[SQUEAKING]

[RUSTLING]

[CLICKING]

**GARY GENSLER:** So we've got a lot to cover, but I'm going to start with a little background about the internet and the payment riddle; something about money, which is at the core, really, of all classes on finance but we usually take for granted; and then Satoshi Nakamoto's innovation-- who was Satoshi Nakamoto, what is that innovation; a bit about crypto markets; the blockchain technology use cases-- and then the core really is, how to think about viability of those use cases; a little touch on central bank digital currencies; and ground truths.

So, a lot to cover. If we don't get through it all, we will talk about this again when we talk about payments in class 6. In terms of some of the readings, I shared with you two write-ups that were done for a class that Neha Narula and I teach, an online class called Cryptocurrency, which is available through MIT. And those two write-ups, the "Economics of Money and Technology"-- I'm sorry, and the "Responses of Big Finance" sort of give you some of the challenges and how to think through these technologies.

Also, the Bank of International Settlement did a review just earlier in 2020 about the central bank digital currency space, because so much is going on there. And particularly after Facebook announced their Libra project in June of 2019, many central banks took note and said, wait, maybe there's something going on here that we too need to do more. Now, before Facebook Libra, there were many projects the bank-- one of the world's largest central banks, the Riksbank in Sweden, was already looking at an e-krona project. There were other projects. But all of a sudden, that Facebook Libra project kicked into high gear central bankers around the globe, and particularly China's look and review and announcements around the Digital Currency Electronic Payments Project also got kicked into gear.

So regardless of where you come out, whether blockchain technology, cryptocurrencies, are getting rolled into the stack, rolled into the technology stack

of big finance. What we can say as of 2020, what's really the case, is that cryptocurrencies and blockchain technology have at least been a catalyst for change, an important catalyst for change pushing upon big finance, pushing upon central banks to reconsider how they do payments, how they do the basics of money.

And I laid out a few questions. Again, Romain will look for some hands. We're going to keep this a little shorter than we usually do, just because we have so much to cover, but, how does Bitcoin fit into the history of money? What are the strategic and tactical considerations assessing viability and value propositions? And how are these central banks thinking about what they're doing?

And Romain, if we can just see if we could get one or two people in kind of each of these three questions-- and these are the essential questions I'm going to try to cover in the next hour or so.

**AUDIENCE:** OK. Sounds good. Who would like to get us started? I'm watching for your blue hands.

**GARY GENSLER:** Quiet day today.

**AUDIENCE:** If you wish, Gary, I'm also happy to cold call.

**GARY GENSLER:** All right. Well, I'm going to start. I'm going to kind of just go. But I hoped that everyone would come in. I start with this scene-- and I don't know anyone who wants to raise a blue hand and tell me what movie this is from and the era.

But this is the opening scene of a movie from the mid 1990s, *The Net,* 1995, Sandra Bullock. Now, I start with this, because Pizza Net was actually real. Now, this cyber security sort of spy thriller with Sandra Bullock sort of cracking through the computer network-- remember, let's place this. Mid 1990s.

It was only the early 1990s that Tim Berners-Lee, associated with MIT, actually came up with the protocols that connects the world wide web. The internet had been around for some time, coming out of DARPA and the Department of Defense in the US and academic institutions. But by the early '90s, it was actually something that

those of us in the public could use beyond universities, beyond the defense establishment and the like.

But what hadn't been solved, what hadn't been solved by 1995, was how to move money on the internet. And Pizza Hut founded something called Pizza Net, which is thought to be the first commercial use where you could actually order something online-- just 25 years ago-- order something online through Pizza Net.

There was only sort of one problem. You ordered the pizza, and guess what? You couldn't pay online. Nobody had figured out how to pay online. You had to have the pizza delivery at your door, and you paid.

So just think. It's in the middle of the corona lockdown, we're sheltering at home. And if it weren't for these inventions of 25 years ago we're about to discuss, you would be paying for that pizza at the door when the delivery truck arrived, or for your groceries, or for any other household goods that you have.

So this riddle, what I call the payments riddle, what others call the payments riddle, was at the core of this new technology, the internet. Now, the internet has been fully adopted into the technology stack of finance by now. But in the mid 1990s, it was, in essence, fintech. But the question is how to move value on the internet, to do it securely, efficiently, and really importantly, similar to the packets of data that move on the internet as packets of data, and thus peer-to-peer.

So the internet doesn't really have central control. All the data that we're live streaming right now between and amongst us, between 78 participants on this Zoom meeting right now, is through packets of data that's not through one central control, even though we think, well, Zoom might be controlling all this. But the challenge really was, how could you prohibit double spending? How could you send a packet of data to one person and ensure that that packet of data wasn't also sent to another, in essence, double spending? Having some data like an email that we might send to two people-- they were both reading the same email, they don't know that each are reading the same email.

So that was this payments riddle-- secure, efficient packets of data, but avoiding double spending. Lots of challenges, lots of attempts. And there were dozens of attempts. Somebody even went to go in to get patents and started businesses,

raised money. Some of them through the earlier days of venture capital were backed like CyberCash and DigiCash, and E-gold, B-Money, all of these failed. All of them, and dozens more beyond what I list here in the 1990s, and the hurdles were, well, of course the same hurdles that any startup would have around merchant adoption-- would the stores actually adopt it-- but this issue of double spending.

And the only sort of solution to double spending was using centralization. There was one central computer, one central controller, to avoid the double spending. Or the other side of it, how did you form consensus? If you didn't have a central controller, how to form consensus on the say of who had the money and who didn't have the money.

So this sort of central payments riddle, a big issue in the 1990s, attracted the interest of a cryptography group called the cypherpunk community. I kid you not, it's called cypherpunk community. It was an email list that had started in the late 1980s and had gone on for some time. And so there were early digital solutions that were a little bit different.

And some of the cryptography that was brought to it was not brought from the cypherpunk community, it was brought to bear from great cryptographers, some of them at MIT, some elsewhere, that came together by 1996 with a solution. It's this updated today the same solution we use now-- secure socket layer and transport layer security. These two protocols, on hop of Tim Berners-Lee protocols about the world wide web from four or five years earlier.

These are the main protocols-- there are many others that were added. But these are the main protocols that allowed us to secure the internet. It's how we do it right now-- a transfer of data that's secured by the use of cryptography. And what did that lead to? That led to a lot of things where we could accept Visas and MasterCard, American Express, by the mid 1990s.

Amazon, eBay were both formed in 1995. It's a founder's dream to get formed right when a technology is transitioning. If Amazon, if Jeff Bezos had been formed in 1992, would it still have been around by 1996 when the secure socket layer and the cryptography was there for him to get going? If Jeff Bezos had decided to form it in 1998 or '99, it might have been too late.

Now, there's a lot of things that Amazon got right and Visa's got right. But I'm saying timing was one that was remarkable. PayPal came along in 1998. And interestingly, the first mobile payments was actually Ericsson teaming up with Telenor in 1999. Now, that product is not around today-- or maybe somebody will correct me and say there's still a little bit. But one of the early ones that really took off was Alipay and then M-Pesa in Kenya.

Now, All of this still left the payments riddle. That payments riddle was still there to some in that cypherpunk community. Now, the internet could get commercialized, the internet could move on. We had this way through cryptography to secure payments. But there was still this question.

And it goes to the heart of, what is money? And so I'm going to turn a little bit to chat about money, but just see if Romain has any questions so far.

**AUDIENCE:** Nobody at the moment.

**GARY GENSLER:** OK. So I'd like to go back in time. I'd like to go back 2,300, 2,400 years in talking about money. It's not the first time money was discussed, because money was really an invention of humankind thousands of years before that. But I'd like to go back to Plato and Aristotle.

Plato did not write extensively on money. But what he did write is interesting. It's that money is a symbol devised for the purpose of exchanges. To think, you and I were going to exchange something-- at the time, maybe it was a goat for wheat, maybe I needed the goat today, you needed the wheat tomorrow-- but we can use this symbol, as Plato wrote, as a purpose of that exchange.

And interestingly, separately Plato wrote-- Plato wasn't in for using gold and silver for money. Now, this is interesting in contrast to Plato's student, Aristotle. Now, Aristotle wrote extensively about money. It seemed like Aristotle wrote extensively about many things, but one of them was money.

And Aristotle wrote that it solves the problem of commensurability-- the same sort of issue that Plato was grappling with, commensurability. You need rice, you need grains, I need goats. How do we have some commensurability between that?

Or the second point here, money is a guarantee that we have what we want in the future. So this is sort of a time commensurability. I need something today, you need something tomorrow. So these two forms of marrying up needs and wants and values-- Aristotle talked also as a philosopher about, what is values? And then talked about four absolute values.

Now, I hate to disagree with Aristotle. But, you know, over time, there are many of Aristotle's great writings that have been challenged-- about the Earth and about the solar system, about the heavens, the skies, the bodies. So why not say that maybe Aristotle didn't quite have it right about money? He talked about durability, portability, divisibility. I still sort of agree. And most monetary economists would agree on that.

It's this fourth point-- did it have intrinsic value? I find myself more associated with Plato, who had said it was just a symbol. It's but a symbol. And so today when we think about money, we often think of six key characteristics. Is it durable, portable, divisible? These were-- Aristotle seemed to-- 2,300 years later people still tend to agree.

But rather than intrinsic value, that it's uniform, acceptable, and stable we'll talk a little bit more about that when we get to the economics of cryptocurrencies. But remember, instead of intrinsic value, that it's uniform; that it's the same unit of account within some local or national economy; that others accept it, because if others don't accept it, how can I know that that which I take today I can use tomorrow?; and then its value is stable. And we think over the last 300-plus years about institutions that help ensure that currency value is stable, we call them central banks.

So instead of an intrinsic value, that we humans create some form of acceptability, uniformity, and stability. Questions?

**AUDIENCE:** None so far, but I'll give our students a few seconds to raise their hand if they want to. Yes, we have a question from Hassan.

**GARY GENSLER:** Please, Hassan.

**AUDIENCE:** Hello, professor. Yeah, my question is, when you said that people could exchange things for other things as a mean. So I mean, how could the cryptocurrency survive if there is no intrinsic value in it and it's so volatile? And when you said that central banks make sure that these currencies are stable, it's because-- like for instance, in my country the central bank has to have gold and other currencies to support our currency, our local currency.

So I'm just baffled to see like someone speak about, well, you know what, it's only a symbol. OK, I know that it is a symbol, but it has to have some value in it. Otherwise, the other party would not accept it as a means of exchange, if that makes sense.

**GARY GENSLER:** So Hassan is associating himself more with Aristotle than Plato, and I find myself more associated with Plato than Aristotle. So this is a worthy debate that's gone on for well over a couple of thousand years.

But when I say that it doesn't have intrinsic value, and it's more about uniformity, acceptability, instability, think about-- I'll take the US dollar. I don't know-- what you're country?

**AUDIENCE:** I'm from Bahrain.

**GARY GENSLER:** So I'm not as familiar with your central bank. But let's take the US dollar instead of Bahraini. If you walk into the Federal Reserve, the US Federal Reserve, and you have $100 bill-- you know, paper currency, $100-- what will they give you? I mean, other than that they would probably send you on your way and the security guard would say, we're in this coronavirus period, nobody's allowed in the building.

But what would they do if you showed up at the New York Federal Reserve or the Richmond Federal Reserve, and you said, I want something for this $100?

**AUDIENCE:** I suppose that a few years ago that they would give you like gold, if that makes sense.

**GARY GENSLER:** OK. So we got rid of that in 1933. So "a few years ago" would be like at the beginning of the Great Depression under President Roosevelt. What would they give you in 2020?

**AUDIENCE:** They would give me, I think, the government's-- that the government basically

would support this piece of paper, I assume.

**GARY GENSLER:** So you're getting at the government which sort of insure, through its means and methods, that it's acceptable by other citizens, and it's acceptable by the government. How do they do that? They say, well, we'll take it for US taxes. We'll take it for Bahranian taxes. And in most economies, the governments are anywhere from a quarter to a half of the economy in some way, so they will accept it for a government.

They'll ensure that other people accept it through what's called legal tender laws. Through the coercive power of the state, they will say, others must accept it. And this is not a new thing. Genghis Khan was doing this in China, and it was pretty coercive. It was kind of [CLICKS TONGUE] the coercive power of the state, you must accept the official currency.

So acceptability can be accepted by the government. It could be acceptability that others must accept it for all debts, public and private. And they can work on stability and form central banks to ensure that-- now, what does it mean by stability? It means addressing the official sector to the supply and pricing of money. Supply and pricing-- the supply we talk about the monetary supply, the pricing is through interest rates.

But can you go into the US Central Bank, can you go into Bahrain and actually get gold? No. You can go in and get a $100 bill, and they might give you five 20's. If you really want, they'll give you 100 1's. But you still have just a physical piece of paper or a digital representation that I would contend-- I'm sort of with Plato-- it's just a symbol.

It's a symbol that our society, no matter whether it's small or big, has come together. And it represents a store of value. It represents a means of exchange. But it frankly doesn't have intrinsic value the way Aristotle talked about it. It has only value because we humans place a value on it.

But Hassan, are you on still on the other side? You feel gold has intrinsic value.

**AUDIENCE:** Yes. I think because it's a scarce metal. And I know that prices could go up and down, but still I know that I could sell it one day and get money or get--

**GARY GENSLER:** So gold is what we now call an element. It's on the periodic table. It's got great attributes because it's scarce. It takes a lot of human resources to get it out of the ground.

The other thing about gold, it's divisible, it's portable, it's uniform. It doesn't oxidize, so it's a really good base sort of element in that way as well. And now we have, give or take, 10,000 years of acceptability, that it's a human shared narrative. Some of it not good, some of it about war, and slavery, and all sorts of challenges in human history. But gold, and to a lesser extent silver, were very acceptable and stable.

But think about this for a moment. All the world's gold that's ever been mined, if you take all of that gold, it can fit in four Olympic-sized pools. Four Olympic-sized pools, you. could put all that gold into one space. Now, it's spread around the world in jewelry and secure vaults. But it's only four Olympic-sized pools.

I would kind of contend that's just a symbol. Again, it has some kind of features that make it durable, and it's got 10,000 years of human narrative and acceptability. And I can assure you that those who are really in times of trouble would probably take a piece of gold-- if it was really in times of war and despair, take a piece of gold over Bitcoin.

But on the other hand, we're going to get into what Bitcoin is and how it creates some digital scarce store of value. So Hassan, we could keep going with a lively debate, but I hope that helps at least frame the sides of this thing.

**AUDIENCE:** Yeah, I just have one thing to say. Now, I mean, if the US for some reason collapsed, what would happen to the whole monetary system? I mean, it's very dangerous, if that makes sense. Because--

**GARY GENSLER:** You're asking what happens if a nation's currency collapses. And we have history of that. We don't have recent history when a world's dominant currency collapses, but we've certainly a history of many countries' currencies collapsing. In fact, right now Venezuela's currency basically collapses.

And what happens in countries that where the currencies enter hyperinflation and start to collapse, you start to see communities reach out to another symbol, some other symbol that is acceptable and has stability. It might be in the common time, in

the current time, that those people will reach out to the US dollar. And your question is, what if the dollar collapses?

But in monetary history serves that usually that when a currency goes bad, people reach out to the better currency. And it could be a neighboring country. It could be a different metal, like when we had challenges between different base metals, or even earlier times, when we had money that looked a little different than we currently looked like. Let me hold that about what happens to the US dollar for a moment and just say, the role of money, because we will lose time, and I want to get going as to what cryptocurrency and blockchain technology is.

So the role of money is three things-- a medium of exchange, as Plato and Aristotle talked about; a store of value, that Aristotle basically said that I can hold it today for something tomorrow-- that's a store of value; and it also then becomes a unit of account. The US dollar is a unit of account in the US, the yen in Japan, the euro in Europe, a unit of account. These three roles of money.

And it's looked very different over time. Cowrie shells in Greece. But today, I put here an Alipay mobile wallet. That's sort of what we use dominantly around the world. We talked a little bit about fiat currency when Hassan and I were going back and forth.

A fiat currency is a representation of some central bank liability. Central banks, an invention of the late 17th century both in England and in Sweden, just about the same decade in the late 17th century, was a check on the sovereign. You see the king, the king in England-- using that story for a moment-- the king was at yet another war with France and wanted to borrow money.

And when the king wanted to borrow money, going to the noble lords, the noble lords said, enough already, king, and said, we need some mechanism to control how much you can borrow. And how much you can borrow is, in essence, a representation of money. And they set up the Bank of England.

And in Sweden it was a check also on the sovereign for a little bit different political reasons than a war with France. And there we had the initial sort of central banks. Here in the US we went about it-- Alexander Hamilton thought we should have something. That was during the 1790s. By the 1830s, Andrew Jackson said, enough

with this sort of centralized banking.

And then we went for nearly 80 years-- about 75 years, from the 1830s to the 19-teens-- with no central bank. We had crisis after crisis, and we formed one during President Wilson's time, one of the great progressive movements of the day and just about a hundred years ago.

But fiat currencies are representations of liabilities. And Hassan would say, well, but don't they have something behind it? What they have behind it is the government's ability to, of course, tax, the government's ability to be trusted to keep its promises to keep that currency stable.

But again, just like when that English king was at war with France, sometimes-- sometimes-- they overprint the money. Sometimes it gets out of control and central banks lose control. But it has very big network effects that we talked about. The acceptance for taxes for legal tender, it's accepted through what Mundell would say was an optimum currency area.

Now, we have 180 currencies around the globe. And some work well and some don't work so well, like Venezuela right now. And so in the midst of all of that, the question is, and this a little humorous, is, what's money's future? Is it digital currencies? Or is it like in kind of the fun movie Star Wars, is it these types of things, credit chips and the like?

Now, I would say if you're a Star Trek fan, in Star Trek Gene Roddenberry didn't have any currency. If you go through all the original Star Treks and everything, they actually didn't have any money. That was Gene Roddenberry's future. So he sort of dispensed with all this Plato and Aristotle--

Let's now sort of go a little bit more serious and then talk about Satoshi Nakamoto. But Romain, any questions?

**AUDIENCE:** None so far. Let's give it a few seconds. No, I think we're good to go.

**GARY GENSLER:** So with that foundation, let's go back to the payments riddle. So we get through the 1990s. The internet is taking off, we figure out how to secure it, and the credit card companies find a way to move money. Some startups happen. PayPal and the like

start up in this area, the fintech of the late 1990s. Mobile payments start by the noughts. We already have Alipay and M-Pesa in Africa.

But this payment riddle is still there. And that cypherpunk mailing list is still there. And on Halloween night in 2008, an eight-page paper is written and is put up on the internet on this cypherpunk punk mailing list-- there might only be a couple people. "I've been working on a new electronic cash system." Peer-to-peer, no trusted third party, no central authority.

And what Satoshi Nakamoto wrote in that eight-page paper, what Nakamoto-san wrote was Bitcoin white paper. Had never used the word "blockchain technology." We've come to call it blockchain technology.

So, what is the blockchain technology? fundamentally, it's a shared accounting system-- a shared accounting system or a shared database system. So Satoshi Nakamoto had timestamped ledgers. And a timestamped ledger with cryptography to secure it was not new. A timestamped ledger-- my little illustration here, Neha Narula and I use this, so I want to give her credit as well-- represents blocks of data. Blocks of data, and between these blocks of data a cryptographic hash function.

And a cryptographic hash function we use every day of our lives, just we don't know we're using it, somewhere on the internet to commit to data. This technology, this idea of taking a block of data and adding another block of data and having a hash function in between, was an innovation of the late 1980s. Two Bell Labs scientists, Haber and Stornetta, wrote a paper about it, even started a company to notarize legal documents by 1995, a little startup called Surety.

That existed. That existed, but what Nakamoto-san figured out was how to have multiple parties. Nakamoto-san solved the consensus riddle, or what some people call Byzantine general's problem. The problem is, what if I don't know the other people keeping a ledger? Again, the Byzantine general's problem was not new. It wasn't even about money.

The Byzantine general's problem had been written about in the early 1980s. It was a computer systems problem. If you tie various computers together, what if one of them fails? Or even in an airplane, what if one of the engines fails? It's the question of fault tolerance.

But what Satoshi Nakamoto did was solved it through something called proof of work. And we don't have the time to go through that, but what this provided together was a decentralized, auditable database. Now, in the case of Bitcoin 10,000 computers around the globe maintain this auditable database. And this audible database builds a block of data on top of a block of data on top of a block of data, but its shared accounting system maintains it.

There was one other thing that went on in this period time. In the late 1990s, a computer scientist Nick Szabo wrote a paper and coined the phrase "smart contracts." Again, not an original idea. But what Nick Szabo said, what if we could take a set of promises, put them in digital form, and then the parties can perform against them? In essence, what if we automate in computer code the movement of a property right?

Now, I grew up in Baltimore, Maryland. My dad had a vending machine business. You know, cigarette machines and candy machines and the like. A vending machine is a smart contract. It's a conditional movement of property rights. It's a pack of gum if you put some money in the machine.

So you can think of a smart contract as digitizing, basically, a vending machine. They're not necessarily smart, they're not necessarily legal contracts. So I'd be cautious about that.

But these two concepts came together-- smart contracts, meaning, can I digitize the movement of a property right? And then this accounting system of a shared ledger, that multiple parties can share a ledger with no central controller. That's kind of the conceptual frame where I want to pause for a second, Romain, and take questions on what I usually cover in a lot more time than the few minutes that I just did.

**AUDIENCE:** Any questions from the students?

**GARY GENSLER:** This must be because we just went through holiday time and we had our Zoom Easters and Zoom seders.

**AUDIENCE:** There are no hands raised now. Ah, we do have one question from Celi.

**GARY** Please.

**GENSLER:**

**AUDIENCE:** So I was just wondering, can you explain a little more the issues of the decentralized audible database? You mentioned it very briefly that it first came out and how [INAUDIBLE] were solved. But can you-- just to understand what issues they are solving. Can you kind of explain a little?

**GARY GENSLER:** So if I understand the question, what Nakamoto-san was trying to solve was what has been come to called double spending. Can you in a digital way move a representation of value, in a digital way move that, without having a central authority?

We move digitally representation of values every day. When you go online and buy something-- you go to Expedia, you go to Amazon, you go to Alibaba-- we move digitally representation of values. We no longer have much of our economy on physical cash. But we always have some central authority-- a bank, a payments company that we'll talk about in class 6-- some central authority controlling that to ensure that you actually have that value, to authenticate and authorize the movement of that money.

So what Satoshi Nakamoto was solving for is, what if there was no central authority? And it was a shared database or ledger, or what I call a shared accounting system. That would be the core thing.

This kind of riddle from the 1990s, we send packets of data around the internet with this out-of-central authority, maybe you could do that. And I don't think it's a surprise this happened in the middle of a financial crisis, Halloween in the middle of a financial crisis, when trust in central authorities was quite low, and especially trust in Wall Street and banking, and banks in Europe was quite low. This burst of innovation came at that time.

I hope that helps. And I think as we're going to chat through today and in other classes, the question is, are there other applications? See, this goes to the heart of finance. It goes to the heart of the plumbing. Satoshi Nakamoto's innovation still survives 12 years later. In this adversarial sort of off-the-grid way, Bitcoins still survives 12 years later.

But are there other applications in finance, where a shared database system, a shared accounting system is the best way to go? And we've had inventions like this, infrastructure technologies that have radically changed finance. And one of them from several hundred years ago was the joint stock company.

When I talk about a technology stack, one from several centuries ago was, can we have a shared ownership of a company? And when that was sort of invented, I guess some people would have said, what do we need that for? This, instead of a shared company, is a shared database.

And so that's the debate. Is it really needed? Will it be useful in the future? It has led to a crypto market, about $200 billion as of yesterday, 2/3 of which is Bitcoin, highly volatile.

Hassan would say, but what's the intrinsic value? It is a digital scarce store of value. And it only has value because somebody else will move it.

When Bitcoin was rolled out in 2009, nobody saw that it had value. It was just a kind of interesting project. But by 2010, one person who was in the community said, let's see if I could get anybody to give me something commercially. And it was actually pizza. It wasn't Pizza Net, the Sandra Bullock movie we started with in 1995.

But 15 years later in 2010, a crypto enthusiast in Florida put out-- on an email asked, I will give you 10,000 bitcoin if you send me two pizzas. Two pizzas, 1,000 bitcoin in May of 2010. It took about a week before anybody responded. But two pizzas showed up at his door, and sure enough this crypto enthusiast in Florida sent the 10,000 bitcoin.

Now, at the time, there wasn't a crypto market. At the time, it was thought that the two pizzas were worth about $42 that he had paid 10,000 bitcoin for. That 10,000 bitcoin today would be valued at about $65 million. So 10 years later, you kind of go, well, that was kind of an interesting time to do that.

It's led to different sectors. There's thousands of these coins. The payment or store of value tokens are the dominant, about 3/4 of the market.

Some of you may have heard of Ethereum. But platform tokens were-- Vitalik Buterin rolled out this thing called Ethereum. And Ethereum is conceptually a

worldwide shared computer. It has many attributes of operating system. I wouldn't compare it and contrasted with iOS and Android, but it does have attributes similar to a worldwide platform layer operating system, upon which distributed applications or dApps can be put on top.

So this is this ecosystem. There's a few dozen payment or store value tokens. There's dozens of platform tokens. There's 1,000 to 2,000 applications placed on top. The conceptual framework in these applications is they're decentralized. Will anybody use them-- different questions along the way.

So, what has this led to? It's led to blockchain use cases around speculative investing. Crowdfunding through initial coin offerings-- from 2017 to 2019, nearly $30 billion was raised by basically selling a token before you had a business. You might have a good idea, you might have the legitimate players, and you raised money off of this. You weren't selling equity, you were not selling debt, you were selling a token that could be used on some site in the future.

Now, those tokens have largely been-- in 2020 this is-- those tokens are largely for crypto exchanges, for gaming, for gambling, for something called decentralized finance, and file sharing. Now, there's something that's consistent about the first three-- crypto exchanges, gaming, and gambling. Some of the users of these gaming/gambling exchange sites want a sort of a basis of staying off the grid. They want censorship resistance.

So the thing about cryptocurrencies, the good and the bad sometimes, is the official sector, though they can track some of it, they can't track all of it. That it's some way sometimes to stay off the grid. I'm not advising this. I'm just saying the economics of it, some of that, is about censorship-resistant.

All of the other uses has been around blockchain technology. And the uses really are potential uses. They haven't taken off. Can we use it in payment systems? Can we use it in trade finance? Can we use it in clearing settling and processing? And there are hundreds of projects that have been in proof of concept or pilot stages, none that have truly broken out yet.

And this is why I say it hasn't come into the technology stack. You can, by the way,

get your MIT diploma on blockchain technology. I'm saying that if you do, you can decide also to get it in paper form.

I thought-- Romain, actually we had a poll just to see how many people-- there's a poll on use of cryptocurrency or something, the first of those two polls. If folks don't mind just giving a little flavor for, have you ever owned crypto, and so forth.

So it looks like a third have owned Bitcoin or Ethereum or AUT Coins. And we have-- does Bitcoin exhibit the three roles of money? A little over half yes, and a little less than a half no.

I'm going to ask if somebody-- one person on the yes side, one person on the no side-- just points to articulate why it does not exhibit the three roles of money-- the store of value, medium of exchange, unit of account. And for this Romain, we'll cold call. So if somebody wants to take the lead on either side.

**AUDIENCE:** Any volunteers? Camilo.

**GARY GENSLER:** And if you can declare which side you're on so somebody can volunteer on the other side as well.

**AUDIENCE:** Yeah, I am on the no side. I mean, I--

**GARY GENSLER:** All right. So just for a moment, so if somebody on the optimist positive side please volunteer. But Camilo.

**AUDIENCE:** Yeah, no. I mean, I think that still as a medium of exchange, Bitcoin and the rest of the cryptocurrencies are really limited. If I want to go to, I don't know, the public and buy something with Bitcoin, it would be so hard. I'll have to find an app that translates my Bitcoin to real money and then try to pay.

And there is also a questionable thing about the store of value. You know, Bitcoin at least-- and Ethereum I think is also true-- had been fluctuating so much that you never know how much value are you're getting for a bitcoin day to day. So I think there is still a long way before fulfilling the essentials of money.

**GARY GENSLER:** All right. So I think Camilo is saying, I can't go to Publix, not a medium of exchange where I want to go. And it's kind of this volatile store of value. And you didn't

address a unit of account. But let's see if there's somebody on the other side who just wants to kind of articulate the other side of this.

**AUDIENCE:** We have Devin.

**GARY GENSLER:** Devin, please.

**AUDIENCE:** Oof. I can give the counter, at least in my opinion. I don't think that the idea of a store of value and the medium exchange are shortcomings of the currency. I think they're shortcomings of the market in which it operates. So you can use it to exchange value. If the infrastructure isn't there, that's not the currencies fault, that's sort of the market participants.

And then with the store of value, it does store a value. That value does fluctuate, that's true. But again, I think that's because of the market it's in and speculation going on around these currencies.

**GARY GENSLER:** Camilo do you want to-- you both are unmuted. You can cross-- and Devin can stay unmuted, too. Any reply just for 30 seconds?

**AUDIENCE:** No, no, no. I just want to say that, although it's true that the value of the Bitcoin, it fluctuates with the market, the point is that if you want a worldwide accepted medium of exchange, it cannot fluctuate as much as a Bitcoin. Otherwise, the financial system-- and even people who have savings wouldn't have their savings in Bitcoin.

I mean, you are not going to put your funding, your savings account into Bitcoin, because you might get losses overnight, so.

**GARY GENSLER:** And [Devin.

**AUDIENCE:** I agree that it does fluctuate. I wouldn't put my savings in it. I never have, I never will. But I do think it kind of comes down to what is the exact definition of the question you're trying to answer. Can you store value in it? Yes. Is the value going to be the same tomorrow? Maybe not.

And that's something that might stabilize over time as-- like, if it gets used more for day-to-day interactions like going to the shop, and it's not kind of speculation and sort of hype around it, then maybe we can kind of converge to a point where it does satisfy everything fully.

**GARY GENSLER:** And this debate that Devin and Camilo are helping frame is debate that's a worthy debate. I will tell you that I'm not a Bitcoin maximalist, but I actually-- I'm probably a little closer to Devin than Camilo on this in terms of, it is a digital scarce store of value. Will it be worth something 10 years from now? Maybe not, maybe not.

But it has survived kind of in this swamp, it's this uncertain sort of world, for 12 years. And it has some value to some folks. Hassan earlier would say, but it doesn't have intrinsic value. And I would say, well, it's just a symbol in any regard. It can be a medium of exchange in certain places.

But it needs an infrastructure. Camilo is absolutely right. The state treasurer of Ohio in late 2018 had announced-- a state controller, I think it might have been, in Ohio, an elected office-- that the state of Ohio would accept Bitcoin for taxes. Was it just for political reasons that this gentleman announced it, that he thought he was associating himself with a new innovation in the economy?

But they needed an infrastructure to accept the Bitcoin. They had to convert it for a 1% fee to US dollars for sure. It's not much of a unit of account. But sometimes it becomes a unit of account inside of these other decentralized apps inside the ICO space.

So it sort of probably exhibits one out of the three mostly. It's a speculative store of value. It can be a medium of exchange. It can be a unit of account. But it hasn't adopted this.

A number of years ago, the Financial Stability Board, a worldwide organization of 20-- the G20 finance ministers and central bankers, decided that they would no longer call Bitcoin and others cryptocurrencies, and they'd call them crypto assets. So they were associating more with Camilo's side. They were saying, we're not going to give this the kind of word to call it a currency.

And yet, the US Department of Treasury some seven years ago had to address itself

to the question of whether Bitcoin and other similar digital assets were currency under US Bank Secrecy Act laws, against money laundering and the like. And for that purpose, they said that Bitcoin was a virtual currency. So there's the US Department of Treasury fitting it into a box.

Now, I dare say they needed to somehow address this public policy issue as to whether it was going to be regulated under the Bank Secrecy Act. So somehow they had to call it a currency, call it a virtual currency. Another part of the US Department of Treasury about the same time said it was going to be treated as property for tax purposes.

So inside the US Treasury Department, clearly for purposes of trying to decide how it's going to be taxed, how it's going to be treated for anti-money laundering laws, one part of the Treasury called a virtual currency, another part of the US Treasury called it property rather than currency. And that fit into that.

So I think I'll move on a little bit. But we can take down the poll, I think. Or do I do that? You--

**AUDIENCE:** So every person should be able to close that little polling window. I do not have control over it.

**GARY GENSLER:** OK. Then I need to do that here for a second so that it closes. OK. So there's a lot of challenges of this shared accounting system. Scalability, performance-- you can move about 7 or 10 transactions on Bitcoin per second. You can move 10 to 20 transactions a second on Ethereum. That's kind of not the shot that we need to this system.

Our shared, centralized equity-clearing system here in the US, the Depository Trust, DTCC, needs to move-- the Securities and Exchange Commission sort of said, you need to be able to move about 100 million transactions a day. Well, guess what? In the middle of one of the most volatile time in February, DTCC was moving 350 million transactions.

And when I say transactions, it could be for a hundred shares, it could be a thousand shares or if the volumes in shares was higher. But I'm talking about how many transactions were moving through that system. Blockchain technology by and large

has a bunch of issues still to sort through, is the point, from public policy issues, commercial use cases, and the like.

And the question is for the 2020, as these scalability, performance, and efficiency issues, as privacy and security, as some of these are worked through, is a shared accounting system, a shared ledger system something that's going to take off? And I go back to economic work from the 1930s by Coase. And i just sort of capture it in a little slide here the trade-offs of centralization and decentralization, and these as a cost curve.

But centralization does lead to cost, about a single point of failure, about economic rents, and about capture. We all know that we pay more for something that's highly centralized. If you want to build an app on top of iOS or on top-- Apple's iOS or an app on top of Google's Android, you're going to pay a fee, because they're the two dominant pipes if you need to deal with certain centralized financial systems, there's more economic rents.

And in fact, the financial sector in the US takes about 7 and 1/2% of our economy. That's double what it took in the 1960s. Now, it's a bigger economy, it's a bigger financial sector. But does it necessarily need to take 7 and 1/2% of our economy? So some would say, those are some of the costs of centralization.

And then there's also cost of decentralization-- coordination, governance, security, scalability. Now, Coase was writing in the 1930s why do you bring together certain attributes inside of a firm. It was about the theory of the firm and why some things are inside a firm. And it was the cost of information, the cost of coordination, that you bring some things inside, some things are left out. The question is, will this change this balance somehow?

Vitalik Buterin talked about a trilemma and said it's hard to get all three of these, to get security, decentralization, and scalability. So Buterin is the innovator, at 19, of the Ethereum network. He's now 25, maybe. But Vitalik Buterin said, look, you can get decentralization like in Bitcoin and secure it. It's reasonably secure, but it's not scalable. You maybe can get towards scalability, but you're probably going to tend towards more centralization.

Now, one of MIT's award-winning computer scientists, Silvio Micali, says, no, he

disagrees. He says you can actually solve for this. Silvio won the Turing Award. He's sort of the father-- considered the father of something called zero-knowledge proofs, and said, no, you can solve for this.

And Silvio actually took a sabbatical leave to create a cryptocurrency and a company around Algorand. And I'm not sort of marketing for him, but I'm just commenting, there's this debate. Can you solve, basically, what Satoshi Nakamoto wanted-- decentralization in a scalable way and have it be secure?

So how does one assess use cases? Because this class is ultimately about sort of sorting through this. Well, first he asked the question, is the project a project that actually uses cryptocurrency, or it services it? And I give examples of companies that are in custody, in software, in exchange operation, finances, the crypto exchange. Coinbase is both an exchange and custody. Fidelity, one of the world's largest asset managers, said, we'll take custody and hold your cryptocurrencies. So you could be on one side of the divide and say, we're going to be even like a hardware company BitMain and create the hardware in this space.

Those are kind of used classic strategy analysis to think about those. The sort of rougher side of this is, how do you consider what are the strategic questions about actually using blockchain technology? What are the value creation propositions? And I think it's embedded in this-- is it worthwhile to have decentralized computing versus centralized computing? Is there an area that you think has such high economic rents that a decentralized competitor can come in?

You could create the case that if Uber and Lyft didn't exist today, that Uber and Lyft, you could say, could be created on a decentralized ledger system. But nobody truly had control of the ledger system, and all the ride sharing could be with drivers and users using that decentralized app. But then again, who would have actually gone into city after city, airport after airport, and should have done what Uber and Lyft and others have done to get into the system?

So I think the basic value question is centralization versus decentralization, and secondly, are you filling a gap in the fiat currency system? Fiat currencies work pretty well. Now, we're going to talk in the next class about the pain points. And there are a lot of pain points in the payment system that take considerable

challenges and costs to overcome.

Clearly, strategically what are the competitors doing-- traditional competitors, those using blockchain. Why use append-only logs, this invention of this ledger system? Why have multiple-party consensus? Multiple-party consensus is a cost.

So if you're going to use it for trade finance, you're going to try to solve something and trade finance for instance, what is it solving, what are the costs? It can lower verification and networking cost. That's the core of its economics. But it comes with some cost.

There are also a series of tactical considerations-- literally, what data is going to be put in? Who is the multiple stakeholders? What are the trade-offs? And I think what we've found by and large is there are not that many projects that have taken off.

I have here a little bit deeper dive. If you get so close to a project that you think, all right, now let's think about it-- I come back to this question about multiple-party shared ledgers. In Bitcoin, the multiple-party shared ledger has worked in part because there was a desire to have a censorship-resistant token-- a token that could be global, truly move around the globe, at times away from what the official sector might ban, away from certain money laundering anti-terrorism laws, that's part of it-- but also that it was, at least initially, hard to track and trace. It's actually gotten easier to track and trace over time.

But really the question is, if you're going to think about using blockchain technology, what verification cost are you really lowering, and why have this multiple-party distributed ledger? A little bit like a shared stock company still has a lot of centralization. You have thousands of people that control a shared stock company, this invention of several centuries ago, but you still have the management team that controls it. How do you deal with that here?

So, what have we found? We found that the incumbents, big finance, by and large, have stayed over to the left-hand side of this screen. They've stayed towards traditional databases. They haven't gone to the cryptocurrency sort of side of this screen-- permissionless open protocols.

They're exploring a little bit the middle, what's called private blockchain, "private

blockchain" saying, 20 or 50 companies get together. Maybe-- like in Australia, there was much fanfare in 2016 into, actually, 2017, there was much fanfare that the Australian Stock Exchange would use a permissioned blockchain technology to update their central clearing. Now, many people would tell you by 2020 that what the Australians have done was inspired by blockchain technology, but it no longer looks like blockchain technology.

It's a decentralized, distributed database. But what the Australian regulator said is, we need somebody to control this. We need a central controller-- the complete opposite of what Satoshi Nakamoto was talking about. Nakamoto was saying no central authority.

But the Australians said, well this is the central clearing, sort of the plumbing, the central plumbing, of the Australian stock market. No, we need somebody who has kind of the overall-- plays the overall referee role, so to speak.

So incumbents by and large are using traditional databases. They're exploring some of these permissioned databases. They're not really off to the side. Romain, any questions?

**AUDIENCE:** None so far. We have 12 minutes left.

**GARY GENSLER:** All right. So let me just say something about central bank initiatives. Central banks-- and we'll chat about this a little bit more when we do payments-- central banks have taken note of this. And they've thought both, can I use the blockchain technology for our payment systems-- because central banks in most countries control those payment systems-- or can we actually create a digital currency?

At first, I mean, Bitcoin was not really on the radar of central bankers. By 2018, it became on the radar because the market had taken off and it was, for a brief moment, worth almost $1 trillion. It's back down to $200 billion, now but they took note. And in some countries like Sweden, they really said, maybe we should be doing something here. We should be creating a crypto equivalent, a digital currency.

And one of the readings was a Bank of International Settlement reading, which showed three different ways that a central bank could do a digital currency. And this is just for your reference to remind you that it was in the reading. But going back to

these projects a little bit, some of the projects are just papers.

Ecuador tried to do a project, actually-- a dollar-denominated cryptocurrency. And it failed because nobody in Ecuador wanted to use it. Ecuador was already dollarized.

But the one to watch most closely, China, which might be a hybrid-- and I'll go back to the chart in a second-- China has announced they're doing a digital currency electronic payment. It will be fully backed by the central bank. It will be fully a renminbi or digital block.

And in a sense, it may be as much a reaction to Bitcoin as it's a reaction to Alipay and WeChat Pay being dominant in the retail payment system in China. And it's also a reaction to Facebook that was starting something called the Libra project.

So this, again, is a central tenet where I am, where I think of this as that the central banks are reacting in part because big tech has been reacting and startups are there. And they're saying, maybe we can do something better. The opportunities that they see, the opportunities is that they say, well, maybe we can stay in the means of payment. We can promote greater competition, and we can address some pain points.

But on the other side, they're really worried. They're deeply worried that if they offer the public a digital representation of central bank money, that they might disintermediate the commercial banks. The central strategic question for central banks is, can we offer the public a digital representation of that which is paper?

So I've covered central bank digital currencies too quickly. I'm going to come back to it when we talk about payment systems as well. But Romain, we only have a few minutes so I'm going to take questions.

**AUDIENCE:** Yeah, we have a question from Victor.

**AUDIENCE:** Hi, professor. I want to come back to this point about handling databases through a private blockchain network, because I didn't fully understand how it would work. Could you give me some more guidance on it?

**GARY GENSLER:** So Satoshi Nakamoto's concept is that you could have hundreds or thousands of folks' computers sharing a database, and it's an open database, and that that

database can secure the ledger through this concept of a log structure-- block of data, block of data, block of data with cryptography. The commercial banks and the financial firms said, we're not comfortable of having hundreds or thousands of people share a database.

In fact, we can't. Under various guidelines of privacy, of data protection, we can't have hundreds of people share that database. But they're looking at, maybe we can have a shared form of cooperation, or what somebody might call coopetition. We'll cooperate around the trade finance platform, and then we'll compete on top of it for the provision of lines of credit, and trade financing, and so on.

So they've come together and said, maybe we can have a shared closed system amongst 20 banks, 16 banks, 30 banks, and the like. And so there's five or six big consortiums trying to put together a trade finance private shared ledger. Now, once you have that, once you say, it's only these 18 firms will share it-- this form of cooperating on a shared database but competing on top of it, that form of coopetition-- you don't necessarily need a token. So there's no cryptocurrency, it's just a shared blockchain technology database. Some call it a Digital Ledger Technology, DTP, to contrast it with cryptocurrencies. I'm a little bit looser in the vocabulary, admittedly.

But that's how-- that's the conceptual framework for it, if that helps.

**AUDIENCE:** Yeah, thank you.

**GARY GENSLER:** Let me just say a couple of ground truths in close. I really do think-- and I don't know which side to end up on, Devin or Camilo's side, in terms of, is it money? But I think Nakamoto solved the payment riddle-- avoiding double spending. It's lasted 12 years.

Whether you like it, whether you love it, hate it, two is-- I'm sorry, Hassan-- I'm kind of-- money is but a social and economic construct. I'm deeply with Plato on that one. But I respect those that believe otherwise. I mean, there's a good debate that's gone on a couple of thousand years.

We already live in an age of digital money. And in fact, the corona crisis will accelerate that. We will still have physical paper money, but we'll use it less and less

in transaction. And physical paper money is more and more just a store of value. We're not using physical paper money much as a medium of exchange right now.

Append-only logs and multi-party consensus actually does provide an alternative, but it doesn't mean it's everybody's alternative. It can address verification costs, but it doesn't make sense to adopt it unless there's really some viability and a value proposition of that shared ledger system. We didn't talk much about it, but I will say one ground truth is that the crypto markets-- that $200 billion market-- it's ripe with scams and frauds. It just is.

And so what's happened by 2020 is cryptocurrencies have evolved to be a speculative asset class, generally not that correlated with equities and bonds. And I'll give you one statistic. The worldwide stock of gold, that gold that could be in four Olympic-sized pools, collectively is worth $9 or $10 trillion, roughly, collectively.

So some people would say a speculative store of value that's only worth 2% of that, $200 billion, might be worthwhile in a big portfolio of a family office or a hedge fund. The ICO boom and bust raised about $30 billion. Not much is being raised there now, but it's worthwhile to take note of. Most of this is lightly regulated, and so retail investors are not getting much protection. I think that's unfortunate.

But I still come back to the last point. I think it's been a catalyst for change. I think it might be one of these technologies we look back in decades and say, it was a remarkable catalyst for change for central bankers, and to think through whether it's trade finance or other areas in finance, was their way to form some cooperation and compete on top of it-- so coopetition?

But just like we didn't know that the internet and geolocation devices would lead to disruption in rides-- you know, Uber and Lyft, we couldn't predict in the 1990s that the taxicab business in New York was going to be completely disrupted. We don't know what blockchain technology and cryptocurrencies will disrupt later in the 2020s or in the 2030s.

So that's kind of my wrap on it. You can sort of get a sense of why I'm not going to say I'm a maximalist in this area. But I'm also not all the way a minimalist. The minimalist would say, no, none of these ground truths matter. I think it's a really important technology, if nothing else, because it's been a remarkable catalyst for

change on how central banks and others think about payment systems, which we'll take up in our next