GARY GENSLER: All right, so we're going to try to-- I was giving a little bit more time for more people to show up-- chat about what did we cover this semester. So I'm going to try to talk about-- we started out-- money and ledgers, and why does that matter, and if you go away from all this.

Satoshi Nakamoto's innovation-- what is that again? The economics of blockchain technology, why the financial sector is so entwined in all of this, though it's not the only place we're going. A little bit about crypto finance and public policy frameworks, and then wrap it up with a quote from Ben Franklin-- will be the last thing we talk about at the end, about paying it forward.

I don't know how many people read the article I wrote for Coin Desk, which will run in a day or two or something, but that, too, just like helped me wrap up the whole semester. As I told you, I'm neither a maximalist or a minimalist, but in a few minutes, I'm probably going to ask you all to kind of let me know where you ended up.

So the role of money. Anybody remember the role of money in an economy, the three things?

AUDIENCE: Medium of exchange, unit of account, store of value.

GARY GENSLER: Medium of exchange, unit of account, store of value. I don't think we really know, when we go through all the history and the archeology of it, which came first, but all three really matter. So how many people think that Bitcoin-- just Bitcoin. I'm not talking about the other 1,600 tokens-- Bitcoin fulfills these three roles of money? James, was that a hand up?

AUDIENCE: Yeah. Yep.

GARY GENSLER: You're saying yes.

AUDIENCE: Yes.

GARY GENSLER: Alexis? Oh, we got two. Hugo? Somebody take the other side. Tom?

AUDIENCE: Nope.

GARY GENSLER: That's it? That's it? A whole semester, and all you can say is nope?

AUDIENCE: Yeah.

GARY GENSLER: Nope? All right. Anybody want to give more? Brotish?

AUDIENCE: So not a store of value because of [INAUDIBLE].

GARY GENSLER: So Brotish says not a store of value, but isn't it $60 billion of value right now?

AUDIENCE: [INAUDIBLE]. So there is a value, but it's too volatile.

GARY GENSLER: James?

AUDIENCE: I respectfully disagree. It's volatile when you think of it in exchange of a dollar, but if you move your mindset, a bitcoin is a bitcoin is a bitcoin. Right? It's only volatile if you think [INAUDIBLE] a dollar.

GARY GENSLER: Oh, my god. Here we go. Ross?

AUDIENCE: But that same thing is true of corn, right? A bushel of corn is-- I'm with Brotish on this.

GARY GENSLER: I'm sorry, were you in the no camp or the yes camp? That it's a store of value.

AUDIENCE: I'm in the no camp.

GARY GENSLER: No? Is it a medium of exchange?

AUDIENCE: Yes.

GARY GENSLER: Oh, medium of exchange. Sean?

AUDIENCE: In response to [INAUDIBLE] none of the currency can actually be treated as a stand alone currency. Everything has to be treated as a pair. So everything's a relative comparison. So you can't really treat Bitcoin on a standalone basis.

AUDIENCE: I don't know if I agree with that. But I would say that pretty much anything can fit into all three of these buckets. It just depends on how dependable it is. In those three buckets, with US dollar's very good at being medium of exchange, very good at being a dependable store of value, and a steady unit of account. But you could also have a bushel of wheat or something.

It would be all three of these things, but it wouldn't be equality.

GARY GENSLER: Right, but-- please, Jihee.

AUDIENCE: So the fiat currency-- the reason why I think US dollar is stable is because there is a US central bank that actually backs up that. Because it's just that fiat currency. It is a liability of the central bank, whereas Bitcoin doesn't have a center to worry that banks have.

GARY GENSLER: Nice music that we're getting. [INAUDIBLE] a serenade.

AUDIENCE: So therefore, I don't think the store of value argument will work.

GARY GENSLER: So you think-- [INAUDIBLE] saying, well, there's no central bank behind it, so maybe it doesn't hold up. But if you take anything away from the class-- and I'm going to have some other takeaways, too. Remember, the three things that about the role of money-- but it's a social construct.

Even with a central bank-- a central bank is, ultimately-- we enshrined in law. We enshrine it in a big institution, and bricks, and mortar, and columns usually. You always have to have those columns. But it's still a social construct.

And Bitcoin does, in some ways, have all three of these. It's just not broadly acceptable. It's rarely used as a unit of account, but it is sometimes used as a unit account in some initial coin offerings. It's not used, generally, as a medium of exchange. But some people are paid in Bitcoin some.

Software developers are actually paid in Bitcoin. And it's $60 billion. It might be volatile. It has a store value. So I'm not trying to take maximalist or minimalist, but I'm probably between Tom and James, because it does have all of those qualities in to some extent in there.

Early money-- remember some of our walk down memory lane. Some of these early monies fell apart, became extinct, when they got debased. And we talked about, early in the semester, even the story about it. It was, I think, a British-- when the British got to the island of Yap, they went off a couple miles and quarried the stones and kept bringing more yap stones there. And all of a sudden, it got debased.

And then, of course, money turned to paper money. And in the bottom left-hand corner, it started as warehouse receipts. So the paper was just a representation of the store of value--

the metal, or the corn, or the wheat that we had earlier.

Another important thing was ledgers. Who wants to remind the class what a ledger is? Why do ledgers matter? Anybody want to-- ledgers? All right, clearly I didn't make it on ledgers. Hugo?

AUDIENCE: It's transaction history, basically.

GARY GENSLER: A store transaction history. What else is there?

AUDIENCE: Balances.

GARY GENSLER: Balances of?

AUDIENCE: Accounts.

GARY GENSLER: Accounts. So it stores a balance and a transaction. So you can think of it as a flow and a balance. The flow is the transaction-- I give Hugo money. Regardless of who gives Hugo money, here's his balance. So an income statement and a balance sheet is a flow and a balance.

But ledgers and keeping ledgers go back thousands of years. So blockchain technology is really about money, but it's also about a database that has ledgers. And ledgers usually store things of value.

So then we got to fiat currency. And fiat currency, as Jihee said, they were represented by central bank notes, central bank reserves, and bank deposits. So there's three things. Does anybody want to see if anybody listened in those classes? [LAUGHS] I'm kidding around. Elan, you're going to say, why is it those three things? They're all forms of fiat money.

AUDIENCE: I thought you were asking about the illicit activity in that list. Is that the question?

GARY GENSLER: All right, answer the question you want to answer.

AUDIENCE: Yeah.

[LAUGHTER]

[INAUDIBLE] there are things that are important in fiat currency, or is helpful. Fiat currency is important for paying taxes. And it is allegedly backed by the social understanding that the central bank will respect those notes at the end.

GARY GENSLER: Right. So it's actually-- you're on to this. It's accepted for taxes. It's legal tender. So actually, society gets together, through its parliament, through its executive, and passes a law that says it's legal tender. That gives it a huge leg up.

But this is what it's really about. It has huge network effects. And I wrote this in the *CoinDesk* article. The question I have for any new currency is, how does it compete with those incredible network effects? And we talk about Facebook has incredible network effects because-- two billion members.

But even money, as a technology, has a network effect because people readily accept it as a unit of account, a medium of exchange, a store of value. And it only loses that network effect, usually, when it gets debased, when people can't be confident that it's a good store of value because somebody else can mint a lot of it, or print a lot of it, or a king starts to print too much of it. But it has an extraordinary network effect.

On the other hand, sometimes currencies are a little bit challenged, like the euro right now. Will the euro ultimately work? That's for a different class and a different lecture, but will the euro ultimately work long term? I have my doubts whether it will work for decades to come, because there's so many jurisdictions. And there's not a unified fiscal account, not a unified economy, and not truly free movement of labor across that continent.

So that's fiat currency. It's sort of the game in town that then Satoshi Nakamoto is was addressing. And you all read the eight-page paper, but that was the first line. "Been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party." Basically, as Jihee said, no central bank.

Forget about that central bank. That was the core inspiration that was there. But interestingly, it wasn't the first try. And we talked early in the semester about at least a handful of early attempts that all failed because they were still centralized-- like DigiCash was still very centralized. Or they couldn't solve the double spending.

On the internet, you can send an email twice. It doesn't need a central authority. So what if it gets copied? But the double spending is the big issue. So how did he solve it, or she solve it?

Does anybody still not know who Satoshi Nakamoto is? No? All right. I was hoping, I was hoping.

So we talked about blocks of data using cryptography and consensus. So if you're at a dinner party, and you can't remember anything else from this class, [LAUGHS] maybe just remember, oh, yeah, there's something about blocks of data using a bunch of cryptography and consensus. These slides are on Canvas. Download this one slide, you're the expert.

Neha Nerula actually created this slide, and I've been using it a lot. But anybody remember who invented this whole concept of blocks of data? James?

AUDIENCE: Adam someone? Back?

GARY GENSLER: Adam Back is a good name, but he's not the guy that invented this. He invented something else, which was proof-of-work. Timestamp append-only logs-- what's the longest running blockchain in the world?

AUDIENCE: *New York Times?*

GARY GENSLER: *New York Times.*

[INTERPOSING VOICES]

AUDIENCE: Crossword.

GARY GENSLER: All right, here he is. So two Bell Labs scientists-- this is one of them. Two Bell Labs scientists came up with this concept that you could take a bunch of data, put it through what's called a cryptographic hash function, and that's a commitment scheme. You couldn't change it, because if you changed anything, the hash function would change.

So what's a cryptographic hash function? That's when I use this idea of you can take the entire library of Congress, and put it into a little thing called a hash function, and end up with a string of characters, a hexadecimal output. But a hash function is the key to what this guy figured out. And, of course, this. That's the key.

There was only two bits of cryptography in this whole class. And I know that it seemed like, oh, why are we teaching this? But it's this idea that you can take a whole bunch of data, put it into this thing called a hash function, and it commits to it. Because if you change any piece of the data-- any individual piece-- you're going to get a different output.

And so it's really the key to it is that it commits something. You can do it with the *New York Times* crossword puzzle, and that was just my observation on it. So it's about data

commitment.

The other thing that Satoshi Nakamoto used was asymmetric cryptography, or digital signatures. I pulled one of the graphics that we talked about. But the idea being that, long ago, cryptography was, how do I encrypt something because I'm in a military campaign? And I would, maybe, just transpose.

The simplest cryptography from thousands of years ago was transposing every letter. An A becomes a B, a B becomes a C. That would be a transposition of one. Well, that's pretty hard to imagine that anybody got away with that. But that was early cryptography, thousands of years ago-- just simple transposition.

By the mid-20th century, there was very complex transpositions, which were called keys and enigma. If you ever go back and watch that movie *Imitation Games,* there was five metal rotors-- they were electronic rotors-- that changed. And every day, the Germans would change the five rotors. But still, they were symmetric cryptography.

The U boats actually had the same five rotors as high command out of-- Berlin, let's say. So somebody came along in the 1970s and said, what if the key is different? It's asymmetric. There's a private key, and a public key. The public key, everybody gets, but the private key, you keep.

And some of those computer sites-- cryptographers-- are here, right here, at MIT. Ron Rivest teaches a course in cryptography. But that invention, in the 1970s, is really key.

So it's hash functions, and this concept of a private key and a public key, and of course a digital signature that goes with it. You probably don't even need to remember much about this class about this. But just know there's something called a private key and a public key.

And then, Nakamoto's real innovation was off of Adam Back. And Adam Back said, if I use some computational work-- if I use computational work to find a hash function that has a predetermined number of zeros, it's not much of a puzzle. It's a random number generation.

People will say proof-of-work is a computational puzzle. It is simply running-- this thing called mining is running-- electricity until you get the right number of leading zeros. But it can be efficiently verified.

So the characteristics of proof-of-work is of work is-- invented in 1997. Blockchains were

invented in 1991. But what Satoshi Nakamoto-- what she did was she pulled that together after like 20 or 30 failed attempts to have a digital, non-central money and said, that that's where blockchain inspiration is.

And so proof of work-- I use this little visual. But each block-- do you remember what the word nonce is? What's a nonce? Ross? Make me proud, somebody. Can't remember.

AUDIENCE: And once.

GARY GENSLER: What's that?

AUDIENCE: And once.

GARY GENSLER: And once-- a number once.

AUDIENCE: Number used once.

AUDIENCE: Once.

GARY GENSLER: Number used once. And so why is a nonce important for proof of work?

AUDIENCE: Because it's a unique number.

GARY GENSLER: It's a unique number.

AUDIENCE: And so establishing the integrity of that [INAUDIBLE].

GARY GENSLER: So all this whole proof of work-- I'm just going back as a review, but the whole proof of work is your computer is going to randomly keep picking one thing that changes. All the data, all the transactions are the same, but keep changing this thing called a nonce until I get some leading number of zeros.

And the whole Bitcoin network around the globe-- all it's really doing is running a random number generation, or nonces, until the hash function is solved to have 18 leading zeros right now. Or I should say-- 18 leading zeros when Bitcoin's value was $6,500 a Bitcoin. It wouldn't surprise me if it's going to fall down to 17 leading zeros, or 16 leading zeros, because that would make it easier to find.

All of that cryptography is just to make the database structure. This database structure that is in blockchain-- to make this work. All that cryptography of hash functions, digital signatures,

and a little proof of work is to make it what's called nearly immutable. And I'm putting the word "nearly" in because nothing's truly immutable. You could overwhelm even the Bitcoin network. Questions about the technology? [INAUDIBLE].

AUDIENCE: Could you just go over the number of leading zeros concept again?

GARY GENSLER: So the concept behind the proof of work that Adam Back came up with in the late 1990s was-- gotta run some data through a hash function. In his case, in Adam Back's case, it was emails. Literally run an email all the way through a hash function, and then add an additional bit of data to it-- this nonce, a number that's used once-- and run that nonce randomly until the hash that comes out. And my little visual at the bottom there has some leading zeros to it.

AUDIENCE: So beginning of the hash will be its number of zeros?

GARY GENSLER: Yes. So in this case, four leading zeros-- in that little visual there. All the data that goes into a block-- in Bitcoin, 1,000 to 1,500 transactions all go in. They're rolled up in this thing called a Merkle tree, but it all goes in. And the only thing that's changing is the miners are trying to find a random nonce until the hash has certain number of leading zeros.

When Nakamoto wrote the paper, the difficulty was, I think, 10 leading zeros. And you could solve that on a laptop. With eight more leading zeros-- and since it's hexadecimal-- I guess it's 16 to the eighth power harder, or something like seven trillion times harder.

AUDIENCE: Yes.

AUDIENCE: Let's assume that you and I were trying to have a transaction today. And I'm going to keep some coins. And I'm [INAUDIBLE] these for everyone who's transacting many, many times and adding layers of difficulty to the transaction that we had. If I want to use my balance in five years, how do we know what my balance is? I need to go back through all the history to know that I have a balance?

GARY GENSLER: So at the heart of the blockchain technology, the Bitcoin network, but also all the other networks, is the entire transaction history is public. This both gives us its strength, but it's also one of its challenges. And so, yes, even five years from now, if you want to use one of your Bitcoins-- which are stored on the blockchain-- you have to be able to show that here is a transaction output from five years ago.

If you remember, there is both transaction output models-- Bitcoin is a system that keeps all

the individual transactions in a set called the UTXO-- the Unspent Transaction Output Set. You'd have to be able to show that you have that in 25 years, you said? 2023-- in 2023, you'd have to be able to show that.

AUDIENCE: So it's also a balance. They all spent this balance in the transaction [INAUDIBLE] a record.

GARY GENSLER: It is a record of an output from an individual transaction. So yes, it is like a balance. But because Bitcoin does not add up all of those individual-- if you had 13 individual outputs, the Bitcoin network will not add up those 13. You'd have to use each of those individually as new inputs.

AUDIENCE: And that one is on the last block, as well. But I'd have to go back [INAUDIBLE].

GARY GENSLER: All right, so the question is, does the last block-- Bitcoin has 550-some 1,000 blocks of data right now. Does the last block store all of the data? And the answer is, no, but it does store a hash function from the previous block, which stores a hash function from the previous block. So your transaction output might be on block number 420,000, 130,000 blocks ago.

But what shows that it's verifiable is that each one of these blocks are linked to another block through this thing called a commitment scheme called a hash function. So technically speaking, the latest block has a number in it-- a hexadecimal number, but a number in it-- called a hash function that is committed to. Because all the data that's come before it-- all the millions of transactions before it-- if somebody even changes one of them, you'll know that it's been tampered.

AUDIENCE: Let's say I want to use that balance I have. Where do the blockchain verify that I have that? Is it on the last block, or does it go back as long as it finds the [INAUDIBLE]?

GARY GENSLER: In essence, it does both, because the last block better be valid. But for you to spend something, it has to really go back and find that the input that you now want to use is an output that has not yet been spent. Eric, did you have something that you were trying to--

AUDIENCE: Yeah, it was a very nice explanation. You have to go all the way where your transaction-- where you got the Bitcoin was, whatever block it is [INAUDIBLE] through the blockchain. If you would try to get those coins and use them as a [INAUDIBLE] for whatever transaction you want to do, you have to go all the way back.

GARY GENSLER: And this complexity is part of the reason why it doesn't have the same performance-- doesn't

have the same scalability-- yet. I'm one that believes in a-- I'm optimistic that some of these scalability and performance issues will be overcome. But it might take three, five, seven years. And it's not three or seven months. But you're absolutely right, because you have to kind of look back-- way back.

The Ethereum network doesn't just do it on transactions. It has balances. And so it's a little bit more efficient that way, and has other inefficiencies-- many other big inefficiencies, but in some ways it--

We talked about smart contracts. Larry Lessig actually spoke to us also about smart contracts. Nick Szabo wrote about this in 1996. I like to talk about the history to say, it's not all about this one person that we don't know-- Satoshi Nakamoto-- but a set of promises specified in digital form, including protocols, where parties keep their promises.

Think about it as a modern way to automate. So if you're out in business in the future, you're thinking about investing, and somebody raises a smart contract issue. Even if you're a Bitcoin minimalist, you might say, wait, wait, wait. There might be some way I can automate that which is currently done by lawyers, or by back-office folks, or accountants. So there's still something there.

And we talked about a use case where the SDA-- the Swap Derivatives Association-- is looking at smart contracts to try to automate some of the previously written mechanisms. So smart contracts, which have come out of this whole blockchain technology movement, actually predates blockchain technology. But blockchain technology, again, as well-- maybe we can do this in a verifiable, nearly immutable way, as well.

So moving value or automating some forms of contractual arrangement. But remember, they're not so smart, and they're not so much contracts. You probably still need the courts, and there's still some ambiguity that can't be pushed into these documents.

So then, we talked a lot about the economics of blockchain technology. And it's around verification costs and networking costs. But it's about lowering verification costs. And some of those verification costs might just be the economic rents of the current incumbents.

So blockchain technology may be a really important way to lower direct verification costs and deal with censorship. And I think that was a lot of what Nakamoto's innovation was about, was dealing with censorship that somebody could deny me the right to use my money when I want

to use my money. But it could also be about lowering economic rents. Any questions?

And then we said, how do you assess a use case? And this was at the core of even my *CoinDesk* article. Before you get to anything else is, how is it going to be, really? It's what's the value creation proposition? Again, what are the verification and networking costs that are really going to be reduced? And what are competitors doing?

With a keen eye on-- in trade finance, there's 20 or 30 efforts, so it's worthwhile looking at those 20 or 30. I don't know which field you all go into, but if you're in a field where nobody has used blockchain technology, no competitor, then ask the question, well, how are competitors using traditional databases? And that might be the opportunity for you. And it might be a golden opportunity.

But always look-- what's the value proposition? What verification and networking cost? What's the competition? And then, you get into the sort of tough details. And if you're investing, if you're a venture capitalist and somebody can't really tell you why multiple stakeholders need to write to the ledger, and what's their data-- what data are they going to be storing on this append-only log-- then I might suggest you invest in something else. I mean, you can always invest in something because you think that it's a momentum play.

And if you invest, it's an early seed investment, and somebody will bail you out. But most venture capitalists-- you're investing for three to six years, or three to five years. And so I wouldn't always expect somebody is going to bail you out. Ask the tough questions. Jihee?

AUDIENCE: But just because that is the best solution, it doesn't mean that they're going to be successful later, right? There are multiple examples of products, or services, or [INAUDIBLE] that are clearly not the best solution but have taken dominant position in a market. So I was curious, should it be the best solution?

GARY GENSLER: Well, I think that's one of the questions. But you're saying, well, what if it's not the best solution? Going back to what Jeff Sprecher said, can it do something cheaper, faster, or better? And it might not be the best solution. But if it can at least answer the question, is it cheaper, better, or faster, you're probably not going to be successful.

And in some cases, it's not the best data solution, but there's such high economic rents that however the mortgage product, the health care product, the product that is being delivered now, the payment solution that you're saying, ah, it's not the best solution.

But this is my solution on how I'm going to do it cheaper, because they have so many economic rents. So maybe that the word should say, why is this a better solution, rather than best solution. I'll agree with that. Other queries?

And then, if there's a native token, I think that's where you start to lose May. But now, I'm going to ask the class. How many people have come out of this semester thinking there's a lot of initial coin offerings that you'd want to personally invest in?

[LAUGHTER]

All right, is there anybody in the class that owns an initial coin offering-- a non-Bitcoin token? OK, do you want to tell us why?

AUDIENCE: Yeah.

GARY GENSLER: Give us the value proposition, or the pitch.

AUDIENCE: So I went to work for a startup, [INAUDIBLE] this summer. And after the summer, they paid me US dollars. But after the summer, they gave me a lot of tokens they have. And I saved a little bit of them.

GARY GENSLER: All right. So you got paid in tokens.

AUDIENCE: No, I was paid in US dollars. After the summer, they gave me most of the-- like a bunch of-- some of the tokens.

GARY GENSLER: As a bonus or?

AUDIENCE: As a bonus, yeah.

GARY GENSLER: I see. As a bonus, you got-- all right. And you sold some of them?

AUDIENCE: Some of them, sold them.

GARY GENSLER: And I see.

AUDIENCE: Some of them I still [INAUDIBLE].

GARY GENSLER: All right. And do you think that there's a use for these native tokens?

AUDIENCE: This specific startup?

GARY GENSLER: Yeah. Names will not be repeated. It's being filmed.

AUDIENCE: I don't know.

GARY GENSLER: I don't know. Sean.

AUDIENCE: So I thought of it-- well, I just thought a little of like Tron, which is a--

GARY GENSLER: Tron.

AUDIENCE: Yeah, it's a gaming.

GARY GENSLER: Gaming site.

AUDIENCE: Which is a-- basically a company started by a friend of mine. So it's kind of a token of support instead of like [INAUDIBLE].

GARY GENSLER: All right. So you bought some tokens as a token of support for a friend, who started a company. Do you think they have some use? Can you use the token?

AUDIENCE: I don't think there's-- well--

[LAUGHTER]

Well, it's supposed to be the-- building up to the biggest gaming network [INAUDIBLE].

GARY GENSLER: But is it pre-functional, or is it functional? It's pre-functional. Hugo?

AUDIENCE: Yeah.

GARY GENSLER: You have-- you are?

AUDIENCE: I have-- yeah.

GARY GENSLER: All right. You don't-- all right. He's got a whole portfolio. I can tell.

AUDIENCE: I don't know. I've been interested in this for over a year now. So I wanted to make a whole radical of like, oh, this one looks like it's going to go well, but this one's a scam. And there are some that seem like sure-- in the long run, they may retain some value. But I probably made some bad investments.

GARY GENSLER: Right. So I don't want to make you sort of grieve those bad investment decisions, but are any of your tokens that you have held or hold currently-- are any of them functional? Like, they can be used on a network?

AUDIENCE: Yeah. And I actually use at least one of them.

GARY GENSLER: All right. Here. Are you an owner, or you've got a question?

AUDIENCE: I'm an owner, but not-- I haven't voted. Both the tokens-- I'm mining the tokens. But in any case, I wouldn't disregard maybe tokens that's a valid way of generating a means to jumpstart a network and create some sort of valid way to drive collective action for some disintermediation effort, because I mean I-- and I think it's a little bit unfair to ask if we kind of join or support ICOs in the context of there's huge amount of scams that are [INAUDIBLE] right now in the media. But I wouldn't disregard the whole concept of tokens here.

GARY GENSLER: [INAUDIBLE]. I admit it might have been an unfair question. I was just trying to get-- I was just trying to get some support in the room for tokens.

AUDIENCE: The concept for me is absolutely valid. I would explore, seriously explore-- if I launch a startup in the blockchain space, seriously explore the possibility of using maybe tokens in the permissionless environment. So I suppose the permission--

GARY GENSLER: So I think that there is definitely a future in this overall technology of making a database harder to tamper with, more immutable on a scale, maybe not 100% immutable, but closer to that immutable and inverifiable. I think that native tokens could help jump start a network. What I think the challenge is I think the challenge is, how do you compete with fiat currency that has such extraordinary network effects?

So the Ernst & Young study, the recent study, I think captures this a bit when they looked at the 140 largest ICOs from 2017. Only about I think it was 17 of 140 have a functioning network right now, where you can use the token, 13%. But of those 17, I think seven of them, the networks that are live, instead of, well, guess what, we'll also take fiat currency for this service that we're providing, whether they're providing file storage or something else.

So they definitely used a native token to jumpstart the network as a crowdfunding, but then when they got to the later functional stage, the operator, the entrepreneur says, I don't want to limit my users. I'm going to also take fiat currency to buy or secure whatever service I'm having. And I think that's the business model challenge.

And it may well be that there are networks, just like in gaming sites, where you want skins or shields, and there's something about only trading those tokens. But to date, that's been a limited class. That's where I probably will declare myself.

I think, of course, there's a bunch of tradeoffs over the next three to seven years that will be sorted out around performance, privacy, security. We talked about layer 2. If any of you are actually interested in work in the blockchain technology field, you're going to learn a lot about layer 2 solutions and side chains and all the performance scalability things that colleagues over at the Digital Currency Initiative are spending a lot of time on this question right here.

And then, of course, this is a business model. Just purely as a venture capitalist, you have to think about, how do I get adoption? How do-- what's my customer user interface? I'm sure, Iman, you're thinking a lot about this, right? You could have the best idea on a data structure.

You could have a really nifty idea on a native token. But you still have to deal with whatever venture capitalist has to do is, how do I get users to use this? Adoption. What's my UI? And it's sort of a much more generic set of issues. Iman.

AUDIENCE: That was my answer to Jihee. She's totally right. It's all about-- it's a tension between adoption and quality of product. And that's why we moved from Ethereum to the public blockchain. But we didn't think that it will be mass adopt by-- massively adopted by the incumbents. So we moved to a permission blockchain because of the adoption.

GARY GENSLER: And I can't remember if you're able to say. Which are you using-- Hyperledger Fabric or Corda or?

AUDIENCE: We're using Corda because of the state channels solution that they provide.

GARY GENSLER: So we talked about frameworks. Over time, it's my thought that that orange line, the slope of that will come down, and we'll move more towards the decentralized side. But for the orange line, the slope to come down, in essence, the costs of the scalability, security, even the coordination needs to come down. It's always going to be some challenge on governance.

In essence, who is going to pay for the software development in a truly decentralized network? And Bitcoin has been supported, for instance, by, really, an incredible group of Bitcoin Core developers, in part because they just believe in it, in part that some are funded by institutions like MIT.

But it's still-- it's always a challenge in a truly decentralized space. Who's going to fund-- who's got the economic interest to fund the continued updates and software? I think Uber could be completely a decentralized network. And probably, drivers would get paid more. But then where would be the incentive? Who would work on the software development to update their ride app? So there's a key tradeoff there.

The financial sector-- well, it moves and allocates money and risk. We talked about that. But it relies on a system of ledgers, and it's always had a symbiotic relationship with technology. The opportunities-- these are the key opportunities, which I think any thought fintech-- it's not just blockchain but even AI and machine learning-- has around finances.

The customer interfaces-- there's a lot of legacy customer interfaces that you can actually compete with, if you're doing a startup. The economic rents are high. There's 7 and 1/2 percent of the economy is finance. Not all of the 7 and 1/2 percent is rents, but there is a lot of extra-- excuse the expression-- a lot of extra vig or juice in that model.

And, of course, we've had repeated crises and instability. And financial inclusion-- we talked about products like Alipay and M-Pesa that were really about financial inclusion using new technologies.

So what are the technologies in our time? I just put up a nice little graphic here. I'm doing some work with a group called FinTech at CSAIL, the Computer Science and AI Lab here. And when we leave with the funding companies, the big funding companies of that unit over there, blockchain is on their list, but it's not number one.

To just put it in context, in terms of their technologies, they're thinking about machine learning and AI would probably be the biggest piece. But just to give a flavor for-- but it's one of the top three or four.

But as we've talked about, they have challenges. The financial sector sees a lot of challenges.

AUDIENCE: I just want to go back to previous slides, and how would the virtual reality impact finance? I'm not sure. [INAUDIBLE].

GARY GENSLER: That has happened--

AUDIENCE: AR and VR, [INAUDIBLE] tech, finance.

GARY GENSLER: I'm not familiar with the projects in that space. But where-- and I'm sure I'm getting now, you're going to inspire me to do some research in the next day or two to shoot your email with some projects. But virtual reality and hearing it does allow for more financial inclusion. And the question really is, can you just, rather-- think of the user experience. If you can find an enjoyable way to spend more money through virtual reality, the banking system wants to tap into that.

It's not one of the top things at FinTech at CSAIL, I'd say AI, machine learning, biometrics, and blockchain. Everything's in the cloud, so they're not asking, right now, MIT to help them with cloud issues.

Open API is a really big issue, particularly in London and in the UK, where it's been regulated that the banks need to use Open API. So I'd say AR and virtual reality is probably eighth on the list there. And I just include it, because I kind of think it's-- they'll find a way to change a user interface.

We talked about there's a bunch of issues, and that's really leading to the use. We talked about traditional databases, which-- where parties can just create, read, write, the ledger, the private blockchain, which, of course, is what most of trade finance, most of payments, all the big central banks that have looked at it or moved from Ethereum to doing Hyperledger projects-- Singapore and Canada's Jasper-- and maybe permissionless.

But the finance is really in the second bucket right now. Eric, it's not to say that native tokens won't take off and, Hugo, that your portfolio will be worth something, maybe. So here, we went through a bunch of use cases. But the biggest use case so far has been the $20 to $30 billion that's been raised through ICOs.

I personally think that's going to come down, way down. But payment systems-- I mean we might differ on the views of XRP, a token, but Ripple and other companies have done a lot to try to be a catalyst for change and payment systems. We talked a lot about trade finance. Again, they're more in the permissions than the permissionless.

Clearing and settling-- what's going on in Australia. Again, permissionless, not-- I mean permissioned, not permissionless. And then some of the non-financial-- had a lively discussion about supply chain management, and James, I'll forever remember that you're not a fan of it. But Walmart and Cargo might disagree with James. And they have active projects on it.

And Lauren gave-- where's Lauren? She's here, maybe-- gave a reason why in supply chain sustainability that you might be on the other side. Digital ID was the last thing we talked about. So there's a lot going on, and when there's $20 or $30 billion raised, there's going to be-- these projects will have some life to them. We'll learn a lot from them along the way.

Crypto finance-- when I first put this slide up, it wasn't $110 billion. And gosh knows I did this yesterday, so I don't even know what it is today. Pretty volatile market. Interestingly, Bitcoin staggered about 55% or 57% of the market. So there's a high correlation, though Ethereum slid, and XRP is number two in that market since we first got together in September.

Here, what I think the challenge is, as an investor-- I'm not trying to pick on you, Hugo, but you know, an investor. But I think that's the number one challenge. I really do. What's the viability of that token? And Eric, I'll agree with you. Some tokens will be worth something. But it's assessing that. But the markets are readily susceptible to fraud.

How do I keep custody for the private key? Fidelity has announced they're going to have a new private key solution, so it's interesting that big incumbents are coming in. It's not just the Zappos and the early stage custody solutions.

Even Backed, the Intercontinental Exchange, has put a lot of money into it. And they'll, in essence, have a custody solution, because you could buy Bitcoin, one day futures, have a Bitcoin, and then they would, in essence, hold custody for you.

And then we talked about crypto exchanges. And the key thing-- and if you take anything away about exchanges, other than right now they're unregulated and they're probably highly susceptible to front running and manipulation, is that they're a little bit different, because they're not just matching agents, which the London Stock Exchange or the New York Stock Exchange are [INAUDIBLE], but they also are counterparties and custodians.

The other thing to take away about crypto exchanges is they're highly centralized. So it's a central irony that Satoshi Nakamoto is trying to have decentralization, and yet there's an awful lot of centralization. So I'm just thinking about core takeaways.

If you're ever investing, or you're thinking about this, or you're just involved in a dinner party conversation, that central irony in a decentralized space, 95% of the real transactions are happening on crypto exchanges. My thought about crypto exchanges-- they'll not be 200 of them that much longer either.

We talked about Initial Coin Offerings. Central takeaway is they're fundraising vehicles. Whether you believe in or not believe in the US and Canadian approach under the Howey Test, but they help build a network, raise money in anticipation the tokens are issued before it's functional. I think the latest study was that-- what was it-- 1 and 1/2 percent are actually functional, and 98 and 1/2 percent are issued pre-functional.

So that's not a problem. It's just-- that's the-- means it's probably an investment vehicle, not a utility token. And that whole thing about utility token versus security tokens, it stretched pretty darn thin.

We talked about public policy frameworks, guarding against illicit activity, financial stability, investing public. My overall thought on this-- and I accept that others will have other views-- is that any new technology, if it grows to be economy-wide, needs to live within public policy frameworks, or society will change those public policy frameworks modestly. But you still want to protect the public against core social goods.

It happened when the railroad came along. It happened when telegram came along in the 19th century. It happened with the internet. Societies don't have technologies fully outside of whatever social fabric we want to create. And we do that social fabric stuff through politics and parliaments and executives and regulators. But we don't leave big parts of our economy outside of it.

This stuff is still small. It's $100 billion. The worldwide capital markets are over $300 trillion. But it's gained a lot of public attention. And particularly, we want to guard against illicit activity. Most folks do. Maybe not everybody. But most do. No, I recognize. Hopefully, you all do. Well, I don't know.

So we talked about the US Securities Law, the Howey Test. It's not-- if you forget the Howey Test, it's totally fine. But it's core to these initial coin offerings, and it was that four-part test-- investment of money in a common enterprise, expectation of profits. So if you get into some debate, and you want to have some fun with somebody, you can say you know the Howey Test.

But it's really more this. I prefer the Duck Test. Just use common sense. This course has been more about critical reasoning skills than anything. So if somebody's trying to sell you something or hustle you on something, and you are now a venture capitalist, and you're

investing, use the Duck Test. You can even remember the Duck Test about whether they're trying to sell you something, and it has nothing to do with the law.

It just-- so where do I think crypto exchanges will go? I think that they'll have to fix this whole custodial duty stuff. They might all use Fidelity's product. Or they'll keep it in-house or spin it off. I think they'll have to start complying with any money laundering. We saw one study that said a quarter of all exchanges don't even have any AML. I think two years from now, that will be way down.

I think margins will compress, and I don't think there'll be 200 exchanges two or three years from now. There'll be five or 10 relevant exchanges at some point in time.

On Initial Coin Offerings, I think we're going to keep seeing a high failure rate. There's still about 200 a month, but there'll probably be fewer of them. I think that there's going to be a lot of enforcement actions. Occasionally, you'll see something-- the Securities and Exchange Commission or some other-- maybe it will be in Japan or elsewhere will be bringing more cases.

And what will be interesting in 2019 is to watch, does any of the big ones go live? And I think this will be a real test. Does Filecoin figure out what to do? They raised a quarter of a billion dollars. Telegram raised $1.7 billion. Do they figure out what to do and make a real live effort in 2019? And it will test the economics.

And by the way, Eric, it might pull me more towards where you are, right? I mean Telegram's-- they got a lot of smart folks over there working on this. And by the way, Facebook has advertisements out hiring people on blockchain technology. So there's a lot of very big tech companies hiring and recruiting in this space.

But I think 2019 will be interesting to see, what does-- what is Telegram? What is Filecoin? What do some of the big, hopefully, well-meaning companies do with these tokens? Central banks-- mostly in the monitor phase. But I'd say the thing to watch is Sweden. It'll be really interesting what they do with their E-krona project. Do they go live and say, inspired by blockchain?

The E-krona project is not blockchain technology, but it's completely inspired by Satoshi Nakamoto saying, well, we, the central bank, Jihee's the central bank says, we're going to do what Satoshi Nakamoto's-- we're going to have a central bank digital token. You can use it at

Starbucks. You can use it wherever. I'd watch that. I think Venezuela will probably fail on the other end. But it'll be interesting. There might be some distressed country that does something.

So how would I conclude? I think blockchain does-- this is my disclosure. I think it does provide a real peer-to-peer alternative. I think it's a legit live application. It might not be the best, but is it better than some others? Is it something you could use? Verification and networking cost-- I'm going to repeat on that-- is the key. But you always, I think, have to assess, is it the right use case? Is this use case the right use case?

But as we've talked, I think there are real use cases more in permissioned than permissionless. Remember anything. Money is just-- we all humans, the 7 billion of us that live now, have to thank somebody about 10,000 years ago, but came up with this technology called money.

Store value, medium of exchange, unit of account-- it's just a social construct, which is a reason why I say, we could have a social construct that is decentralized money. I absolutely believe we could have that.

But we'd all have to accept it. Where I have less optimism is that you'd want to accept it for a closed, bounded ecosystem only for file storage. That's where I'm a little challenged as to, what is the real economics of that?

Financial sector's characteristics and challenges-- is it good? It's fertile ground, because finance is built on ledgers. And finance is big-- 7 and 1/2 percent of our economy. And around the globe, it's anywhere from 5% to probably 8% of those economies.

Most other countries, it's less than the US, but it's still-- it's big. Incumbents are, of course, looking at permissioned blockchains. And unfortunately, crypto finance has a bunch of scams and frauds. And that hurts the development.

But I think adoption will come, but it rests on solving a bunch of technical issues, like the Digital Currency Initiative's trying to solve. What are the commercial use cases and the public policy? I wouldn't lead with public policy. I don't think that's the main issue here. But if this is ever going to be anything, it's got to get over that.

So mostly, it's probably going to be a catalyst for change, more than actual real thoughts. Questions? Thoughts? Eric.

AUDIENCE: On the third point, I--

GARY GENSLER: Use cases must address why versus a traditional database.

AUDIENCE: I always had the feeling that it seemed the permissioned space, where you have the most or the biggest urge to prove where-- if your submission needs a blockchain solution as opposed to a traditional-- I mean making a case against the centralized database is kind of easy, versus a distributed database. I think it's a little bit tough.

But in the permissionless space, I think you don't have to struggle much, because it's absolutely justified that you can-- because you're dealing with a decentralized configuration, where there's no one in charge of guaranteeing that we have a--

GARY GENSLER: So Eric's raising the question, why not use a traditional database? Why ever use a permissioned--

AUDIENCE: In the permissioned space, because permissionless is perfectly justified. But in the permissioned space, I'm not saying it's not justified. The point is being that in our project, we argued for a permissioned system. We made some justifications in that space, so the point is that I just wanted to get your thoughts so that in the permissionless spaces, you don't have to struggle much in that.

GARY GENSLER: Permissionless blockchain technology, looking forward a number of years, looking forward to when some of the scalability and performance gets better, can give you verification costs. And it's censorship-resistant or practically censorship-resistant, unless somebody does a 51% attack. But so I think that the truly decentralized distributed permissionless system has a lot of-- a lot to offer.

But it comes with a lot of costs, too, and challenges-- hard to do the governance and hard to get coordinated action. And as you've heard me say, I think there's only probably going to be a very limited use cases for native tokens, native product-specific tokens like a Filecoin or a restaurant review coin or a health care coin.

I have-- I have my doubts about that. An economy-wide coin, a cryptocurrency like Bitcoin-- I think there's more use, particularly if you have a weak central bank, a weak fiscal policy. A country like Venezuela in the future might adopt something. I think there's a lot to be said for permissionless, but permissioned systems versus traditional databases, I think, also gives

something.

And I'll use the Australian stock exchange for one, but they know their customers. They know they have-- I think the number was 77 members. They can take their database and decentralize it and put it on all 77 member companies, if that's the right number, and say, you're now sharing that. And so then there's no single point of failure, and we can lower what's called reconciliation costs, because you all needed some of that data anyway.

The historic data-keeping, the historic nature of it came up with each of those 77 members having individual databases. So I could see that there is a real benefit in probably efficiency and lowering costs, which means lowering costs of verification, lowering networking costs, because there's 77 members, trade finance. I could see some of that as well. So that-- but you might be right. Oracle might be able to just adopt that in a traditional database. Sabrina.

AUDIENCE: Yeah, so it seems like you're describing that they have some form of distributed consensus. And that's the main reason, right? But there's--

GARY GENSLER: And distributed the data stored on multiple nodes, because it's multiple copies of the same data.

AUDIENCE: Right, but yeah. There's-- I mean if that still can be implemented without watching. I'm playing the Aleem today, since he's not here. But there's no--

GARY GENSLER: No, but we--

AUDIENCE: That's been a long solved problem of how consensus algorithms that-- or you can replicate state on the same state on both the machines and tolerate some [INAUDIBLE] number of failures. So I personally don't really see the use of blockchain in permissioned systems, but I do see a lot of potential for permissionless systems, just because those algorithms already exist out there to do [INAUDIBLE].

GARY GENSLER: So what Sabrina's raising-- you can take the Sabrina seat. You're-- Sabrina's a master's student at computer science at MIT, so she probably knows what she's talking about-- is really saying, well, you can do a lot of that. You can have distributed databases without blockchain technology.

You can have-- and there's ways that this Byzantine-fought tolerance has been addressed in distributed databases that you don't need blockchain technology. The concept of a block,

commitment hash, block, a commitment hash, block technology.

And I accept that. But I'm not going to accept it to say that there's no space for permissioned blockchain technology. What there is space for is the 80 of you in this room to have different opinions on all of this. You want to close out? I want to-- I have one more slide I want to--

AUDIENCE: [INAUDIBLE]

GARY GENSLER: So this is, of course, about money, so I went back and found a quote from Benjamin Franklin that I like. And to me, it's about a concept that I hope you all live by. It's paying it forward. Paying forward is partly because all of us in this room are privileged. We're at MIT or Harvard or Wellesley, but we're at MIT.

And so what did Ben Franklin say? And it does close on money. "I do not pretend to give such a deed. I only lend it to you. When you meet another honest man in similar distress, you must pay me by lending this sum to him and joining him to discharge the debt by a like operation," paying it forward, basically. "He should be able and shall meet another opportunity, I hope, that this may, though many hands."

So Benjamin Franklin, over 200 years ago, he closes, this is a trick of mine of doing a deal good with a little money.