was her Chief Financial Officer. I was an OA to a senior advisor doing economic policy, and outreach, and handholding, and-- oh, gosh.

And then in the middle of those two campaigns, I ran something called the Commodity Futures Trading Commission, which was post-crisis, what do we do? This is a real public policy shortcoming. And I looked at it as an opportunity to, as I said, democratize finance a bit and lower risk.

And so we tried to bring transparency to a $300 or $400 trillion dollar market called swaps, which are just contracts for transference of risk. And they are a form of a derivative that were unregulated. And we were trying to bring transparency to that and lower risk through central clearing.

So that's sort of my professional life. And as I said, I've got three daughters. And they're well-situated. So when Simon said come on up, I said great. And I love him. I'd say, it's just terrific. And you all are great. Unless there is other questions, I'm going to let you go early. I don't--

[APPLAUSE]