PROFESSOR: Welcome back. I know we're sort of getting into the middle of the week. Some of you maybe want to keep your laptops open to work on other courses' midterms, but I will ask you to try to focus on Blockchain and Money today. Today, we're going to chat about permissioned versus permissionless systems.

I want to thank-- I have a guest here. I call out guest when they're here and I know them. Mark Snyderman, who runs a fund at Fidelity-- Mark runs a 6-- about $6 billion? Called the Real Estate Income Fund at Fidelity. And you might say, well, why does he want to come to a Blockchain and Money course? It's because we went to high school together.

[LAUGHTER]

So-- and I was at his wedding. And he's getting married again next week. Yeah.

[APPLAUSE]

But you can all inundate Mark later about Fidelity, because he's been there for a lot of years. See what I'm going to do? I'm shamelessly for MIT and MIT students. So let's get going. I was letting a little bit of time for a few more people to wander in. Today, we're going to talk-- of course, we're going to chat a little bit about the readings and study questions.

Going to go back again to, what are the technical and commercial challenges? And this is relative-- this is relevant for all of our lectures, but it's particularly relevant today, because we're going to be talking about two different database structures. One's the permissionless blockchain of Bitcoin.

But now, today, we're going to introduce and go deeper into the permissioned, or private, set of blockchains, like the IBM Hyperledger and Corda. But the technical issues relate to all of that. And then, of course, we're going to talk about that against a third type of database-- traditional databases.

So aligning permissionless, like Bitcoin, permissioned-- IBM Hyperledger type of-- and then traditional databases, and why, in a business setting, you might think of one versus another versus another. And I'm sure if I run off the rails anywhere on traditional databases, which I have not personally studied, Alon will help bail me out somewhere. Is that a deal? Maybe?

AUDIENCE: OK.

PROFESSOR: All right.

[LAUGHTER]

AUDIENCE: You asked for it.

PROFESSOR: Yeah, I asked for it. Mark, Alon is a computer scientists from other parts of MIT, so he helps me out in subjects I don't know, and even in subjects I think I know. So let's just start a little bit with what did you take from the readings? There were four or five readings, of course. But what is a permissioned or private distributed ledger?

Now, I can do this. I can light them up, as some people said, because Toledo's given me my list. But again, class participation-- anybody who hasn't spoken yet might want to sort of chime in and give it a shot. I'm not seeing any volunteers. If I can-- ooh, yes. Do you want to tell me your first name again?

AUDIENCE: Jayati

PROFESSOR: Jayati.

AUDIENCE: Jayati.

PROFESSOR: OK.

AUDIENCE: So the permissioned DODs, unlike the permissioned [INAUDIBLE] Bitcoin, they limit the number of participants. Essentially, they require the participants to be authorized before they can enter into this sort of technology. And in addition to that, they are said to be stakeholders.

And since they are the only ones involved in verifying the transaction-- unlike the permissionless ones, where it has to be verified at all the nodes, this limits the permissions required [INAUDIBLE] stakeholders, which increases, also, the transaction speed. So it's like the triangular dilemma we learned about, about the security and decentralization and

scalability. So it moves away from decentralization and towards scalability.

PROFESSOR: OK. So Jayeta--

AUDIENCE: Jayehta.

PROFESSOR: Jayeta went through a whole lot. It's about the number of nodes and permissioned into it, and that it addresses some of that Buterin's trilemma. So at its core, it sort of addresses some of the scalability issues. But it does that at a trade off that it's not truly open. It's not, anyone can write to the ledger. I mean, that's sort of the fundamental things.

Anything else that folks took out of the core readings as to how it separates and how it's different? I mean-- all right. We'll get a chance to add a little bit. And then we're going to dive into Hyperledger and Corda a bit. We'll talk about Digital Asset Holdings. What's Digital Asset Holdings? Anybody know this company? Alon knows it. Brotish knows it. Eilon. So Eilon.

AUDIENCE: Yeah. It's basically a competitor of [INAUDIBLE]. They're trying to build a DLT protocol that will allow financial institutions to exchange information and value. And they started, to my understanding, in 2016, which is two years after R3 Corda funded by [INAUDIBLE] JPMorgan, Goldman Sachs. They're basically the same amount of money-- $110 million.

PROFESSOR: And who, other than Alon can tell me who runs Digital Asset Holdings? Just, it shows that you did the reading. Somebody out there. Yes. Priya?

AUDIENCE: It was--

AUDIENCE: Priya.

AUDIENCE: Yes. Blythe Mas-- Blythe Masters, or Blythe--

PROFESSOR: Blythe Masters.

AUDIENCE: Yes.

PROFESSOR: All right. Does anybody know who Blythe Masters is and what she's famous for beyond Digital Asset Holdings?

AUDIENCE: She worked at JPMorgan, and she [INAUDIBLE] credit default swaps.

PROFESSOR: So she worked at JPMorgan, and she's known around the world of credit default swaps. Gillian

Tett, who some of you-- the Sloan Fellows will get a chance to chat with Gillian Tett in New York in a few weeks. Gillian Tett wrote a whole book about credit default swaps and JPMorgan. And Blythe Masters is a central character in that whole narrative art.

And this is what she's doing now. She's brilliant, and she's a very good businesswoman. I ran the Commodity Futures Trading Commission and had an opportunity to meet with her a lot because she ran the swap dealer association ISDA at the time, or was the outside chair of ISDA, if I recall.

And then we're going to talk about the business trade-offs as well. But what do you think some of the central business trade-offs, if I could get two or three of you to help me out on what are the central business trade-offs between permissioned and permissionless blockchains? Let me see if I can get somebody other than Pria. Yes. Remind me of your first name.

AUDIENCE: Misha. So permissioned blockchain have better privacy and protection, and better scalability. And no mining [INAUDIBLE].

PROFESSOR: Misha, let's pause for a minute. So better scalability, better privacy, and the third point you're saying?

AUDIENCE: No mining.

PROFESSOR: No mining. Or, mining is associated with this proof of work. Any other business trade-off?

AUDIENCE: So for permissioned, you have some more flexibility with governance. If you need to make changes, you don't need to rely [INAUDIBLE].

PROFESSOR: So more flexibility of governance, in essence, because if you have a club deal or group deal, maybe you can do that governance changes amongst the group instead of having thousands of people participating. Kelly?

AUDIENCE: There's also a key technological differentiator, which is the coding language sort of that the inputs can be made in. So with Hyperledger, they can use the smart contacts in any variety of them, versus the alternative, which is the domain specific language.

PROFESSOR: Right. So Hyperledger at least promotes themselves in their own write-ups-- because the reading was really from them-- that their embedded language is much more flexible, and that you can use Java, you can use Go, and so forth-- at least they say they can. I don't know if it's

really as limited in Ethereum. But they think and they promote that they're more flexible than Ethereum. So Kelly's right in that, too.

So these were the readings. And now, so we're back to basics again. What is a blockchain? I know we've spent four or five lectures on it, but these key components-- let's start. Append-only timestamped logs. Are they both-- by show of hands, are they in permissionless blockchains? I hope every single hand goes up.

Are they in permissioned or closed blockchains? I'm watching. I'm not-- I'm just going to watch. All right. Every hand should go up. So both sets of blockchains have this concept that goes back nearly 30 years to our friend Haber, who started the whole blockchain that's in *The New York Times.* This whole concept is in both sets of blockchains. Brotish?

AUDIENCE: So I have a question about basically kind of [INAUDIBLE] append-only [INAUDIBLE] of the ledger. I think I read in one of the readings that Corda has a feature where you can make some changes to the history, which is not equivalent to a hard fault. So that will probably be one example where it is not purely append-only in a permission [INAUDIBLE].

PROFESSOR: So Brotish is raising that there's certain features that are promoted in one of the private blockchains, Corda, that may allow you not to append-only, but in essence, delete data, or replace data, possibly. And I'm not-- because there's also, in private blockchains, an inability to partition, and in essence, sh-- it's kind of a form of shorting-- but to partition the data. I don't know enough about Corda, whether they literally allow you to delete-- or is it something in this partitioning? But maybe Hugo?

AUDIENCE: I was going to raise a similar point that if-- I mean, to my understanding, if you have a permissioned system and there are only a small number of-- we'll still call them nodes, then if you realize you did something wrong, or something needs to be changed, can't they all go in and change that?

PROFESSOR: So Hugo's raising the point, if you're down to, like, three nodes-- as I've shared with you all, the Australian Stock Exchange is putting a permissioned blockchain up using Digital Asset Holdings, which I think is backed by also the Hyperledger Fabric technology. But if it's just the Australian Stock Exchange, and it's one node, or three nodes, couldn't they just change it on all three?

And I think, in essence, yes. I mean, that may not be what the database structure is, but I still

think it's potentially yes. So as you get more concentration, you have more chance. But Brotish, I will try to research the Corda thing more specifically. Other thoughts?

So then you create an auditable database-- some database with cryptography. Hash functions, which half the class said they understood and the other half was sort of, you know, a little rough on, all is in permissioned systems, using cryptographic schemes to ensure for the validity of the data and, so to speak, the immutable nature of the data.

What's different is consensus protocols. In essence, it all goes down, except for Brotish's point, maybe, about Corda, as to who gets the chance to add the additional data. Is it a small club deal, or is it broad, wide open? Everybody together, roughly? So back to the technical features.

Remember, it's a bunch of cryptography. Love it or hate it, it actually allows us all to use the internet-- well past, obviously, the blockchain that we're discussing in this class. Network consensus, and then all the ledgers. So both permissioned and permissionless have ledgers, have cryptography. It's that middle bucket that's different between the two.

So what were some of the challenges that we talked about in blockchain? We just talked about them 10 minutes ago, which is, what's the list again? See, this is the easy part. If you haven't spoken yet, this is, like, the easy questions. Oh, I'm hopelessly shameless. Yes. Do you want to say your first name so Toledo takes you off the list?

AUDIENCE: [INAUDIBLE]

PROFESSOR: Did you get it? No. Do you want to say it louder? Because Thalita [INAUDIBLE].

[INTERPOSING VOICES]

[LAUGHTER]

AUDIENCE: [INAUDIBLE] issue about the scalability.

PROFESSOR: Scalability.

AUDIENCE: [INAUDIBLE] takes the time to create the next block about [INAUDIBLE].

PROFESSOR: All right. So scalability and some time. So efficiency and scalability. Anything else?

AUDIENCE: Privacy?

PROFESSOR: Privacy. So it's basically the scalability, the privacy are two big things that permissioned systems address. Interoperability-- basically, how does this blockchain talk to other blockchains, or how does this blockchain talk to other legacy systems? Permissioned and permissionless systems both have issues of interoperability.

However, the smaller the club deal, the more likely that a bank or the Australian Stock Exchange might address its interoperability right within the system, whereas if it's a big open-sourced, open project-- so IBM would say, we can even help you with interoperability. IBM would say, we can help you with all four lines.

We can help you with scalability, efficiency. We can help you with privacy. We can help you with interoperability and governance. I think it's less clear they can help with all four, but they can certainly help with the first two. And Alon, you've switched from using a permissionless to a permissioned system--

AUDIENCE: Correct.

PROFESSOR: --in your startup, right? Which of these four is the reason why you switched?

AUDIENCE: So actually, I switched--

PROFESSOR: Or something else?

AUDIENCE: Something else. So for me, it was a business use case. So I was trying-- my business is selling to banks.

PROFESSOR: So that's the next line-- commercial use case.

AUDIENCE: There it is.

PROFESSOR: There's a setup. So what was the reason that you switched?

AUDIENCE: So I was building on Ethereum, which is public. And I thought that it's unlikely that, in the near future, banks are going to adopt Ethereum as their underlying technology. And then I learned about R3 and Corda, and learned that banks actually funded that project. So I switched to where the banks put their money.

PROFESSOR: So I would contend that it's a bit about interoperability. You felt your users would be more likely

to be able to work with your system if you were using Corda, with which they were familiar.

AUDIENCE: Correct. So there's a business reason and technological reason.

PROFESSOR: And then, of course, there's the public policy reasons. And IBM would even say that they're going to score higher points on the public policy if, for no other reason, that there's better privacy and security. Now, I'm not trying to shill for IBM. I'm just saying these would be their selling points-- or Corda, or elsewhere.

We talked about Buterin's trilemma. But in another way, many people would say decentralization competes with scalability and security. If you want scalability and security, you can't have decentralization. I'm not a big believer in this trilemma, even though I've now raised it twice. But it's often talked about at blockchain conferences, and blockchain papers, and business discussions.

So I've always told you I want to be a fair representation of the debate that's going on. I think it's more possible to solve these three over time together than some others. But maybe I'm just a cockeyed optimist about technology.

So public policy framework. What were the big three slipstreams? So I went fast last time-- last class. Leonardo, what are you going to tell me about the-- it's because you were adjusting your glasses.

AUDIENCE: Yeah. No, we spoke about the difficulty to implement framework. And you were talking more about the need [INAUDIBLE] offer security to protect people.

PROFESSOR: To protect people-- so it's sort of a privacy thing. I think I have a hand up here from Catalina.

AUDIENCE: There are three big things that [INAUDIBLE] public policy working against illicit activity--

PROFESSOR: Illicit activity.

AUDIENCE: --financial instability, and protecting the investors.

PROFESSOR: There you go. All right. So you know my style. I try to drop things into three buckets. But it's the only way I can remember anything. But it is the three big buckets, of course. And since I went fast last time-- and we're going to be coming back to a lot of it, but were there any questions that you have? And this is just an opportunity. Brotish?

AUDIENCE: So I have a question on the [INAUDIBLE] stability point. Like, you mentioned that because of the world value of the digital currency is very minimal compared to, let's say, [INAUDIBLE].

PROFESSOR: The value of crypto finance is about $220 billion right now, compared to worldwide capital markets that, in aggregate, are over $300 trillion of debt, bonds, and equities.

AUDIENCE: So my question was more like [INAUDIBLE] opinion on this, that this value is also concentrated within a limited number of people compared to the other assets that we are talking about, and hence-- I mean, it can still be important to regularize on the financial stability side, because it can have a effect which is not in proportion to just the size.

PROFESSOR: So Brotish is asking the question that even though it's only $200 billion versus $300 plus trillion of worldwide financial assets, couldn't it still be relevant to financial stability? And the answer is yes. But it's still relatively-- it's less than one one-thousandths of the broad size.

AUDIENCE: [INAUDIBLE]

PROFESSOR: Yes, please. Better you than me.

AUDIENCE: So basically, we did an analysis between the correlation [INAUDIBLE] public market [INAUDIBLE] and basically there's a correlation of roughly 80% to 85% when the public-- when the Bitcoin market's down, within the past year, the public market's likely to lift up. Because there's a lot of leverage built into the system.

And once the volatility kicks in, a lot of the investors [INAUDIBLE] they have to get money out from the public market, and that kind of feeds into a loop.

PROFESSOR: So you're saying there's correlation, and there may be feedback loops. Tom?

AUDIENCE: Sort of a related question. So Mervyn King was in this room a couple hours ago, and he was talking about, in the '08 crisis, two issues of trust-- one where there was a counterparty trust issue. Even though the overall derivatives market was [INAUDIBLE], banks didn't individually know which other bank was most at risk. And so they wouldn't trade with each other or lend to one another.

And then on the opposite side, the solution-- the salvation-- was two people in a room trusting each other that the central bank-- that the government would fund tens of billions of dollars [INAUDIBLE] capital. And so I wonder your thoughts on blockchain's role in addressing that

first problem of knowing your counterparty, or at least being able to trust their position, and then the risk of eliminating the second chance of injection of capital into the financial system in a blockchain.

PROFESSOR: Russ, [INAUDIBLE].

AUDIENCE: I had a question. It's related to this--

PROFESSOR: All right.

AUDIENCE: --which is--

PROFESSOR: Thanks, Brotish. [INAUDIBLE].

AUDIENCE: But the question is this. It does strike me that you only have a financial stability problem if people are relying on the value of people's Bitcoin holdings, for example, which is the bulk of crypto assets, right? The reason you have the problem during the crisis is you have all these banks.

They're carrying these assets on their balance sheet. And all of the sudden, people think they don't know what they're worth, right? Who, if anyone, is actually carrying a Bitcoin assets on a balance sheet that someone else is relying on? Or, to put it differently, who's extending the leverage?

PROFESSOR: All right. So let me--

AUDIENCE: [INAUDIBLE]

PROFESSOR: Let me wrap these together. I think that what many central bankers and the Financial Stability Board would say, at 200 billion versus 300 trillion, it's probably not that financially relevant at this point. Where it could get relevant is, as Russ has sort of suggested, is if there's leverage behind it.

If it's in a balance sheet, it's an asset on a balance sheet, and there's a liability on the other side. And thus it could bring down that entity, whether it's a hedge fund, whether it's a bank. But something that's relying [INAUDIBLE] to tie it back to the questions that Tom raised is, could blockchain lower systemic risk? Possibly, if it's a better database solution. If it answers-- what Mervyn King was speaking about, we also addressed in the late 90s.

I remember quite well when Secretary Rubin called a number of us into his office and said, I don't understand. The banks can't tell us their exposure to Korea. A number of countries-- South Korea was about to have-- but they didn't default on their debt, but they were coming close to defaulting on their debt. And of course, it was only a short while before other countries, like Indonesia and Thailand, were getting into that same debt challenge.

But why couldn't banks tell the US Department of Treasury their exposure? It's usually through derivatives. And derivatives, both in the late '90s and the financial crisis, were often something that propagated risk through the system. Now, the numbers were larger-- I mean, depending upon the time. The '90s was less than this. But it was $300, $400 trillion of notional amount of derivatives.

So just the sheer notional size, even though the capital at risk in derivatives was much smaller because the leverage of this notional-- big, notional size. And the transparency was pretty low. It wasn't zero, actually. It wasn't zero. But it was really low. And so I think that's what Mervyn King would have been mentioning. And I do think blockchain can help in that transparency. But it takes a big collective action. And so Europe, the US, and Asia-- a lot of laws were passed to get more transparency in the derivatives space.

Brotish, I would say that there could be problems. And I've had conversations with elected leaders that say, don't get lulled into the sense that it won't have financial stability issues. Because that was what happened in the 1980s and '90s when people said, well, derivatives will not create instability, because it's only the institutional investors, the sophisticated investors-- the so to speak big boys or big girls, you know?

And I was part of those debates, that consensus that formed that it was only institutional and it wouldn't-- but there was a lot of leverage and a lack of transparency when big leverage-- multiple hundreds of trillions of dollars-- associated with it, of course, was part of the crisis-- not the only part of the crisis. But any other questions before Hugo?

AUDIENCE: Yeah. On the protecting the investing public front, I was just wondering, like, a lot of people are now using Robinhood and zero fee things like that to invest in the stock market. And companies like Robinhood and Vanguard often sell order book data to high frequency traders so that they can kind of know what's going on and maybe front run.

So I was wondering how that fits into what we were talking about last time where there's no transparency on many of the cryptocurrency exchanges. And then in addition to that, big

institutional investors can, I think, buy upwards of 5% of any stock and then wait a few days before they have to report on that. So that can also have a huge effect on stock price. And then they can, afterwards, dump on people. So how is that different from what's going on in cryptocurrency exchanges?

PROFESSOR: All right. So that's an investor protection one. Was there another one in the-- is this investor protection, or--

AUDIENCE: No, it's a little bit different.

PROFESSOR: A little different. All right. Any other investor protection? Because I'm going to collect them and then [INAUDIBLE].

AUDIENCE: It's about the former. I was a little bit-- it was kind of [INAUDIBLE] to me when you say the blockchain can help to stabilize the financial markets--

PROFESSOR: All right. So that's back to financial stability.

AUDIENCE: Yeah. If it can--

PROFESSOR: All right. Can I hold it? Let me just answer Hugo's investor protection one. So all markets-- not just crypto markets-- all markets are susceptible to some forms of front running. In essence, if you have a client relationship and you get information from your client that might affect the market pricing, you might jump ahead of that client with their information.

Their information might be a buy order, a sell order. Or frankly, it might be some other information. But traditionally, if they have a buy order or a sell order, you have information. And then you're sort of jumping ahead and saying, all right. I'll buy or sell in front of them. That's the classic sort of front running, even though there's other methods. It's not supposed to happen.

On regulated exchanges, you have some policing of it. Even before governments stood in, you could have some policing of it in self-regulatory organizations. In the crypto world, there is Katy bar the door. Anything can really happen. And it's my belief and understanding that many crypto exchanges-- not all of them. Not all of them. But many crypto exchanges are basically trading in front of their customers.

And in fact, most crypto exchanges make markets, as they are both market makers-- meaning

they are buying when you're selling and selling when you're buying. That's the nature of a market maker. It's very typical, very legal, very important function of market. But the exchanges are both market makers, and then they show order books. And so it sort of helps them do front running.

Not that a lot of people necessarily agree with me, I think these markets would be better off if there were some forms of rules about front running and manipulation in markets and the like. On your 5% question, can we take it up in office hours or something? Because it's sort of outside of crypto. But I would be glad to talk about the SEC rules about the 5%. Is this investor protection? And that--

AUDIENCE: I think so. The reading that we had that talked about the Fabric technology, it mentioned something about execute order validate. Does that mechanism tie into the way that front running would work at all?

PROFESSOR: All blockchain technology, whether it's permissioned, like Fabric, or permissionless, can-- if it was efficient and scalable-- could help out, because you could actually timestamp when did the order come in. When did the client's information get to the exchange, and is somebody standing in front?

AUDIENCE: So it's sort of like a cascade that you can't necessarily pause once it starts?

PROFESSOR: Right, right. So if you look at the algorithms at the New York Stock Exchange right now, which are not blockchain-- they're not permissioned, and they're not permissionless blockchain. But if you look at both the algorithms and the data flows, they have very good timestamping. I'm not going to say it's perfect, but they have very good timestamping to ensure when are orders-- basically message timestamping every message that comes in.

And some order books, like the New York Stock Exchange-- some order books are price and time priority, price priority meaning high bid gets hit before the next bid, or lowest offer gets lifted first. That's price priority. But they might also have time priority for any bid that has the same price and any offer that's the same price. So they have to have very good timestamping.

I truly believe you could not use a blockchain solution for the New York Stock Exchange order book right now. Whether you can in 10 years, I'm not sure. But time latency is so relevant in the middle of those order books-- you know, the nanoseconds that matter. I'm going to take this stability question. There were two stability-- and then we're going to move on to the rest of

today's lecture. You're having fun now.

AUDIENCE: Can you explain a little bit more about, like, well, say if blockchain can be a better database so it can help stabilize the financial market? Can you give some examples?

PROFESSOR: So how blockchain could possibly help-- be a stabilizer. A lot of financial instability-- or, beyond the financial markets, instability is a question of resilience. And when things are centralized, you create single points of failure in any system-- really, in military or financial.

You centralize something, you then, thus-- you know what to attack. You can also maybe have higher walls or better moats, but you still know of something to attack. So blockchain, in its decentralized nature, might be a more resilient database, because even if half or two thirds of it goes down, you still have the other third.

I'm going to say something about the New York Stock Exchange again. Whether it's the New York Stock Exchange, the London Stock Exchange, the Chicago Mercantile Exchange, they all are required by their various local laws to have backup data centers. And those backup data centers even have to be lots of miles away if, God forbid, a bomb comes and takes out the center.

AUDIENCE: [INAUDIBLE]

PROFESSOR: What's that? It's called-- Its basically disaster recovery. So maybe blockchain will be more resilient. I'm going to take two more questions and then get back to permissioned versus permissionless. Way back in the corner-- your first name, again, is?

AUDIENCE: Matt.

PROFESSOR: Matt. Thank you, Matt. I should know that.

AUDIENCE: So I'm kind of just curious how, essentially, the nasency, for lack of a better word--

PROFESSOR: The [INAUDIBLE]?

AUDIENCE: Like, the nasency-- how kind of, like, new this market is and how that affects policy, because when you're shaping policy, and you don't necessarily have a bunch of years of knowing how people are going to react to that policy, I feel like it could almost be a chicken and egg situation.

PROFESSOR: OK, I understand. Anybody else with the same theme? No? So the question is, how does it affect policy makers when a whole technology is new? And I would say, we have a lot of history with this. Whether it was railroads, or the telegraph, or the telephone, or television, we have a lot of history. Technology and commercial applications move ahead of the public sector. I mean, it's just inevitable.

The official sector, the public sector-- unless it just basically does what Mark Carney says, and the choice is to isolate something, to sort of put up the moats of a society and says, we can't use that technology here. Unless you have that, technology usually supersedes the markets, and the markets and technology come before official sector. Depending upon the area, it can take single digit years and sometimes decades for public sector to catch up, literally.

But let's take the internet. The internet was being worked on for 15ish years. But the protocol layer that helped take off was the worldwide web in 1991 or '92, and then the security protocols in '96. Just taking financial regulation, the SEC was asked in 1995, could bulletin boards-- there were electronic bulletin boards listing stocks and bonds-- be exempted from being considered stock exchanges?

Well, the people that were asking that were the people putting up the bulletin boards. They didn't want to be regulated. The New York Stock Exchange that was fully regulated, and NASDAQ that was fully regulated, was coming at the other side and asking the SEC to shut them down. They didn't want the competition from the disruptors.

It took three years for the SEC to answer that question. I don't mean answer it, like, with a letter. They had to propose a rule, and they had to do a final rule, and it was three years to do that. And blockchain, I think, we are through some of the big questions. We know how most jurisdictions tax-- T-A-X-- tax it as property and not as currency, and some of the tax issues.

We know, in most jurisdictions, how it fits into, broadly, Bank Secrecy Act and illicit activity. There's very choppy implementation, very spotty implementation. I would say the investor protection side, we're at the early stages. And it's going to take, in most jurisdictions, another three years, maybe, to sort through some of how-- and this is just crypto finance.

I don't know. Matt, does that-- I'm giving you some predictions. Some of it could be multiple decades. We're still, today, trying to figure out-- the public sector's figuring out how to regulate Facebook and Google. I'm going to take one last question, because I've got to do permissioned.

AUDIENCE: [INAUDIBLE] because I was kind of, like-- it kind of answers the side following the technology. But I think, for me, what I was kind of wondering about was this, the way we're like-- as soon as you apply regulations to something that at least a good portion of the market seems to value being deregulated, it seems like a lot of the activity will change, either in scope or scale.

PROFESSOR: So Matt's raising there's a trade-off about bringing something under regulation or into the public policy sphere. I'm probably just one voice of this, but I think it's probably true. There's very few economic activities that grow large that stay fully outside of the public policy framework of a society. It doesn't mean that public policy frameworks don't change, get adopted, get adapted.

The internet comes along, and at first, it's a question of-- you know, with Amazon, is it going to be taxed or not? Is there sales tax? And then later-- you know, at first, it's not. Later, it is. And in some jurisdictions, questions on the internet was liability. And this was a very critical question of early internet was, was there liability for any of the information or the flow of information? I'm talking about libel laws and all the liability issues and so forth.

And so in the US, there's a section of the law in 1996 was passed. And now we're coming back and saying, wait a minute. That gave too broad-- it basically exempted the internet from liability as carriers. But now, that was modified in 2018-- 22 years later-- to say, well, if it has to do, I think, with basically children trafficking and slavery and everything, maybe we should tighten that up a little bit.

So I don't believe any broad economic activity is going to remain fully outside public policy frameworks. And I'm glad to be challenged on that. And I think blockchain, and particularly crypto finance, is at this grappling stage to get in.

So let me move forward, because this is more about permissioned and permissionless. I just wanted to cover some of these. We will cover initial coin offerings and the public policy issues around initial coin offerings in the Howey Test. We will cover crypto exchanges, and we will cover central bank digital currencies a lot in the second half of this semester.

So back to the trade-offs that we talked about already-- the trade-offs of centralization and decentralizations and Coase's work from the 1930s about the firm. This is the cost, remember. This is the cost. As we get centralized, there's more cost of economic rents, single points of failure, and capture. Some fragility, in a sense, in the system. But decentralization has its cost

as well.

You'll notice that these two lines are crossing somewhere. It was my failed attempt to say, you know, maybe there's a balance. Maybe overall, while some organizations will find all the way to decentralization, and some to centralization, I think economic systems tend more towards the centralized side of things. But you can change the slope of these two lines if you want. I'm just trying to give you a framework of thinking about it.

So as we've talked about, the financial sector pretty much favors permissioned systems. The financial sector is saying, going back, no. Too many costs of coordination, governance, security, privacy, and scalability. We're over in the other side. And so that's where they are today. I'm not sure that's where they'll be in five or 10 years, but it is definitely where they are today.

So let's go back down our list, in a sense. I'm going to have a bunch of check marks and x's on the right. Where do you think I'm going to have check marks and x's? This is the same three big buckets, because I can't think of anything. Emily, do you have a point of view?

AUDIENCE: I mean, I think in terms of the permissioned technical features, one of them is obviously that it's not using that proof of work.

PROFESSOR: Not using--

AUDIENCE: It's not using the same proof of work.

PROFESSOR: Not using proof of work. So I had to give away-- you know, reveal the [INAUDIBLE]. All the cryptography that's used in permissionless systems is used in the permissioned systems. It might be used a little differently. I'm not going to say the Merkle trees are exactly the same. But all that broccoli we were eating a few lectures ago are relevant on both sides. Sorry, Alin.

AUDIENCE: [INAUDIBLE]

PROFESSOR: What's that? You--

AUDIENCE: I like broccoli.

PROFESSOR: You like broccoli. A computer scientist speaking. Everything, though, about digital signatures and hash functions and so forth are relevant to both of these. But they're not necessarily relevant to every traditional database, which we'll talk about in 10 minutes or so. But as Emily

said, there's really not-- I said, no. There's not decentralized network consensus. I'm stretching it a little bit, because permissioned systems can be decentralized. There could be five or 10 or 20 nodes.

And so that is decentralized. So I shouldn't have really said no. I should have said maybe, or hybrid. And instead of proof of work, the permissioned systems use a bunch of consensus mechanisms. And I just listed a couple notary nodes or PBFT for Byzantine Fault Tolerance again. But they don't have native currencies. So that is a very big difference-- no native currency.

If you have a solution for your final projects, or you have a solution for some entrepreneurial business that you're going to do in the future that you want a native currency, you're probably more over into the permissionless world. You want to have an incentive structure, something to motivate customers or users, or create token economics.

Token economics is more in the permissionless. I say more because you can create a token even in the permissioned space. We'll talk about it in a moment. And then transaction script or UTXOs. They're not technically UTXOs in a bunch of permissioned systems, but you need some ledger. This last box, if I just called it ledgers, you'd still have ledgers in. So it's really the consensus mechanism in the middle, as Emily said.

A couple of key design features. First, membership's limited to basically an authorized set of nodes. So does anybody want to say, if you were a bank, who you might-- you know, what might you do if you were a bank, and who might you authorize if you're doing a bank-- I don't know. Let's say that it was loans, or if it's Mark Snyderman's real estate. It's real estate loans. Could you ever see real estate loans going on a blockchain, Mark?

MARK SNYDERMAN: Loans, maybe. Loans could.

PROFESSOR: All right. So--

MARK SNYDERMAN: Loans aren't traded as much.

PROFESSOR: So if real estate loans were on a permissioned blockchain, who might be that membership, the limited-- who would-- it's not just a rhetorical question. Who would actually care about the database of the loans?

MARK SNYDERMAN: Broker dealers that are active in loans, institutional investors that are active in loans.

PROFESSOR: So the broker dealers who are actually trading the loans, and maybe the investors. Alon?

AUDIENCE: Yeah. Just rating agencies when you securitize those loans--

AUDIENCE: Loan servicers.

AUDIENCE: Loan servicers.

PROFESSOR: Amanda, loan servicers. So maybe loan servicers, maybe the rating agencies. So it's basically, who has a need and needs that data? I'm not sure that this is the right community, but it's the discussion I'm thinking about. And again, as you're thinking about-- I'm jumping again to a little bit final projects, but when you're thinking about who actually needs data and who has a reason to amend the data, or write to the ledger-- because if you don't have a desire and a need to actually amend or change the data, move value in the system, you might not need an open database. Please.

AUDIENCE: When we were talking about that additional layer of blocks, is that layer also-- can you change the membership with that layer?

PROFESSOR: I'm not sure I follow your question. When you say an additional layer of blocks--

[INTERPOSING VOICES]

PROFESSOR: Oh, I'm sorry. Layer 2.

AUDIENCE: Yeah. Can you alter the-- because it's a different level of refinement of information that's stored.

PROFESSOR: So what Kelly is asking is, we've talked about how to make permissionless blockchains more scalable by having a layer 2, like the Lightning Network. That's what you're referencing. So in permissionless systems, it's open to everyone, even though if you're opening up an individual payment channel in the Lightning Network, it's really just two counterparties opening up a channel.

So in a sense, you've already narrowed the scope, because you might just have a payment

channel between two parties-- some side chains or multiple parties. Lightning Network and payment channels tend to be two parties. So I don't know if-- was that what you're asking?

AUDIENCE: That network in and of itself is a mechanism of membership.

PROFESSOR: The layer 2 can be a membership. That is correct. But it's a technology that's available to everybody. So it has attributes where you can open up bilateral channels. James.

AUDIENCE: I was just going to say, for permissioned blockchains, couldn't you imagine that the layer 1 would be, say, the Fed with all of the big commercial banks? But in effect, if you're thinking about a different layer, you could have another layer on top of that, which [INAUDIBLE] central banks. So you could naturally--

PROFESSOR: All right.

AUDIENCE: --have two layers of deals with--

PROFESSOR: So where we're headed is, is do permissioned systems have the same need to have a second layer as permissionless? And even if they don't have the same needs, might it actually provide something? So I would say, I don't think they have the same need to have a second layer, because they're more scalable, they're more efficient right now. And they're already closed clubs.

But even if they don't have the same need, they might actually want to put a second layer on top. And some of them actually do this right in their technology. And it's what I put up here as the second and third bullet point. The transactions can be limited to only authorized known participants. So in many permissioned systems, it's a one broad technology. It might only be 20 people that can authorize transactions.

But now in some transactions, it will only be Anton and May. And in other transactions, it will be Alpha and Amanda. So I might not be able to-- by the way, Alpha might be Goldman Sachs, and Amanda might be Barclays. And then it might make more sense. And Mark might be Fidelity. And I don't know, am I the US Department of Treasury in this one? Mark and I both started out in finance. I just went off to public service later.

But so Corda and Hyperledger and many of the private blockchains literally allow for partitioning right in the blockchain. I don't know if you'd need to put a layer 2 on top, because they allow for partitioning and segregated pools of authority inside of the blockchain. I'm sorry?

There was a question, I thought. Oh. Oh, yeah.

AUDIENCE: [INAUDIBLE] you see insurance companies, like title insurance, as part of this.

PROFESSOR: Can you speak up? [INAUDIBLE].

AUDIENCE: Insurance companies for title for the houses--

PROFESSOR: Right.

AUDIENCE: --I think blockchain could be really helpful, because sometimes you have the trust issue around who owned the house before you, or the title where it goes backwards in history. So I think title insurance companies would be part of this blockchain in terms of [INAUDIBLE].

PROFESSOR: So your point is, is that titling of real estate could be an important part of blockchains, and as [AUDIO OUT]

MARK SNYDERMAN: Probably someday, but every little town has its own system for keeping property records. And getting them all to cooperate in a blockchain kind of solution seems remote. They don't think they have a real problem that needs solving.

So yeah, maybe someday. But I doubt it will happen anytime soon. But it makes some logical sense. And that would probably be a permissionless system, because there's not a huge amount of times a piece of property transacts, right? So it's not like moving money around the world. It's a much simpler, less frequent event.

AUDIENCE: Yeah--

MARK SNYDERMAN: And land records are public. People often have to go to the town offices to look at them.

AUDIENCE: Yeah, you have to pay a lot of transaction fees, whether you're transacting on a plant or anything that involves real estate here in the US. You have to pay considerable amount of fees to the title insurance companies. And in my mind, that could eliminate that role if you have blockchain and [INAUDIBLE] where the system.

MARK SNYDERMAN: Maybe, but you're paying money because you're asking--

AUDIENCE: Somebody to--

MARK SNYDERMAN: --them and lawyers to make sure the title's free and clear.

AUDIENCE: [INAUDIBLE]

MARK SNYDERMAN: And there's all sorts of claims on a title to property-- somebody that fixed the roof, or the utility company that has an easement through the middle to put lines and so forth. So there are some complications that are different than just transferring money.

PROFESSOR: So to bring it back, to broaden it out, the que-- it's Rahim?

AUDIENCE: Rahem.

PROFESSOR: Rahem. Rahem's question is, is, well, what about real estate and title? Might that be appropriate? And as Mark has given us a sense of, yes, it might be. But we're back to that sort of thing of the collective action issues that we've talked about in previous classes-- the collective action of many municipal authorities that keep the land records, that keep the real estate records.

Yeah, it might help, but why do I need to do this? And it's also a [INAUDIBLE]. It's a low volume, low transaction. And yet, it could be an enormous benefit, because there's something called title insurance. And title insurance trying to clean up the title and making sure that something is free and clear could be recorded in the future.

So I'll be a long-term optimist. I don't see this one being solved in the next handful of years-- single digit years-- particularly because of the [INAUDIBLE] collective action issues. I'm sorry. We have somebody here who's going to take the other side before I give my conclusionary estimate. Yes?

AUDIENCE: Yes. That's exactly my startup. The first phase is collecting all the data from all those munis departmentals [INAUDIBLE]. The information is there publicly. So yes, they will not probably immediately adopt a Corda node and record their stuff. But you can publicly pool that information and then use that information and record that information on the blockchain. And then once I become stronger and bigger, then they will probably have to adopt it.

PROFESSOR: All right.

[LAUGHTER]

So maybe I'll move up my estimate from double digit years to single digit years. But I think it's going to be, with all respect, some time. Pria, then I'm going to move on.

AUDIENCE: So I used to work at Habitat for Humanity International. So access to proper land rights or land title, that was a big issue for us overseas, not so much in the US. And so I could see a real application there, where in several countries where there is no land record, or there are no title systems, or they're buried in layers of obfuscation. This is a great solution to get something like that started in those contexts, where there is-- establishing the property right of record could be of immeasurable social value.

PROFESSOR: You know, I agree, and I think there's been a tremendous amount of literature in the last 24 months around whether blockchain can help free up a lot of illiquid capital and assets. I'm just saying I'm probably closer to Mark's thinking than to Alon's thinking. I think it's going to take some time.

AUDIENCE: But depending on the context, right? In the context--

PROFESSOR: Context, the country, the system, the legal system, how decentralized, and how tough the collective action issues are. So just going back to private blockchains, technical features-- let's go back. Membership limited to authorized nodes. Transactions can be partitioned as well. It's kind of Kelly's point.

Right in the technology, you can partition and segregate information. So data and ledgers can be partitioned because transactions can be partitioned. That doesn't mean you can't have a layer 2. I'm just saying there's a lot less need for a layer 2, because they do it in the data structures itself.

The consensus is permissioned private protocols. They do have a consensus. Somebody has to agree on the next block. But it's a tight, limited group. It does use cryptography, but often, there's something called a registration authority. The registration authority is helping mask data. So they address privacy two ways. They address privacy because it's a smaller group. They can actually see the whole network.

But even within the network, even on the network, they're further addressing privacy that Alpha's and my transaction, Amanda maybe can't even see, even though she's on the network, because it's encrypted. And then there's sort of what's called a registration authority,

or authority within the system, that can unmask it. Yes.

AUDIENCE: I just have a question about the-- how is a segregated system a subgroup of two [INAUDIBLE] different from a layer? If [INAUDIBLE] is already doing subnetting off of calculations, or whatever it may be-- transactions-- and then the net [INAUDIBLE]--

PROFESSOR: All right. So I've got another question I have to follow up on. I have to follow up on Brotish's Corda question, and now James' question about, well, wait a minute. How is this partitioning different than a layer 2? And it's beyond my knowledge, but I'm going to see if I can get it for you. That's a good-- they're both-- they're good questions.

And then smart contracts-- yes, smart contracts can happen on these systems as well as permissionless systems. IBM-- they say they use chaincode. But they say chaincode really could be any language, at least they advertise, and no native currency. So that's kind of the technical-- not deeply technical. It's not like learning hash functions.

But yes to cryptography. Well, they partition the ledgers. The consensus is closed loop. Yes, they have smart contracts. But they can even have additional privacy. But it comes at a cost. There's an authority that has to protect something-- a registration authority inside of it. Oh, I forgot. The code is generally open source. It does not have to be open source. Hyperledger is open source, but it doesn't have to be open source.

So this was from one of the readings. I'm just putting up that chart that was in the reading. And I just found it helpful. It's a different way. It's not Gensler's way. It's somebody else's way of thinking about Ethereum, Hyperledger, and Corda. I'm only using Hyperledger and Corda because they're two of the biggest private platforms. There are many others.

Different programming language-- you might say, from a business point of view, who cares? And to some level, you're probably right. But you're not completely right. I mean, there's probably more that people can write on top of Hyperledger Fabric. They say more developers could work on that than Solidity.

Governance-- that's the governance of the system itself. They all can do smart contracts. We've talked about consensus. And the scalability is much harder. Ethereum, remember, almost crashed on CryptoKitties last December. And I shared that story about one initial coin offering was 30% of the Ethereum network on the one day it was closing [INAUDIBLE].

DTCC, in a given day, can do as much as 100 million transactions in a day. That's the

Depository Trust Corporation. Ethereum does about a million and a half transactions a day, and Bitcoin, about 400,000 to 500,000 transactions a day. So you know, we've still got a ways to go on this scalability.

So what about traditional databases? I think that to talk about permissioned versus permissionless, a lot of people, even some of my colleagues here at MIT, says, well, if you're talking about Hyperledger, Corda, and Fabric and Corda, that's like Oracle. That's just a traditional database. That's not really blockchain.

The Bitcoin and blockchain purist would say, if it doesn't have Nakamoto consensus, forget it. It's not a member of the club. That's not how I've chosen to teach that this class, as you know. I think both are relevant, possibly, to business solutions, and it's worthwhile to think of them.

But so what separates-- and this is not in the reading, so I'm just going to, you know, kind of-- but what separates it versus a traditional database? Well, back to the basics. Permissioned private blockchains have append-only logs. You're adding-- I know. Thank you, Brotish.

But basically, they have append-only logs. Traditional databases-- and I'm at the edge of my knowledge-- you can create. You can read. You can update. You can delete. Again, I'm taking the mainstream traditional databases, or what's called CRUD, if you wish-- C-R-U-D. Whereas these, you always are adding to the database.

Two, these databases use cryptography to have commitment schemes. You may remember, what is a hash function? It not only compresses data, but it means you're committing to the data. And when you finish *The New York Times* crossword puzzle, you can actually send it in.

And if it's identical to-- and hash it. And if you remember our discussion about *The New York Times* crossword puzzle, if it's hashed, and the hashes match, voilá. You solved *The New York Times* crossword puzzle. So you can have commitment schemes for the data. And it can be distributed. Yes, Joequinn.

AUDIENCE: So even if it's append-only, if you take away the proof of work, you can rewrite it in a very quick manner.

PROFESSOR: So Joequinn's raising a very important point. So even if it's append-only, you get rid of proof of work, can't somebody go in and rewrite it? Permissioned blockchains make a different trade-off on trust. Permissionless system say, we're going to address trust through this proof of

work. And at least 51% of all of the network has to, in essence, agree and validate, and the like.

Permissioned basically are saying, I'm going to trust the 10 or 15 or 20 nodes that are in the system can validate against each other. And so there's something about the club that's authorized in the network. But they're still using append-only. You're right that within those 20, somebody could try to rush through and do a whole entire new append-only. But then within the club, it's exposed.

AUDIENCE: If the club agrees that the last two days have to be rewritten, they can do it in a very easy way.

PROFESSOR: Correct. But I would contend that even in Bitcoin, if 10,000 nodes decided to rewrite the last two days, they could. It's a--

AUDIENCE: Taken a lot of time, because they have--

PROFESSOR: Yes.

AUDIENCE: --to find--

PROFESSOR: That's correct.

AUDIENCE: [INAUDIBLE]

PROFESSOR: That's correct. So what Joequinn's saying is in Bitcoin, what protects against that is partly the proof of work, and partly that it takes 10,000, or at least 51% of them, probably, to rewrite the last two days. The economic incentives in Bitcoin is, is why waste all your computer power and electricity and so forth doing that when you may as well just go forward?

I think Bitcoin could be susceptible to state actors. I think, you know, if North Korea wanted-- or Russia wanted-- to spend probably single digit billions, but at most maybe 10 billion, they could overwhelm the whole system and bring-- they could do a 51% attack by buying up enough mining equipment, the ASICs, and just bigfooting the whole system.

But it's multiple billio-- and there's academic papers on this now. It's single digit billions. A state actor could-- an individual wouldn't want to do it, because you'd crush $110 billion market cap down to [INAUDIBLE]. So that would be kind of unwise. This is a very critical part of what a private blockchain-- to me, economically, what a private blockchain can do and facilitate better than a traditional database.

I'm not saying this list is the only list. I'm not even saying this list is completely the right list. This is Gary Gensler's list trying to say, what's the business that separates traditional blockchains? Append-only timestamping. Some cryptography and schemes that makes the data immutable so you can put it in a ledger-- so it's back to ledgers and so forth-- and thus, finality of settlement. Does anybody want to remind the class what settlement means? Anybody? Take a shot. Where's my accountant? Aviva's not here. Oh, please.

AUDIENCE: [INAUDIBLE] do with the UTXO.

PROFESSOR: No, forget about UTXO. Just tell me what settlement means.

AUDIENCE: Oh, like, making off your debit and credit.

PROFESSOR: Yeah, debits and credits. Settlement means changing the data in a ledger, and doing it with finality. In essence, do I have $10 or $11? A payment settlement system is when you finally say, I've got $11, no longer $10. And Amanda's got $9 instead of $10. You went down. I went up. Is that all right?

AUDIENCE: Yeah.

PROFESSOR: Thank you. You'll hear a lot about clearing and settlement. The word settlement means to finally change the data in a ledger, and that we're not going to come back to it. It's done. It's final. If we're moving something of value-- and the value could be grapes. The value could be diamonds. The value can be real estate. The value can be money.

But if we're moving something of value and storing it on a ledger, it's more adaptable to blockchain. If you're doing some database that has nothing to do with things of value and ledger, you don't need final immutable settlement. I would contend you probably have less reason to use any of this blockchain stuff. Zan.

AUDIENCE: Can you maybe talk a little bit about a real-world implementation of this? So I saw recently that Walmart is forcing their suppliers to basically add themselves into this private blockchain to basically track their supply chain. I'm having a really hard time understanding why that needs to be on a blockchain, whether permissioned or nonpermissioned, and why that needs to be.

PROFESSOR: So the question is, why is Walmart putting supply chain with a bunch of agricultural products on a blockchain? Agricultural products are something of value, whether it's corn, wheat,

grapes. It's something of value. And when it moves from one owner to another owner, if you keep that on a ledger, you can record that Amanda has the grapes, and Gary no longer has the grapes.

And another thing that blockchains help with is they lower the cost of reconciling multiple databases. We could keep-- as in agriculture-- we can keep separate ledgers, separate databases. The farmers keeping their database. The wholesaler with the grain elevators are keeping their database, and up the supply chain, from the farm, to the grain elevator, to the millers and merchants, all the way to General Mills, all the way to Kroger and the store. Right now, those are multiple databases that, by and large, don't have to communicate.

So the question is, will Walmart get to the place where that's a good idea? But I'm just pointing out if you're moving things of value where you want to keep final settlement that you know who owns that thing of value in ledgers, and lastly, if you want to lower any reconciliation-- if you have multiple ledgers and things of value, blockchain, I think, is more valuable. Zan's asking, well, is that Walmart? I don't know. We're going to find out. Tom, and I've got about seven minutes to finish.

AUDIENCE: There was a talk last year. Somebody [INAUDIBLE] came in and talked about the-- they were then piloting this program. But the example they used was, in E. coli outbreak in their spinach supply, rather than taking a whole supplier, an entire wholesaler offline and recalling all of that product, through the blockchain, they could trace it to a particular farm and a single point of origin almost instantaneously and just take off a much smaller portion of it.

PROFESSOR: So let me do this. Let me just-- hold on. I know we've got two questions here. Let me just hold on, just for-- is that all right? All right. We got permission. So this was what we talked about earlier-- Coase's trade-offs of costs. Let me try another one, which is going to be my shot at blockchains and traditional databases.

So one is access control. Who has access to the ledger? Who has access, if I might, to the data? Three different types of approaches we talked about-- open permissionless, multiple permissioned, and client server. I'm using the word client server just to say traditional database. You can use another words. But I'm just trying to say three different types of data structures.

And to Zan's question, why would you be in one bucket versus another? And I'm saying this. If you're a venture capitalist one day, and somebody comes in to you with a blockchain solution,

this is the same thing. Hopefully, you'll make it better. This is just my approach to it.

Public blockchain-- do you need, basically, public write capability, that lots of people can write to these ledgers? Do you need that somewhere? Secondly, do you want some peer to peer transaction capability across the distributed ledger? Do you kind of not want any central intermediary? Maybe you don't want the central intermediary because they're slow and sluggish. Maybe you don't want the central intermediary because they have a lot of economic rents.

It doesn't matter to me why you want to get rid of the central intermediary. But if you want to get rid of a central intermediary, or lessen their control, or lower their control, raise peer to peer transactions, have a lot of public writing-- oh, and by the way, if you want some token economics, you're probably somewhere over here. I'm not saying you have to have all four. But to me, those are the kind of three or four things that are floating around why you might be over there.

Private blockchains-- well, maybe you actually don't want public write capability. You need private. Whether it's just the Australian Stock Exchange or 15 to 20 club deal, you still want kind of multiple people to write, but you want it to be private. But if you still need finality of data and an append-only log, that you need this appending-- the log, and you need some public verifiability, that you still need that data to be verified amongst-- and this public means 15 or 20 players. But you need it to be able to be verified-- so the trust mechanism is not thousands and open. The trust mechanism is 15 or 20 or 5 parties. But you still need it-- you might be there.

Where I come out is there's some cases that you just don't need any of this. There's a trusted party that hosts the data. Your trust mechanism is one party. The trusted party can do the-- I use the letters CRUD. That's the create, and update, and delete, and so forth. And that's based on client service architecture, this client server architecture.

There's always, in that circumstance, somebody right in the middle that basically owns, updates, governs that whole architecture. My business judgment on this is if you're moving things of value, you want those things to value to have some final settlement and immutability. And immutability append-only logs give you some of that final settlement.

We talked very briefly about a lawsuit that was 300 plus years ago-- the Crawford case in Scotland that you won't have to remember. But this-- watch this. So steal this from me. Just do

me a favor. Just steal it. OK. Right now, I have a right of action. But if you give it to-- who are you going to give it to? I don't have any rights against you. No. Well, wait. It depends whether he knew you stole it from me. But it's gone. That's final settlement. Those $2 are gone. That's final settlement. It's immutable. I can't get them back. What, Christopher? You want them?

AUDIENCE: I just was asking for the money.

PROFESSOR: You were asking for the money. I just use that as a visualization. Money is a social consensus and a social construct. But if you think of it in terms of ledgers-- look, the money's gone. I can't get it. That's it, you know? That's good. You all go to Sloan, I can tell. Yeah, yeah. But it's an important concept. I think of this whole that way.

So there were two questions, and then we'll-- and then this is the decentralized end. Bitcoin and Ethereum are kind of at the decentralized end. I would contend Bitcoin's more decentralized than Ethereum. And centralized databases-- initial coin offerings that we'll talk about later, I think, are actually maybe a little bit more centralized, even, than permissioned blockchains. But we'll get to that.

AUDIENCE: No, mine was already answered. And then the other comment was more about the supply chain link. When you think about the millions and millions of dollars, the element of transparency that blockchain kind of brings in to all the parties probably saves an insane amount of money to what you're talking about kind of reconciling all the databases.

PROFESSOR: So we're going to talk about finance next Thursday and some of the strengths and weaknesses in finance, and some of the attributes, and you know, one of the readings-- Sheila Bair-- and there's a bunch of optional readings about what's happened after the financial crisis and so forth. And then we're going to talk about the economics.

But I've had three or four groups come in already talking about the final projects. So I'll just say, think about whatever you're working on as this new technology-- blockchain-- whether it's permissioned or permissionless-- either one-- does this new technology really address some pain point that you're trying to solve, whether it's about payment systems or-- actually, there's a group that's talking about doing supply chain on wine. And I figured, why not? I'll probably approve it.

But it's, what is the pain point that you're actually trying to solve? Or will decentralized peer to peer networking somehow create a business opportunity in a new model? It might not be a

pain point. It might be a business opportunity that decentralized systems solve. Or it might be an opportunity that token economics can help solve.

But if there's no pain point you're solving, no token economics, no decentralization peer to peer, I ask you to use your critical reasoning and move to the next use case, because this is really about-- this is a business class. This is about finding places for this incredible set of new technologies in the context of markets and to have a really healthy sense of ground truth about what's possible. If not, traditional databases. Move on. I'm not looking for projects at the end of the semester that are using traditional databases. It's got to really use blockchain. So I thank you. I'll see you next Thursday.