GARY GENSLER: So we're going to come back again today to blockchain economics. A lot of what we're going to talk about today while again anchored in the readings will also be relevant as we now turn to after Sip week to act three where we're going through use cases but also hopefully relevant as you're starting to think, OK, what about this final project and so forth and what do we need to do?

Five or six of the groups have come in either as an individual person or teams of three or four have come in and bounced ideas off of me. So I want to thank all of the groups that have come in, because you've helped me also organize some of my talking points for today as to what we're going through. And those of you who haven't come in, feel free to set things up if you find it helpful. It's not mandatory. But you can also thank the six groups that have come in, because now I'm trying to anticipate your questions as well along the way.

So, the overview of course our reading and study questions will come through. There was the letter to Jamie Dimon. So we're going to dive into that one a little bit. I found it interesting when I read it about a year ago. And then I thought, why not throw it into to the mix here?

The McKinsey report, which, again, I found this to be true for years. It's not just this class that you can find some consultant that's put a generalized paper out, it does sort of just skim the tops, but you're getting a sense of how they're trying to gin up business.

Their business model is to write some of these reports. And some of you are going to go into consulting and maybe even write these reports at some point in time. But it's often a good way to see what I'll call it just a survey, a topical survey in how folks think about things.

Quickly a little bit on potential use cases. In the heart of today's discussion and kind of the heart for thinking about the final projects is how to really assess the costs and benefits of any potential use case. So I'll skip through the study questions. But these are the key.

I didn't see anybody go in the discussion board. I looked. Did you see anything there? No. we did set it up. But what are the potential benefits, and how do you assess the cost of trusts? And that is going to be true in every single project you look at. If you take anything from this class, it's this core critical reasoning of like-- and hopefully after the Roubini paper last Tuesday, we're going to come out of the doldrums and we're going to pull back out of the minimalist side and get more in the middle. I might not get Alin lean out of the minimalist side, I don't know.

But it's interesting. Some groups come in and I find the three or four people that are sitting there I ask. In and even amongst the group, there's somebody who's a maximalist and somebody who's a minimalist. So I think we're being successful that we're not going to come out all in the same place.

So, of course, since we're going to talk about the reading, let's jumped through, a letter to Jamie Dimon. Anybody want to tell me what you took from that letter?

AUDIENCE: I really loved this article. It is my favorite reading so far.

GARY GENSLER: Oh my gosh, 12 classes. All right.

AUDIENCE: So I though that he really great job of stripping some of the hyperbole, both the maximalist and the minimalist hyperbole surrounding this out of it to lean on really what it is and a very good explanation of how it works. And then also, the note of caution to see if these are the dimensions around which-- you should wait til you put a word in, but these are the reasons why there's potentially big implications.

GARY GENSLER: Right. And he wants to add to it. I'm going to hold-- there was a hand before Alin?

AUDIENCE: Yeah, no. I actually was going to say something similar. But I thought he highlighted a lot the trade-off between trust and the decentralized properties of blockchain versus the cost you must be willing to pay.

GARY GENSLER: And remind me your first name.

AUDIENCE: Leonardo.

GARY GENSLER: Leonardo. All right.

AUDIENCE: I agree with both of them. Also, very good writing and style. One thing that I didn't like is that at some point, he raised the question, well, who needs censorship resistance? Because it seems like this is the only benefit of these decentralized applications. And he didn't answer that question actually. He just gave two vague broad answers, but didn't answer that question. So I think that's a really good question. Who needs this stuff, anyway?

GARY GENSLER: All right. Censorship resistance. We're going to come back to it. Stephanie.

AUDIENCE: Yeah. So actually, I thought censorship resistance was also one of the more interesting parts of this letter. Because to me, when you read through what they highlighted that Jamie Dimon had said, one of the things was people who use Bitcoin or Blockchain are criminals. And I didn't find that his focus on censorship resistance really rebutted Jamie Dimon's argument.

GARY GENSLER: So-- Sean.

AUDIENCE: Oh, I think that censorship resistance is really interested in a way that now I actually almost feel why we spend so much time and energy on trying to understand public policy or why is public policy such a big thing in response to decentralized apps. I think this is a key question.

GARY GENSLER: So I think of--

AUDIENCE: I just wanted to-- well, I definitely agree. Because that was one of Dimon's points, that, well, yeah, if you're a criminal, this could be useful. And then he talked about how it's worse than a lot of aspects except censorship resistance. But I think the analogy he used was the rise in encrypted messaging that has just become-- it wasn't really predictable that that would be such a big thing, but now that's gotten use cases in the world.

GARY GENSLER: So it seems like people really like the writing, not just the style but that it took on and had a balanced approach. But you're highlighting, wait a minute, he ends with censorship resistance, but then doesn't take it the next way. Like, what does that mean? And so I think we're going to try to tease that out a little bit, but I think of it as in two ways. It's the individual. Any one of us could be blocked from doing something. We could not get a service, we could not be allowed to take credit if somebody is allocating credit. Think about Uber. If Uber were censoring, we can't get a ride any longer. How many of us rate everybody a five when we ride our Ubers because we think, well, maybe they'll pick me up. If I rated everybody a three, maybe they'll censor me.

I don't know, but maybe you all give more legitimate feedback. I just hit five. So it's the individual censorship, but I think of it as a second thing also, is barriers to entry, a commercial more broad market barrier. And that in some ways, the blockchain technology might allow to build something where incumbents already have barriers to entry. They might have used public policy to get the barriers, by the way. They might have regulatory barriers as well. But more specifically, he did define-- it was kind of interesting-- crypto assets. And he was one that-- I'm trying to remember the gentleman who wrote it because it was on Chain. It was the head of Chain. What's that?

AUDIENCE: Adam Ludwin.

GARY GENSLER: Adam Ludwin. But he too said, let's not use the word cryptocurrency. Let's use the word crypto assets. They enable a decentralized application. And that was a key thing he was trying to say to Jamie Dimon. It depends on how much you believe in decentralized applications. If you don't see a value in decentralized applications, Ludwin, said, all right, I get it, I'll agree with you, Mr. Dimon. But there is a benefit for decentralized applications and a mechanism to allocate resources to a specific organization. So some incentive way, some way to allocate resources.

I would say this. We've studied money a lot this semester, the medium of exchange, unit of a cat, store of value. But it's also possible that these crypto assets have some other benefit, that they're not really truly competing with the US dollar or competing with the Euro, but maybe they're competing with-- who's my friend who's the gamer over here? Skins, yeah. What's your name again?

AUDIENCE: Mike.

GARY GENSLER: Mike. I'm going to be always looking to my right for the-- but it could be an incentive and be competing with skins, in a sense. And so I took that, that, Mr. Dimon, don't think of it only versus the Euro or the Dollar because maybe you're right. But it could have something to do with decentralized applications. Kelly.

AUDIENCE: To add to that, Bitcoin is capitalism still. He should love it.

GARY GENSLER: That you should still love Bitcoin and capitalism, and that the banks aren't going away. They will probably still have banks.

AUDIENCE: It is incredible that he didn't use the word blockchain till the very end to asterisk and say, you'll notice I don't use blockchain, and I thought kind of a genius way to separate [INAUDIBLE].

GARY GENSLER: Right. I'm not as genius as him because the whole course is called Blockchain and Money.

[LAUGHTER]

Oh, well. So what are decentralized applications, at least in this write-up? Anybody? Kelly?

AUDIENCE: Basically, it just says it allows you [INAUDIBLE] but without the trust part.

GARY GENSLER: So you don't need a centralized trusted party. That's what in the 1990s so many people tried and failed with, in a sense. And the internet became this way, in a decentralized way, to distribute packets of information, even though there is centralization on the internet as well, as we discussed Tuesday and so forth. But this decentralized application-- so in this context, he was using it broader than just something built on top of Ethereum through smart contracts. Because he even said Bitcoin was a decentralized application. So he was using it in the broader context, not in what some people would call dapps. But a new model for creating financing operating software.

And this is what Christian Catalini wrote about as well, that it might be that there's a new way to finance a software development. Maybe raise some money for the file sharing before you have the file sharing. Might be an incentive system as well. And then he talked about two structural trade-offs from the design. Now, this blockchain design has a lot of complexity. It has a lot of additional cost, whether it's mining costs for proof of work or some other cost to basically secure the data. And so there has to be a trade-off. And what can pull you out of the minimalist end of this is whether there's some benefits as well. And we're going to chat about that in five or 10 minutes again.

And then the censorship resistance. These are my words, not his. I really do think it's the individual censorship, but also, what I'll broadly call the market. Are there barriers to entry in the current system that are, in essence, censoring economic activity broadly, not individually? And I think, though, that was not how he defined it-- and I agree with Alin. It would have been great if he had written a few more paragraphs or another page. But I think it's not just the individual, it's some barriers to entry for whole market structures. And often, centralized institutions, because they have such a networking effect, it's hard to break in when somebody is basically the hub of a hub and spokes network for almost anything.

How do you topple Facebook at this point in time? Because it can censor other market activity, as an example. So then we had the McKinsey report. Anything that people took from yet one more survey paper that you've had? Akira? It's just because I can see your name on the board there.

AUDIENCE: From [INAUDIBLE], I found the use case [INAUDIBLE] use case to be [INAUDIBLE]. And one thing I found interesting is the switching costs. Because the incumbent financial institutions have to think about not only the benefit of the cost reduction, but also, we have to think about [INAUDIBLE] costs, existing infrastructure, a lot of the affect on the people watching [INAUDIBLE].

GARY GENSLER: So Akira's raised a very important thing about switching costs. And we wrote about this, even though I'm not detailing it again, in the joint paper that Simon, Johnson, and Nihon, and Michael, and Joan, and I wrote. Now, this the last time-- it's the third time you had to come back and supposedly read a little bit more of the Geneva Report. But we talked there about the switching cost as well. And by the way, to Alin's question from Tuesday about interoperability, a lot of switching costs relate to interoperability. If you're an institution and you're thinking about putting in place some blockchain solution, permissioned or permissionless, but how does it communicate with the existing network?

If the Australian stock exchange is putting in a new back end clearing and settlement system on a blockchain-- and they are and they're using digital asset holding-- they have to think about, well, all of our customers are currently communicating with a legacy database system. And now we're creating a blockchain system. How does that communicate? How does the old system literally move information over into the new system? And all of those from a business perspective are a question of how do you operate or interoperate with the legacy system and all the network. Because any blockchain solution that you're going to come up with is likely to be replacing some other economic activity, and likely, you're not going to try to replace the entire network. You're going to be surgical.

You're going to decide-- I'm not trying to give anything, Eric, but can I say what you all are talking about it in your final project? You have intellectual property, so I don't know if you wanted to share it. But do you want to say what--

AUDIENCE: Could you elaborate a little more? In the point we were discussing, I was kind of lost.

GARY GENSLER: Well, so Eric's group-- and Brotish, and Catalina, and Ross-- are talking about maybe doing a permissioned blockchain application for credit reports. Not credit reports for the commercial side, but consumer credit. Basically, an-- uh-oh, Alf. Are you competing with them? Did I just--

AUDIENCE: No, no.

GARY GENSLER: OK. All right. Maybe you are, so I shouldn't say much more. No, it's all right. But I won't say anything more.

AUDIENCE: Maybe it would be interesting to point out the fundamental-- or one of the interesting things that comes up from the discussion of the topic we're engaging is how to approach a blockchain solution from an entrepreneurial perspective. Going back to the letter to--

GARY GENSLER: Jamie Dimon.

AUDIENCE: To Jamie Dimon reading, we're trying to get rid of intermediaries or getting economic rents with that differing kind of paradigm that justifies the costs of using a blockchain approach to promote [INAUDIBLE]. But from an entrepreneurial point of view, you would end up trying to get some benefit from that kind of implementation. So you don't want to replace intermediaries with another intermediary. So you would have to be really creative in terms of how to come up with really lowering costs and gaining some profits in the process.

GARY GENSLER: So Eric's raising that if you're just replacing one intermediary with another intermediary, will you be successful as an entrepreneur? Yes, if you're providing a better service or a lower cost structure, lower economic rents. So I wouldn't doubt yourself. I would say, we might be able to do it. In your use case-- and apologies, maybe it's multiple use-- maybe it's two or three groups thinking about it. There's a lot of market power right now, and thus a lot of economic rents, but a lot of market power and economic rents and credit reporting. Equifax, First Union, and others earn a certain fees for all of those FICA scores.

In the US, we use this. If you're getting a job, somebody runs a credit report on you. If you're buying an automobile and taking out an auto loan. It feels like each of us probably have a credit report pulled on us multiple times a year. Sometimes we don't even know it. But back to interoperability and switching costs, just to pull it all together. How could you convince the commercial banks to use-- I'll call it Eric's project, it's four people, but how could you convince all the banks to use their project and how about all the auto dealerships on the other side who right now are very comfortable using First Union?

Everybody's probably paying a little bit extra. And there's a fat market power, economic rents. And so that's part of the switching costs that Akira mentioned. And to the interoperability, I believe they'll be more successful if they don't try to completely change how data flows, that at some point you need to know that you can't be successful by biting off too much all at once. I'm sorry, Catalina.

AUDIENCE: I was going to say that, precisely, that is one of the forms of blockchain he raised in the paper. And it's not changing one intermediary for another. Financially, what they say is that he's going to be more successful for-- blockchain's going to be more successful in the permissioned than in the permissionless because the incumbents are more willing to work on the permissioned than with the permissionless.

GARY GENSLER: In essence, Catalina is saying you might be more successful not trying to disrupt the entire community, whatever that community in some ecosystem, some business community, and do it in a permissioned versus permissionless. But we're going to play with that a little longer. Kelly.

AUDIENCE: I feel like they addressed the timeline of where the strategic value is. For example, they said, currently the best way to reap the benefits from blockchain are to focus on this, this, and this. And then they say, however, feasibility at scale, they say, is probably three to five years away, exactly what you've been saying. So--

GARY GENSLER: Oh, my god. We could both be wrong. All right. Jack.

AUDIENCE: Something else I found interesting. There's a lot of talk right now about robotics and supply chain using blockchain. And the McKinsey report kind of touched on that. No matter how secure the blockchain is, when you start involving actual real products and assets, it could be completely corrupted, even if the blockchain folds.

GARY GENSLER: Right. And also, it's interesting-- I think, Jack, if I can pick further on that. When you have something on the blockchain, even if it arguably should be there, it's a property right and so forth, but it's an off-chain asset, it's not just a digital asset, and secured and verified on a blockchain. But in supply chain, it's often an off-chain asset, and often a physical asset. Then there's additional challenges. I think there's some really interesting use cases, but it's a little bit of a different place. James. And then I'm going to-- no?

So McKinsey defines a blockchain. And they point out it doesn't have to necessarily disintermediate to generate value. I thought that was an interesting intuition. Don't always think that you have to disintermediate to generate value. They might be right or they might be wrong. But you might actually still end up with something that's kind of-- as-- did Catalina say it? I can't remember now who said it, but they also said they gave a timescale. A short term value might be predominantly-- Kelly did, sorry-- three to five years away.

How to capture value. Be pragmatic and skeptical, but you need to go down to a granular level. And that's also what I'm going to ask you to do in the final paper, is really to challenge yourself, challenge your group to go down to the granular level and say, wait, what transactions are we actually going to change the flow? What ledger system might we shift? And even though it's the back office-- and to some people, you might say, oh, my god, that's kind of the boring side of business. But that's really what blockchain is about. It's a database and ledger management system also. And to be successful, you have to get down to that granular level and figure it out in terms of whatever that current ecosystem is or the regulatory system.

They said it's particularly valuable in low trust environments. And that could be where currently we can't trade directly and you've created a new way to do peer to peer, or where there's not currently a central intermediary. You can go right at it. You could be like this bold group that says, I want to take on Transunion, I want to take on Equifax. That's something which is a central intermediary right now. But it is correct, we're not really trading directly. It's not like when I walk into the auto shop or to buy a car and I'm going to take a loan out that I can transact. They want to validate that I can pay back that darn loan. Yes?

AUDIENCE: Just two points, particularly the fact where your-- well, you can't trade directly now, but there's a lot of trade happening where you don't have an intermediary, but some sort of intermediary would help. I couldn't help but think of ag markets in very--

GARY GENSLER: You're saying ag, like agriculture?

AUDIENCE: Agriculture markets in very remote parts of the world, where actually being networked. And precisely, there's no trust. That kind of environment exists. So a good use case for that, extreme remote parts of the world where internet is there, but not necessarily financial institutions or regulatory environments.

GARY GENSLER: Right. And there are many parts, particularly in the third world that are still unbanked. I've said this statistic before, but the World Bank report on banking in 2017, half of sub-Saharan African was still unbanked. But half of that half has mobile phones. So it's just-- those gaps might change, but then it will move. Yes, they might have a banking account, but it would be not something they can really do with agriculture.

So two opportunities-- and I'm going to come to the question-- is like, do you go head-on against a central intermediary and use this technology to do it better?

[PHONE RINGING]

Look at that. I should turn this off. Head-on against a central intermediary? Or some market structure that has no really core intermediary, but you can build a better trustless peer to peer network?

AUDIENCE: Yeah, [INAUDIBLE] that's when it comes to private permission. Architectural blockchain, it's highly likely to be more scalable. Why is that?

GARY GENSLER: Highly likely to be more scalable, yes. So permissioned blockchains, they've made a trade-off. So Nakamoto's paper comes out. For a few years, people don't really notice it. But then it starts to get some lift and folks are looking at it in 2013 to 2015. And the financial industry starts to think about this and says, this actually is pretty interesting. We're not sure what it's going to do, but we're pretty interested. And they get attracted to it because it might be a way to move data around, it might be able to literally lower the costs of the back office. Many banks keeping the same set of records-- I have an equity trading business, you have an equity trading business. We both have to confirm and correct those records. But we keep full databases.

What they found attractive was real. But then remember, Bitcoin can only do seven transactions a second. So all of those challenges of scalability, privacy, security led them to think about, was there a way that we could literally toss some of the technical things over the side? And most of them thought, we don't need a native token. We don't need an incentive structure. And if we limit the number of nodes in the network, we can increase scalability and we can get rid of proof of work. So my narrative might not matter, but it's important to understand it. The permissionless thing comes along, and then they say, it's not scalable. What can we toss overboard and make it scalable?

And what they tossed overboard-- they didn't even feel they needed the native token, and they tossed overboard proof of work, consensus, and had a club deal. In the Australian stock exchange example, they might only have two or three nodes. But in some of these, there's 15 or 20. So why is it more scalable? Fewer nodes and much more efficient consensus mechanisms. But the trade-off is you better damn well trust now those 15 or 20 nodes. And when we talk about 51% attacks, you could revise a whole permissioned blockchain if those 15 parties wanted to.

Now, some people say, well, you could just do a hash function. Remember that whole hashing. You could do a hash function of a whole permissioned blockchain once a day, once a week, once an hour and store it somewhere else. In fact, you could store the hash of all of that on Bitcoin. You could use a ledger like Bitcoin and just store it there. So there's some feedback loops. Does that help? Give you a sense?

AUDIENCE: I was also just going to build on that. So the power of a permissioned blockchain is that, unlike Ethereum or Bitcoin, it's not public. So there is no public ledger. You can make it public, but it's permissioned, not permissionless. Because you need to have trusted entities in this network. So this can also be, you could say, a feature, not a bug when it comes to scaling. Because essentially, you control the scale. So you control these nodes. And then like mentioned, these nodes are only relevant because they are trusted pieces of this puzzle. Yeah.

AUDIENCE: Right. I think it's easier to get scale, but there is not a large enough market to actually make it scale or make it reach to the critical mass.

GARY GENSLER: So are you worried that there's not enough to get to the critical mass? Now, I'm not sure-- so a permissionless blockchain and a permissioned blockchain both can be open to public users. You can have millions of people use a permissioned blockchain, but only 15 have the right to amend the records. So one might think of who has a right to read it, who has a right to write on it. Read, write. But also, absent even that, it might provide a service, like file sharing or some service. There might even be a third list of who has a right to use the service.

Now, usually to use a service, you actually have to read the data. But you could partition and say, how much can be read as well. Yes, and remind me of your first name. I'm sorry.

AUDIENCE: [INAUDIBLE]

GARY GENSLER: [INAUDIBLE]

AUDIENCE: Yeah. I really appreciate your perspective from how you envision [INAUDIBLE] permissioned projects.

GARY GENSLER: The pathway, you said?

AUDIENCE: [INAUDIBLE] in terms of its relationship with [INAUDIBLE]. Do you think it would pave the way towards the true decentralization eventually? Or you were just [INAUDIBLE] Or you would just become irrelevant just as the intranet compared to internet.

GARY GENSLER: So [INAUDIBLE] question is unanswerable, but I'll try to give my opinion in 2018, and then we'll see. And it's being recorded, so we'll see how I'll do. But the question really is, what's the relationship for permissioned and permissionless blockchains? And what is it going to be longer term? I think today in 2018, because of the scalability issues and some of the privacy and security issues, the dominant place that the investment will be is on the permissioned side, especially with what's called enterprise applications, the banks, the large institutions.

There's not enough scalability because 1,000 users a day or 1,500 users a day on the big apps right now on the Ethereum network, that's just not enough beyond gaming sites and some small hobbyist type things, like CryptoKitties. It's fun, it's interesting, but it's not truly scalable to 7 billion people living around the globe. But I wouldn't-- and I've said this to some IBM folks. And they have 1,000 people at IBM in the hyper ledger team. Anybody who is a blockchain minimalist-- you haven't heard this number?

AUDIENCE: I've heard 2,500.

GARY GENSLER: 2,500? All right. So it's more than I thought. So 1,000 to 2,500. I knew it was more than 1,000. IBM is throwing a lot of money there. Now, they might be doing that to protect their risk. They might be investing even if all those 1,000 people ultimately produce nothing. But I think that five years from now or seven years from now, the gap will close. I think that permissionless systems will always have a lot of challenge about governance, collective action. How you have collective action is not just a matter of technical and coding and smart scientist at MIT and elsewhere.

I think that's going to still be a challenge, and there will be trade-offs. So it might be that they coexist, but I think the gap will close. And you said, well, will it be like the intranet went away and the internet was there. There are some people that believe that. And that might be-- I'm probably not there. I'm probably not all the way there. But I think when the gap closes, some of these permissioned systems will not be as necessary. Zero knowledge proofs, other ways that come along that make it more usable. Yes, Zann.

AUDIENCE: Totally understood. I'm a little bit skeptical on the permissioned blockchains. One of the--

GARY GENSLER: Are you skeptical-- if I can interrupt you-- and thus it moves you over to traditional databases? Or skeptical and you're moved over to permissionless open? So I don't know, which way is it pushing you?

AUDIENCE: Depending on the use case. For enterprises, I think traditional databases for the enterprise use case. Reading here, this line killed me. It said, "Accenture developed immutable blockchain in which the content of individual blocks can be modified." It's a ridiculous statement considering the definition of blockchain is anti-- this is the antithesis of basically--

GARY GENSLER: Right. So Accenture created an immutable blockchain that isn't immutable, is what you're saying, it can be amended. So it's a backdoor I can change. And yet, the economics of it is that a lot of times, people do want a backdoor. And the challenges-- and these are the weaknesses as well, as Nouriel Roubini says. Why would you create a system where if you forget your private key, lose your private key, or the cave collapses-- that you're hiding the private key in a cave and maybe it floods-- that you've lost your assets? Wouldn't you want a backdoor?

But I respect-- you would say this isn't even a blockchain. I'm trying to teach this class in a little bit neutral between permissionless and permissioned blockchains. But you need something to get out of the traditional databases. And I've chosen, at least for purposes of this class, that means you've got to have an append-only log, you have to have time stamping. So the basis of multiple people writing to the ledger, even if it's only three or five. But these are not well-defined vocabulary terms. Alin.

AUDIENCE: This is why we should stop using them. And this is a perfect opportunity to actually talk about append-only ledgers because that's actually meaningful-- a meaningful notion that's been studied in computer science for decades. Or consensus algorithms, which is another meaningful notion studied in computer science for decades. And consensus algorithms on append-only ledgers, sometimes referred to colloquially as blockchain, and then we would know what are we actually talking about. If we--

[LAUGHTER]

GARY GENSLER: Well, I will try to help. But we're only 80 people, and there is a lot of people using these terms. And when you go outside of this class or even when you read an open letter to Jamie Dimon-- of the somewhere between 25 and 50 readings you had so far this semester, they've used the word blockchain in multiple ways. I'm agreeing with you. You're just asking me not to ever use the word blockchain again?

AUDIENCE: Yes.

GARY GENSLER: Oh, my god. And he's sitting in the center of the class. Let's keep going. So we're going to study these. This is just this list that we've talked about. But in Act Three, we're going to come to it after SIP week and start to go through venture capital payment systems and so forth. It might be some of what you're picking up for the final projects. But here-- and I stress the word, potential use cases. Will these all work? Will they be places? In the non-financial space, supply chain management I put on this list, but it's kind of financial and I wanted to include it. Digital identity is both within finance and outside of finance.

Property and asset registries-- you can call it finance, but I'm not going to dig into that a lot in the rest of the semester. Medical records, internet of things, and so forth. This isn't going to be exhaustive. If you come on Tuesday, October 30, to the Bitcoin blockchain dinner that Simon Johnson sponsors, we'll have somebody doing election and voting. So there's a lot of other interesting applications. I tend to be a little doubtful about the voting because I think official sector and governments want something so centralized in that. But maybe it will be more decentralized. Maybe it's append-only without a consensus.

McKinsey, they broke it down into six buckets. They had the record keeping and the transaction-based. And a lot of these are the similar buckets. It's just to give a spur to all of it. So accessing costs and benefits. So we've talked about what are the benefits. These are the questions that I would be saying. And some of this was in the Geneva Report, but rather than trying to tease it out of all of the discussion, here I would lay out four big buckets as to how I think about this and how I might get your feedback. If you see other ways to look at this, I want to learn from you all as well.

And when I say four, this is the first bucket. Basically, what are the benefits of using this technology? Whether it's this idea about consumer credit or some of you have had ideas about government procurement or payments, wherever you are, what is the true benefit? You've got to find a pain point. Every entrepreneur always has to find a pain point, something that you can be solving it for a group of stakeholders. And who are the stakeholders you're solving something for? Or if you're a company, is it an internal pain point? Pain point is some constraint to making more profits, more revenues. Or it's a friction, it's a cost and you want to get rid of a cost. But what is the pain point for providing a good service or making more money?

How can you capture the value? As an entrepreneur, if you do something for eleemosynary purposes, meaning you don't care about making money, I applaud that, that's terrific. You can even hand that in for your final project. But I'm assuming that you're going to be thinking like me, how do you capture value? Not only do something, but also capture that value and get a little of somebody else's economic rents if possible. Thirdly, what are the competition doing? What are the competitors doing? Even if they're using traditional databases, how are they addressing the same pain point in anything you're doing?

And why is blockchain technology-- or, as Alin would wish me to say, why are append-only longs and consensus protocols-- what is the answer? What is it about append-only logs with their time stamping, with their final settlement, the finality of that settlement, what about that? Or even a full consensus protocol and a native currency. So I'd add a third thing because permissionless would also have an incentive system in a native currency. So what is it about append-only logs, consensus protocol, and a native currency? How am I doing?

AUDIENCE: I love this.

GARY GENSLER: You love it, yeah.

AUDIENCE: Talk like this all the time. Don't forget it.

GARY GENSLER: Yeah. Oh, my god.

[LAUGHTER]

Oh, I need this. But that's the core. And I talk about it being the final project, but this is going on right now. $28 billion dollars has been raised in initial coin offerings and a few extra billion, 3 or 4 other billion has been raised by direct venture capital in this world, but call it $30 billion. It's not fully mature, but it's maturing, and a lot of venture capitalists are saying, wait a minute, wait a minute, we're past the hype stage. What pain point are you trying to address? How are you creating value? What are the competitions doing? And why do you need append-only logs, consensus protocols, and possibly native tokens?

AUDIENCE: I just wanted to follow-up on that point about the Accenture--

GARY GENSLER: You're not going to tell me how to define something? All right, Kelly.

AUDIENCE: The Accenture thing he was talking about from the--

GARY GENSLER: It's immutable but amendable.

AUDIENCE: Right. So we ask ourselves the question-- that seems a little bit-- it defeats the purpose, right? So I then ask myself, what value is being created by doing that? If it's not necessarily for their customers, where is the internal value lying?

GARY GENSLER: I don't know what the application was. But I think that in every application that we find, not just in blockchain but in other applications, you have to ask absolute final settlement. If you can never amend it, if it is truly immutable, what cost does that also make? I assume that in this application that was too great a cost for them and they wanted a backdoor, a way to amend that which was supposed to be immutable. Again, I don't know that application. But that is one of the-- I think it's a feature of blockchain. But it's both a feature and, to some, a bug that you cannot amend something.

AUDIENCE: Yeah. It says that one of the benefits was that it allowed different entities involved to draw on the same record. So yeah, of course, I can see where that's valuable. But then it also begs the question, if you want to change it, then why not just use a traditional database?

GARY GENSLER: Vitalik Buterin in 2016 helped when an organization called DAO, the DAO-- is it Decentralized Autonomous Organization? Thank you for those who-- it was one of the largest at the time initial coin offerings. It raised about $160 US million. And very quickly, right in the smart contract-- it wasn't in the base Ethereum layer, but I believe it was in the smart contract on top, somebody saw what has later been called a bug. I don't know if it's truly a bug. It was programmed in, in a sense, but there was a way that they could see how to get in there. And they took about a third of the tokens, so the equivalent of about $50 million.

But the way the programming worked, there was about two weeks before it actually was truly final. It was something in the code also, and that wasn't a bug. And the whole Ethereum community was debating it. And Vitalik Buterin said, no, we can't let this happen. So in a sense, they big footed it. They almost did what Essentia. Now, he might say, no, actually, it was right at the 11th hour and 59th minute because there was this 10-day or two-week period. But they basically, Vitalik Buterin even did kind of what Essentia did at that moment.

AUDIENCE: They forked it then, right?

GARY GENSLER: I don't even know. Was it a technical fork because of how they did it?

AUDIENCE: [INAUDIBLE]

GARY GENSLER: Right at that moment.

AUDIENCE: Ethereum classic still has the DAO--

GARY GENSLER: The stolen $50 million or whatever, the number of tokens. So that led to the fork. The majority of the community went with Vitalik rather than what the fork happened. So how immutable is immutable if there's a broad consensus? Now that's the backdoor, in a sense. Second-- was there another hand? I'm sorry, Brodish.

AUDIENCE: I think the [INAUDIBLE]

GARY GENSLER: To address Kelly's and Zann's.

AUDIENCE: And the word blockchain.

GARY GENSLER: And the word blockchain. All right.

AUDIENCE: So I think when people are talking about blockchain as a term, they're essentially referring to a set of potential benefits of this technology. And some of them can be relevant for a particular use case. Some of them might [INAUDIBLE], some of them might actually [INAUDIBLE] for that particular use case. So the way it can be thought of is that we have an umbrella term which talks about referring potential benefits. We take what is [? referred ?] from that. It could be append-only, it could be not append-only, it could be consensus, it could be permission, permissionless, whatever.

And then we cannot calibrate with them and create a solution which is applicable for the particular use case that I want to look at. That is why even if it is not immutable, it is still a potential use of blockchain, from my understanding. Because we are bringing up some of the benefits of the umbrella term.

GARY GENSLER: I think you're correct, but I'm not going to go all the way to where you are. I think you're correct that, broadly speaking, many people are using this term to promote their own innovation, the innovation of their colleagues, and so forth. And yet, some want a backdoor, like Essentia, and make it less immutable. And so all of a sudden, if it has a big backdoor and you can amend, is it really an append-only log any longer? What I do want to say is, in this class, I am going to say, anything you're working on for your final paper, it has to be at least a permissioned or permissionless system. Thus it has to have a-- what's that?

AUDIENCE: Not mine.

GARY GENSLER: Not yours? But you're going to get there. You're going to get there, Brodish. You're going to get there. Since I told you earlier in the day, get to yes. But if it's a traditional database, I'm saying stretch your minds, try to figure out something. Even if it's got a little bit of risk into it as to how you get to using append-only logs, and even in a permissioned closed loose private consensus, but some consensus. Think about whether you use a token that gets the permissionless. Uh-oh. Eric's going to plead his case.

AUDIENCE: I'm just going to try to completely reconcile this.

GARY GENSLER: And then I need to keep going.

AUDIENCE: Yeah. Those two apparently divergent points--

GARY GENSLER: Right, Brotish and Alin.

AUDIENCE: Yeah.

AUDIENCE: I actually agree with Brotish.

AUDIENCE: The point is that--

GARY GENSLER: That he might agree with him.

AUDIENCE: I'm still in the middle because from a technical standpoint, it's true. You have append-only log in a consensus mechanism that make up the original use case that brought the term blockchain.

GARY GENSLER: Plus a native token in that one.

AUDIENCE: Yeah, of course. [INAUDIBLE] But to the point, though, what happens if you want to change or amend the log? Then is that really a blockchain? That's exactly the reason why the term [INAUDIBLE] later technologies came up. Because to a certain purist extent, it's not an append-only log because you're actually updating it from a purist definition. That makes sense, of course. But then the nature of a distributed database that's not located in an intranet that governs the updates and whatever changes you make it, it's the reason that make up these ledger technologies that are blockchain inspired, if you may.

So it's OK, you can say if you amend the log, then it's not blockchain. Right, but it's DLT, and the DLT is blockchain inspired. So we can keep everything in the neighborhood.

GARY GENSLER: We're going to keep this discussion and debate going. And we're probably not all that far off. It's not about vocabulary, it's also about I'm trying to spur you all to get to yes, even if you're a minimalist. Think about some project that uses the essence of this, and not just inspired. So then what are the specifics of this append-only log and consensus use case or blockchain use case? So what cost of verification or networking are you actually reducing? Back to Catalini's work about verification cost and networking costs that we talked about on Tuesday.

What is that cost you're actually reducing? Which transactions need to be recorded? What accounts or transactions, you might say, need to be recorded on this log? What stakeholders need to be able to write? If there's only one stakeholder that needs to update something, I'm not really entirely sure that you'd be in this distributed decentralized place. So I list these questions that weren't directly in the readings, but I list these questions to say this is a way to start to get your mind around where this technology, however we label it, this technology can help.

In essence, does it lower cost of verification and networking? And if so, which ones? Which ones are you trying to address? Which ones are you trying to dig and basically create value for your startup? What transactions or accounts are you trying to record? Transactions, like changing property rights or moving around birth records or land records or supply chain. But where's that? Which stakeholders actually need to write to this distributed ledger? Because if it's only one party-- I'm still trying to get my head around why the Australian Stock Exchange really needs it, but OK. What is it that multiple parties need to write to this shared collective state of what is there?

And then the last one is also terribly important, is, what's the customer user interface? And a lot of challenges are basically like, currently we're not in a place where a lot of blockchain applications are distributed, applications have great customer user interfaces. But that as well. Then what are the cost of the transitions? Akira mentioned this from the Geneva Report and the other readings. But what are the costs and challenges? Well, of course, we still have a bunch of scalability and performance issues. We have the privacy issues and coordination.

I'm not trying to hold us all to that, by the way, for your final projects. If we're not going to get to scalability for five or seven years, I'm not going to say, well, then you all have to write about permissioned systems. No. I'm OK if you say, well, this is a pilot and somebody else is going to solve through layer two or zk-SNARKs or something, these other things. But I'd like you to at least identify what are the issues of scalability, performance, privacy, security, those issues that might hold your implementation out. Can a permissioned blockchain adequately addresses whatever the use case is? And how can you actually jump start broad adoption? That's your network challenges.

How, when you start Uber, can you get a lot of people to use your Uber app? But in this case, if I can use that consumer credit-- I thought the consumer credit idea was really a neat one. Maybe it could go right at the heart of a lot of market power. But now, how do you get all the auto dealers, how do you get all the employers, how do you get the banks to actually say, I want to get rid of First Union and I want the Blockchain and Money final project team's-- and by the way, just replacing one central monopolist with another central monopolist, a lot of commercial banks aren't terribly excited about that.

Maybe you're going to have to give some ownership. Maybe you'll have to give 50% of your ownership to the 20 banks that are now a part of this. There are other ways to build incentive systems. Maybe you put a native token in there and you give them the native token. So there may be other incentive ways to beat the current monopolist. But having been around commercial banks for a long time, they really are looking for ways to replace their aggregators and their back office, whether it's clearing, settlement, exchanges, credit agencies. But they are deeply understanding-- because they are pretty ambitious and very good at making money as well, they deeply understand that every idea that's pitched to them is somebody who currently is small but wants to get big and gain market power.

So they're also always thinking about how to ensure that there's a check to slow down your startup from gaining market power 5, 10, and 15 years from now. They don't want you to be the next Clearinghouse, like the Chicago Mercantile Exchange or Intercontinental Exchange. They don't want you to be the next central node of market power. So you might share some of that with them, or you might find an incentive system. And then what are the net? So key questions for companies designing blockchains. This is something from MIT's own Sloan Management Review. It was not a required reading, but I thought it was a nice little way to do it.

What are you trying to do? Are you trying to record something? Track something? Verify something? Aggregate something? This was in the Fall MIT Review. What value do you want to capture? Literally, here's a list of the things you might want to capture. Is it about contracts? Is it about permissioned? What is the value we're trying to capture and for whom? Obviously, is it for suppliers or customers and so forth? So it's another slice by thoughtful people, MIT. That's a link to the reading if you do want to read it. It was a well-written five page article. I even held back on one reading.

So the benefits of blockchain-- we reviewed this last Tuesday, so I'm not going to go through it again. But again, as you're thinking about this and thinking about which use cases and so forth, think of these costs of verification. Which of these are you really trying to hit? Or is it networking? And I changed the networking a little bit, but a token incentive system, which could be like the skins, rewards, and affinity, identity could help you start it up or operate it. Or it could be like CryptoKitties, where it's like a collectible. So that's another way that you have token economics floating in.

So this you've seen. I've flipped it around, but basically, do you use a traditional database? Do you think about a private blockchain? Do you think about a public blockchain? If you're over here, I really ask you, Brodish, you've got to get to yes. You've got to get to here. You wouldn't want me to just be teaching a traditional database, how do you build something in Sloan, right? This is blockchained money. Or as Alin wants me to relabel it, append-only logs, consensus protocols, and money.

[LAUGHTER]

AUDIENCE: And a native currency.

GARY GENSLER: And a native currency. But how many of you would sign up? Would you recommend that I list it in the course catalog that way for next September?

AUDIENCE: No.

GARY GENSLER: Really? No, not really. All right. But if you want to really juice, get to here. Put an append-only log in there and some even private permissioned system. Or be bold. Try to get all the way to there. Don't stay there, please. All right. I've made my point. James. Where are you? Are you there or there?

AUDIENCE: I think I'm in the middle, private blockchain.

GARY GENSLER: Ah, come on.

AUDIENCE: [INAUDIBLE]

GARY GENSLER: All right. Good. Yeah, but they're going to get at least to there. They're not staying there, they want to get a good grade.

[LAUGHTER]

No, no. Really, this is going to be fun. Listen, I get it. It's not just like any Sloan class, where you have a final and everything. I've given you a hard test. There's $30 billion chasing around to try to find uses. There's thousands-- 2,500 at IBM or whatever-- there's thousands of people trying to do this. And there's no really true market-wide applications right now. But that's the nature of what we're doing here together. And I'm not asking that somebody actually be able to go raise money and actually start it. You don't have to code it, except for you, Alin. But you don't have to actually code this thing.

But I'm really looking for your business savvy, and it's more about critical reasoning skills. And these four or five pages, pull it off of Canvas and think about it, think about how it fits in with your projects or not. Yes?

AUDIENCE: Given that-- well, the question in previous slides are helpful. But I still find it's hard to decide whether we should really use blockchain database [INAUDIBLE] traditional database. So is there a non-technical model or framework that we can [INAUDIBLE] between those two?

GARY GENSLER: I think of it-- I apologize if to go back to the slides, so I'll try not to. But I think about it as, are you moving around something of value? Do you need multiple people to be able to help in that network? Because it's peer to peer. If it were the 80 or 90 of us in this room, you might be just there right now, that there's a benefit of that peer to peer movement of something of value. Or frankly, even back to this, if there's a lot of economic rents. If there's market power in this, if there's big market power and somebody is just collecting lots, that might be your opportunity because this is the technology that can get you there.

And you might say, well, I don't absolutely have to have an append-only consensus native currency type of technology, but it's how I get to peer to peer. So it might be that that's the way that I'm going to disrupt the party with the big economic rents. Like the letter to Jamie Dimon, if there's a bunch of things about censorship risk. And again, I don't know what use cases you're thinking about. But I think if you don't have one of these six, the verification costs, it's unlikely you need an append-only log and consensus in the whole mechanism.

But I think if you do have something here, hopefully not just economic rents but market power, this might be the way you get underneath it, by having a decentralized peer to peer approach. So if that helps. And it could be something that has no central authority right now, no central intermediary, and it's just how to jump start something. I think in that circumstance, it's more likely you need a native token.

I think if you're trying to jump start a network-- and there's a lot of collective action reasons that will still face you. Some of our colleagues, Andy Lippman and others over at the Media Lab, spent a lot of time a year, year and a half ago on a medical records approach with Beth Israel Hospital locally here. And if Andy were here, he'd say, but I still have the collective action issues. How do I get a bunch of hospitals and a bunch of doctors and how do I get all that collective action to work together to use one database system, if you wish? So I think to get over that collective action issue, you start getting into, well, this native token might be an interesting way to do that.

AUDIENCE: Right. It seemed that Uber satisfied the things you just mentioned.

GARY GENSLER: They did. They did. But would they have done it differently if they started in a different era? I don't know. It's remarkable that they took on and just completely transformed the ride share business, the taxi business, if you wish. But I'm pretty confident of this, there will be something that we don't envision right now that really transforms the next thing. As my brother said when he said, it might be five and 10 years from now and you won't even expect it. Who would have thought the internet in the 1990s was going to go straight and transform the taxi business? Nobody in the New York Taxi business would have envisioned that, which was one of the things that he mentioned.

So why use blockchain versus traditional database? We did that. I know, you got it got, Brodish? Right there? OK. No, I'm having some fun. So the trade-offs we've talked about, so these are costs. This is the cost of centralization versus decentralization. We've looked at this slide before. I think this was an earlier question. Over time, I think what's going to happen is these graphs might have different slopes. So it's just like, OK, what if the slopes change?

I think that the cost of decentralization are going to come down. But that's more my forecasting prognostication. And then you'll have more applications that feel more comfortable over using something around this space. Now, I could be wrong and it could go the other way. Just saying. And this would be more of the minimalist side and says, well, you can address some of those centralization costs and it comes down the other way. So it's just a visual way to think about what will happen over time with innovation. But I think innovation will pull down the slope towards that from where we are today because of the newer technology, this decentralized how can we do this. And I think there will be more opportunities around it.

All right. So on the 30th, we're going to be talking about basically our first area. We're going to talk about payments. We're going to talk a lot about payments. I'm going to take two days to talk about payments. So we're going to lay out a lot about what's going on in finance outside of append-only logs and consensus protocols and blockchain. But we're going to have fun because what we all live together. And some of you actually live in these countries. But whether it's Alipay, [INAUDIBLE], and M-Pesa, so all these initiatives. And then how could maybe blockchain fit into it?

In terms of the use cases, these are all those use cases that we're going to be doing from October 30 to December 6. But this gives you a sense, what I call Act Three. And we're going to really be trying to challenge each other about-- some weeks, I'm going to give you a heads up, it's going to be a little thin. I'm going to be looking for who's got really good use cases. If you have something to bring into the classroom that you're saying, hey, this reading list I put together in late August-- and by November, it might be that there's somebody that's actually moved something further.

So don't be bashful. Shoot it into me in time and I'll distribute it to the whole class. But in a couple of places, digital ID, for instance, I thought it was thin. There's the Estonia case, but it's not really-- not sure it's a blockchain. I'm admitting in advance, some of these are a little thin but still good. And the readings for the 30th-- the Federal Reserve Payment Study really shows a bunch of information. And you have to read the words, just look at the few charts. But it's going to give you trends. You're going to really see some interesting trends in there. What the best mobile apps are, and the global payment report, and things like that.

Any questions on any of that? And then what did we talk about? Blockchain technology can address costs through verification and networking. The potential use cases-- the devil is in the detail. It's true in most things in life, but it really is these natty little details about what transactions, who am I going to try to disintermediate, where am I going to create value, why use a permissioned or permissionless blockchain rather than a traditional database, and really get some value. I think you really have to address this question, but I think there's potential there. Or why a public blockchain versus a private? Is a token going to help you jump start something?

And remember, there's two different types of tokens. There's the broad currency type token. That might be Bitcoin, and they might have won the whole thing, or it'll be somebody else, or there might be two or three. I personally don't think there'll be hundreds of those. But then there might be, in essence, use case-specific tokens. Right now we have 1,600, and most will fail. So that's it. Any other queries or anything? Yeah?

AUDIENCE: Once all the bitcoins are mined in 2040 or 2030--

[INTERPOSING VOICES]

AUDIENCE: 2040.

GARY GENSLER: But by 2040, it's a very slow inflation curve. It's probably a slow inflation curve in the middle of the 2030s.

AUDIENCE: The incentives, if there will continue to be incentives for node operators to continue operating benevolently, if there's no further incentives--

GARY GENSLER: So the question is, what happens in 20-- when there's very few mining rewards? And the answer is-- I'm going to have some fun with you here. I'm going to show you one other thing. The answer is, yes, because it's fees. And the fees in the system-- I apologize. It's just one thing that I want to show you that's fun. The fees in the system-- so right now you can have fees, if you remember how there are fees in the system.

And instead of having mining rewards, right now there are very small fees. So for every transaction you put into Bitcoin, you can actually say, instead of taking at exactly that the inputs equal the outputs, you have inputs greater than the outputs, and the net is fees. And what is the case there is that in 2030 or something like that, I think the fees will continue to increase, I think, if this takes off. The question is, does it take off? So I just had some fun because this day is an important day for me since you met him. So whom is whom?

[LAUGHTER]

I sent this picture to Rob this morning because today is our birthday.

[CHEERING, APPLAUSE]

AUDIENCE: (SINGING) Happy birthday to you--

GARY GENSLER: No, no, no, no, no, no, no. That's all right.

AUDIENCE: (SINGING) Happy birthday to you.

GARY GENSLER: No, no, no, no.

AUDIENCE: (SINGING) Happy birthday, dear Gary. Happy birthday to you.

[APPLAUSE]

GARY GENSLER: So who's who?

AUDIENCE: You're in the white.

GARY GENSLER: White in striped shirt or not? OK.

AUDIENCE: Solid.

AUDIENCE: Your stripes.

GARY GENSLER: All right. How many striped shirters? All right. All right. How many solid shirters? Wow. So I sent it to Rob this morning, and I sent it to my three daughters, and I sent it to my girlfriend. I said, who is this? It's split view there, too.

[LAUGHTER]

I went with striped shirt, but Rob said he doesn't know.

[LAUGHTER]

We were three years old there. So that's just a goof around with you. All right. Thank you all.