GARY GENSLER: Thank you for everybody coming back. And I should tell you, when I start the session with that little shh, I learned from a congressman in Baltimore. As some of you know, I've spent a lot of time around politics. And one of my roles in politics was that I was the treasurer of the Maryland Democratic Party. Which, if you anybody ever asks you to be the treasurer of a state party, come. I can give you some advice about what that's all about when your home state senator asks you to do it.

So I had to quiet down the annual Jefferson Jackson Day dinners. I'd organize these big dinners, and there's 400, 500, 600 people at these dinners. I couldn't do it. I couldn't get their attention. And Congressman Elijah Cummings comes up, and he just leans into the mic. Shh. And it quieted the whole place down.

I said, Congressman, what is this? Is this something you've learned in politics, something you learned from your minister, your priest? He said, it works every time, works every time. So Elijah Cummings gave me that little duty.

Blockchain and money, we're here. I know it's a little bit like eating broccoli these last couple of classes, because we went through cryptography, and then we moved a little bit into consensus protocols. And today, we're going to pick that up and try to finish up the design bits of Bitcoin.

I wanted to introduce, though, one walk-in. We're going to have walk-ins from time to time in this class. But Patrick Murck, he's hiding over here with the cap in the hoodie. He's got the look for a lawyer who's been spending his time around Bitcoin for seven years. Now, he's currently affiliated with Berkman Klein at Harvard. And I didn't know Patrick was going to be here, so I'm calling him out. He's also special counsel of the Cooley law firm. And he has a bunch of clients who try to do the right thing by the law. But sometimes they find themselves dealing with the Securities and Exchange Commission or other fine government institutions. But Patrick was also general counsel to the Bitcoin Foundation. And for a short while, you ran it, didn't you, before it kind of went puff?

PATRICK MURCK: Yes. [INAUDIBLE]

GARY GENSLER: Yeah. But Patrick's the type of lawyer that wears a hoodie and a baseball cap. He's a Bitcoin lawyer. If you ever need Patrick for one of your entrepreneurial efforts, I'm sure Cooley law firm will like advising you, too.

AUDIENCE: Do you take bitcoin?

GARY GENSLER: What's that?

AUDIENCE: Does he take bitcoin?

PATRICK MURCK: I have. [INAUDIBLE] In fact, I've never bought a bitcoin, ever. [INAUDIBLE] paid 100% in bitcoin, so it's all good.

[LAUGHTER]

GARY GENSLER: So Patrick, when you get paid 100% in bitcoin from a client, how long do you hold it?

PATRICK MURCK: Well, it depends, right?

AUDIENCE: [INAUDIBLE]

PATRICK MURCK: Often, in the early days-- not very long, because I had to pay for my mortgage and my kid's daycare and things like that, and they don't take bitcoin. So I've sold a lot of bitcoin over the years. Something sadly, but I never bought them. I just earned them.

GARY GENSLER: Earned them-- so you're like a miner, except for you're a lawyer who gets bitcoin.

[LAUGHTER]

PATRICK MURCK: I mine with my mind.

[LAUGHTER]

GARY GENSLER: The study questions for today was, we were going to turn to that last piece about transactions and something called the unspent transaction output, and script code that is a computer code that's used inside of Bitcoin. We're going to talk a little bit about the design features bringing it all together, and particularly around the reading, which was the academic pedigree of Bitcoin. Which is also a reading that Patrick assigns when he does his study group at Harvard Law, as

well.

And then, yes, all of you are going to be able to participate. And we're going to take a survey amongst all of you as to who's Satoshi Nakamoto. Ah, yeah, yeah, yeah. Or would you rather do more on transactions script?

[LAUGHTER]

All right, we'll do a little bit of both. The readings, of course, the *Bitcoin Academic Pedigree,* which we're going to talk about in the latter part. And I'll do a little cold-calling and get some feedback as to what you thought from the reading or if you're still skimming it. And then there was a CoinDesk article, just making sense of it all.

And so as I said, we'll go through the transactions. We'll do a little bit of putting it all together and the *Academic Pedigree.* We'll have a little fun. You all are going to have a chance to tell us who Satoshi Nakamoto is, or was, or the committee.

So transactions-- you've seen this graph before. But transactions, the format in a transaction ledger-- not only in Bitcoin, but really everything-- is somebody on one side of a transaction and somebody on another side of a transaction. So in Bitcoin, there's an input. And the input inside of Bitcoin is an ID of a previous output.

So not only is Bitcoin a series of blocks of information-- each block that has 1,000 to 2,000 individual transactions-- but in a sense, there's a separate chain that's going on. I sometimes think of a blockchain as, yes, there's the chain of big chunks of data, but there's also a chain of individual transactions. Shimon, is that a hand raised or just scratching your head?

AUDIENCE: I'll be more careful.

GARY GENSLER: No, that's all right. Shimon is a faculty member of the Finance department here at Sloan. And some of you might take his Finance 1 course, I assume. Somebody in here is, probably.

So the input is just really the idea of wherever the output was. You can think of a chain of a transaction. Can anybody tell me where all transactions come from? Where's sort of the genesis of the value, if you follow a transaction chain back to its origin? Hugo.

AUDIENCE: Coinbase.

GARY GENSLER: Coinbase-- so anybody want to say what a Coinbase is?

AUDIENCE: It's a generation of a freshly minted bitcoin.

GARY GENSLER: Right, so the generation of a freshly minted bitcoin-- not the way that Patrick Murck got it when he's selling his services for the law, but how a miner gets it, they get their transactions. Remember initially, 50 coins was what happened initially back in 2009. Now it's 12 and 1/2 coins. And in a short couple-- maybe it's about 18 or 20 months, it goes to 6 and 1/4 coins. And it keeps splitting half and half and half, eventually to no Coinbase. But every transaction, in essence, had to go back all the way to Coinbase-- some Coinbase, some 50 or 25 or 12 and 1/2 coins being issued.

And then the output-- so a transaction format is pretty straightforward, in a sense. The input is a previous output and a digital signature, and then, to whom do you want to send it. And it's sent to Bitcoin addresses. That's why we spent just a moment-- we just glossed over what a Bitcoin address is. It's sort of a translation to a public key, but it's not identical to a public key. And of course, you need value. Value measured in bitcoins or satoshis, or if we're on the Ethereum network, it would be an ether and gas, et cetera, et cetera. On 1,600 different platforms, it could be a different native currency.

Lock time, I don't think lock time was in any of the readings. But anybody want to tell me what a lock time is? It's relevant to some of how the technology goes. Anybody want to take a guess? Where's Alin? Not Alin the PhD, but Alin from the digital currency initiative. No? You're hiding. You don't want to say what a lock time is?

AUDIENCE: I thought it's some sort of protection mechanism for, I guess, double spending.

GARY GENSLER: It is a protection mechanism, but not so much about double spending. Tom, did I see your hand up?

AUDIENCE: This is a guess. Is it when the transaction is hashed?

GARY GENSLER: It's when. It's about time. It's when the transaction can happen. So right now, it's 2:45 on September 20. If you put a lock time in at 2:50 or 2:55, it couldn't happen until 2:55. So you can actually conditional the transaction. That's all lock time is. But you can say, it can't happen until. You could put tomorrow's date.

AUDIENCE: The counterparty sets that, so it's like the date on a check?

GARY GENSLER: It's a little different than a date on a check. Because one of the things that gets validated in Bitcoin is, is that it will not validate a transaction early. And if you put October 6 on a handwritten check, the bank might still take it, even though they probably shouldn't. So it is like the date on a check, except it's verified and validated and so forth. I'm going to take Emily and then Shimon.

AUDIENCE: So if you were to set the lock time in the future, could that mess up the blocks in the chain? What is kind of the right chain of events that you're recognizing if you're choosing to set a lock time in the future? I guess the broader question would be, why would you set a lock time in the future?

GARY GENSLER: Shimon, were you answering that?

AUDIENCE: No, no, no. I want to ask you, in the [INAUDIBLE] question section, is what purpose does it serve, right?

AUDIENCE: It's not a really Turing complete language, so you're not really trying to create conditions here. But this is sort of a condition.

GARY GENSLER: So it's a condition. Because at any point in time, you might want a condition of payment. You might want a condition of payment on time. And we're, in a few slides, going to talk about the scripting language, the computer language that allows transactions to happen. Shimon said, was not Turing complete.

From the readings, anybody want to tell us what Turing complete is in computer science language? No? Anybody know who Turing is? Anybody see *Imitation Games.* Anyone know what the Turing Award is? It's sort of the Nobel Laureate for computer scientists.

AUDIENCE: Isn't that the award when the machine can actually can pass as a human being?

GARY GENSLER: Well, that's one thing associated with Turing. But the Turing Award is an annual award, sort of like a Nobel Laureate, but for computer scientists. Turing complete allows you to do loops inside of computer programs. And the script language does not allow that to happen. Every function needs to sort of have some language. I know Alin looking at me to see I don't dive.

But to answer Emily's question, it's just, there's so many different ways to condition a transaction. And Satoshi Nakamoto thought, well, let's put it in here, right in the transaction format, that you can condition on time. And then two parties could do that. To your question

about whether it could inadvertently lead to double spending, it's a very good question. Can I hold it until we just do validation for a second?

So this is a unique identifier for the input. But it's really uniquely identifying from a past output. What's the block number? Is it from the 250,000th block or the 300,000th block? So it takes literally a block ID. And then within that block, which one of its 1,500 transactions might it be? So you can find any transaction on an entire blockchain by knowing the block, and then within the block, which transaction. It's just a data mechanism on how to store data. And through this mechanism, there's a chain of transactions, as well as a chain of blocks.

And then the value we talked about that-- I think there's, if I did my numbers right, 10 to the 8th satoshis in every bitcoin. It's a little hard because I think there's 10 to the ninth gas in every ether. And that's a coin. That is what is a coin. When Satoshi Nakamoto did this, it wasn't really a coin, because it was a question whether anybody would give value. And until about 18 months later, when those two pizzas went for 10,000 bitcoin, what was it? Or until somebody started the first exchange, a crypto exchange, to exchange that.

So you can also have multiple inputs and multiple outputs. And I'm going to use an example that I just created of, I want to send some bitcoins to two different people. And I need some bitcoins. So I might grab three former inputs. And these are just Transaction ID 6, Index 3. Of course, it wouldn't be ID 6. It might be ID 300,000. But the point being is, grab 10 bitcoin, so I want to find three inputs. And I needed to send six bitcoins, let's say, to Amanda. You like that. And just because you're sitting up front, James, I'm just going to send three.

But I'm not using Amanda's name and James' name. I'm using your Bitcoin address-- Amanda's Bitcoin address, and James' Bitcoin address. So rather than being account-based, like if you have an account at Bank of America, and you say, I want to send $10, I just check to make sure I have more than $10. In Bitcoin, I actually have to fine individual transaction outputs that add up to-- in this case, I want to send nine bitcoin, six to Amanda, three to James. Not really, Amanda.

So what's 10 minus 9?

AUDIENCE: 1.

GARY GENSLER: Thank you. That was really hard. We are at MIT. But I might not send one back to me. I'm going to send 0.9 back to me. This is kind of my change. So a Bitcoin transaction can either be

equal, the inputs equal the outputs. I could have sent one back to me. But I've decided to incentivize miners and leave a little extra, 0.1 bitcoin, which would be a lot of fee, actually. That would be about, what, $640 or so?

I probably wouldn't do that. I would probably leave for a fee 10 or 20 or 100 satoshi maybe. I don't know what the current market is. But this is a transaction. Multiple inputs, multiple outputs, but you always have to send back to yourself. What happens to these inputs if this transaction actually happens? They go away.

The actual inputs disappear once they go through this. And so inputs always have to equal outputs. When a transaction is validated, one of the validation methods is to make sure that the lock time has actually happened, that you've passed the lock time. Another validation point is that inputs are greater than or equal to outputs. If outputs are greater than inputs, the transaction will not be validated.

The digital signatures have to be validated, going just back to the prior slide. That digital signature has to be validated, as well. And that, this previous ID and index actually exists. And this is getting to your question Emily. It still exists. But these inputs, once you've used them, they no longer exist in the database. They're kind of in the past.

So that's the transactions. That's the core. I know it's like eating broccoli, but it's an important part of all of blockchain technology. The Coinbase transaction we've already talked about, so I'll slide over this quickly. But it's a reward for solving the puzzle. In the case of Bitcoin, it's solving the proof of work. Tom.

AUDIENCE: Sorry, can we go back to the miner incentive. It's the 0.1 or 1 satoshis. And how is that different than the cost of trust when you use a financial institution as the [INAUDIBLE]?

GARY GENSLER: So Tom's question is, the miners' economics. Of course, they get their 12 and 1/2 bitcoin, and they might get some transaction fees. Tom's question's the other side. Why is that any different than paying some central intermediary? Anybody want to try doing this? I could cold-call, but does anybody want to-- this is an economics question about markets.

AUDIENCE: I would say that the person that is sending the transaction has the ability to choose how much it will pay for that transaction. And in the bank, it's regulated, and you pay. Maybe that's one of the differences.

GARY GENSLER: All right, so one difference is that the bank is setting, generally, a fixed fee schedule, and this

is a decentralized market mechanism for setting fees. Sean.

AUDIENCE: The fee for intermediaries a lot higher compared to Bitcoin, the transaction fees.

GARY GENSLER: So Sean's second point is that, currently-- this might not be true in the future. But currently, central intermediaries are able to charge higher fees than in this decentralized system. Alin?

AUDIENCE: I think that, conceptually, it's not different from a centralized intermediary. It's just, the functions are the same. The amounts, maybe the amount that I pay, the amount of the fees are different, but the concepts are the same.

GARY GENSLER: All right, so Alin is basically saying, well, maybe it's not so different. I mean, though it might be floating rather than fixed, it might be currently lower rather than higher, but you're saying, fundamentally, it's about the same. One minute, Shimon, let me just-- because you're faculty. You're going to actually tell us the answer.

AUDIENCE: Question-- is this mandatory?

GARY GENSLER: Very good question-- it's not mandatory.

AUDIENCE: So that could create a big misalignment of interest.

GARY GENSLER: So it's not mandatory. Fees are market-based. And at times, like last December, they were really high. And now they're quite low, partly because the Bitcoin network is not humming at full capacity. It can readily fit 1,000 to 2,000 transactions a block. And it's not like there's a jamming to get 10,000 and 20,000 transactions into a block, as there was last December. I'm sorry, Shimon.

AUDIENCE: I think it's very different, in the sense that you're basically inflating the fee in most [INAUDIBLE] inflation. So even if when you don't transact, you're paying implicitly for other people's transactions, and that's going to change over time. So that's actually kind of a clever mechanism of how, structurally, these are going to shift over time in the network, as it hopefully matures.

GARY GENSLER: Why don't we take one more here-- Alexis.

AUDIENCE: That's like when you have [INAUDIBLE] they're going to keep the money. And they could use it for making [INAUDIBLE] or whatever. So they make money on a spread. Whereas here, for the case of Bitcoin, the money's going to stay in the system, and it's going to flow to another

miner, who is going to use it for another transaction. It will stay within the same network, I would say, rather than just going to another destination.

GARY GENSLER: I hear you. But it might actually leave the network to lawyers, like Patrick. Or it might leave the network if you use it at Starbucks, if Starbucks would accept it. So I'm challenging your thought, but you can challenge mine back. Why don't we close out with Eric, and then just move on.

AUDIENCE: The difference might be in the perspective. From the person that's originated a transaction, it's basically the same thing. But if you think about it as a system, there's no single entity gathering all the money from transactions. You have a network, a [INAUDIBLE] network, of [INAUDIBLE] that are getting that. And besides, once we get out past the 21 million bitcoin generation cap, then all the systems must be using [INAUDIBLE] in some way. And transaction fees would be [INAUDIBLE].

GARY GENSLER: So Eric raises two points that I'll-- there are other points, but two that I want to repeat. One is, this is more decentralized possibly today than the current commercial banking system, for instance, for transaction processing, or the transaction processing that Visa and First Data do, which we'll study when we get to payments. So it's possibly more decentralized. I think you said it was more decentralized, but I'm putting the word possibly in there.

And two is that, at least in bitcoin's case, there's two revenue sources for providing the services. The miners do it for the Coinbase transactions, 12 and 1/2 bitcoin per block, approximately $80,000 US per block currently. But also, there's this little incentive of fees, which, over time, will have to grow as you go down. If it's only going to be one bitcoin per transaction, and then ultimately almost 0 bitcoin for transaction, there will have to be more satoshis in the fee side.

And some alternative coins-- not Bitcoin-- are more modeled on fees, and some coins are more modeled on mining rewards. The economics-- Satoshi Nakamoto, whomever he or she was, or were, if it's a group, had to think through a bunch of economics. They've survived for 10 years. It doesn't mean that's the best set of microeconomics for a blockchain system. Tom, you look really skeptical.

AUDIENCE: I'm skeptical. But maybe this would be the moment where I take my 12-hour dive.

GARY GENSLER: That's right. So you're about ready for your rabbit dive? Maybe.

AUDIENCE: Maybe.

GARY GENSLER: So the Coinbase transaction we've talked a lot about. The reward, at least in Bitcoin, halves every 210,000 blocks. A very important thing that Nakamoto put in is, you couldn't use your Coinbase reward for 100 blocks. So it was sort of stale or frozen for 100 blocks.

I can think of two reasons, but maybe you all would think of another reason. Anybody want to give it a shot as to why you might do it? Xiaojian

AUDIENCE: Maybe you mine the block, and you're trying to mine a block that shouldn't be-- or it's not legal. You spend the money right away so you can get--

GARY GENSLER: This is the principal reason that's talked about, not only in the literature, but in the early blog post, was, well, how many blocks does the chain have to go before everybody really thinks it's consensus? You could have said 5, 10, 20. Satoshi picked 100 blocks, saying, that, hopefully, is pretty settled, or about 1,000 minutes. James.

AUDIENCE: If you mine, and then you can spend, couldn't you just perpetually create blocks and then pay yourself and create more and earn more and then keep building up [INAUDIBLE]?

GARY GENSLER: So James is asking, could you just kind of game the system and keep mining and spending and mining and spending?

AUDIENCE: Then your rewards go down.

GARY GENSLER: Sorry, Aviva?

AUDIENCE: Then your awards go down over time.

GARY GENSLER: Well, that takes 200,000 blocks.

AUDIENCE: But if there are many of you doing that at the same time, then you accelerate the--

GARY GENSLER: So in some ways, that's what miners are doing. But they have to wait 100 blocks. And so that was what Satoshi was trying to get at. If you have to wait 100 blocks, it's probably now the consensus chain. It's probably been so validated, unless we got into the problem-- Patrick, you weren't here. But some of the students raised the question, well, what if one country as large as China walled off their whole network, and just China went one way and the rest of the world went another? The theory of the case is that, within 100 blocks or 1,000 minutes, somehow

that would be discovered. But if it weren't, you might have a little bit of what James is raising as a question. But that's at least the theory of the case.

It's always recorded as the first transaction in the Merkle Tree. Highly technical point, but it has to roll up into that darn thing we were talking about, the data compression at the Merkle Tree. And here's a little fun fact. You can add 100 bytes of arbitrary data in a Coinbase. You might say, why does he raise this? Well, because it's just a fun little place that some people express their creative wit, artistic stuff, send secret messages to each other, that, buried in the Coinbase transactions, there is a whole forensics of fun little things that sometimes miners put in to the Coinbase, for those of you who are artistic.

The very first genesis block had this sentence. "The Times, January 3, 2009, Chancellor on brink of second bailout for banks." That was a headline out of the *Financial Times* that says Satoshi Nakamoto put in the first block of Coinbase. It's just a little fun place. There's a playfulness that goes on amongst miners, sometimes talking to each other. Did you ever get a message? Did anybody send you--

PATRICK MURCK: Not that I'm aware of. I know what you're talking about. There's one miner that likes to put Catholic catechisms in.

GARY GENSLER: That has put in the whole catechism?

PATRICK MURCK: In every block, there's a little catechism that he puts in. It's a Allegis mining pool. It's a small one. So there you go.

GARY GENSLER: There you go. And do they pay you in bitcoin, too?

PATRICK MURCK: No, they're not a client.

GARY GENSLER: OK. So it all rolls into a database called the unspent transaction output. These are the unspent transactions. If it's been spent, it's kind of burned. And bitcoin transactions that haven't been spent fall into this. And you can use it. It's created because it speeds up the whole system. Instead of going back and looking for all these things, there's actually a database that has all the unspent transactions.

I include in here what I find as a sort of interesting revelation or irony. When Satoshi built Bitcoin, and for the 16 versions that have come since over the 10 years, all the developers, the Bitcoin core developers, have kept the unspent transaction output, not on a blockchain

specifically, but in a database called a LevelDB database.

So those of you who are closer to computer science than I could say all the pros and cons of a LevelDB database. But I'm just observing that, even within the most used first central database for blockchain called Bitcoin, they chose to use not a blockchain, but, in essence, a more standard database to keep the unspent transaction output. Now, in a sense, it's all part of this blockchain solution. I'm just saying, it's one database within the blockchain world that's actually not a blockchain. It's just sort of an interesting irony. But it also sort of says, economically and technologically, Satoshi was trying to create a money system. He wasn't trying to use blockchain for every bit of data.

So this is the actual size of the unspent transaction output. If you can't see, there's-- I think it's about 50 to 60 million. It was higher. There was about 60 million unspent. It's not 60 million bitcoins, because there's about 17 million bitcoin. So you could average it out. You could say, well, each transaction has less than 1 bitcoin.

Well actually, there's been surveys and studies showing that about half of these 54 million transactions are so small that they go by the term of-- they're called dust. That there's so few satoshi that it's not even worth the fees to try to redeem them. They only add up to less than a half a percent of all the outstanding bitcoin, but they're just dust. So maybe out of these 54 million unspent transaction outputs, half of them will never be used, because it's not economically worthwhile. It's like the pennies in the top dresser drawer that you all might not spend. There's this similar thing here. Hugo.

AUDIENCE: Yeah, I guess I have a question about that. It might not be feasible now, but maybe with layers on top of bitcoin that people can do these micro-transactions. Because like, our pennies might be worth a lot of money, [INAUDIBLE].

GARY GENSLER: So Hugo is raising that, just like the pennies in your top dresser drawer might be worth something one day, what I'm referencing as Bitcoin dust, about half of these unspent transaction outputs, a satoshi here, 10 satoshi there, might one day be worth something. Good point. It's just like the pennies in your top dresser drawer though. Have you lost them in the meantime? They might be worth something. But in the meantime, have you lost the private key to those little satoshis?

I put on here three moments of time just to give you the sense of the actual number of

transactions that have happened. There's been 342 million transactions on the Bitcoin network to date, or as of a day or two ago when I put the slides together. So of the 340 million transactions, only about 54 million are still outstanding. The other 290 million have been spent, if you wish. Yes.

AUDIENCE: So then where are these outstanding transactions stored? Are they still being included in the blocks themselves, where you add them to the [INAUDIBLE]?

GARY GENSLER: Which outstanding transactions, the 54 million that are still available? The 54 million all reside in a database within the Bitcoin software called the unspent transaction output, UTXO. And UTXO-- these aren't letters I'm making up-- that's a database, 54 million transactions. Separately, they are actually in the blockchain itself. So all 340 million transactions that have ever happened are in the blockchain. But to make it easier for the software, the 54 million that have never been spent reside in a software. Does that answer the question? Work with me.

AUDIENCE: So it's a distributed database amongst all the different nodes.

GARY GENSLER: Correct. All 10,000 of the nodes can have the full UTXO set. Some wallet providers have the full UTXO set, but they don't have to. Somewhat lightweight nodes usually don't, but can. But a lightweight node would never want to have all 340 million and the full blockchain. So in essence, they're in multiple places, because they're in the full blockchain, 10,000 nodes. And they're also in the UTXO, not only on the 10,000 nodes, but occasionally elsewhere. Alin.

AUDIENCE: So I heard you say the word spent transaction, which is a bit misleading. Because a transaction can be spent and not spent. Because, for example, you would have two outputs. One output is spent by a future transaction, and the other output is not spent. So it's a bit misleading to say spent transaction, because that only happens when the transaction has only one output and that output is spent.

GARY GENSLER: Well, I'm using it lightly. I'm saying that, of the 340 million transactions that have happened, 290--

AUDIENCE: Have an output that is spent, or what are you saying exactly? Because transactions have multiple outputs. They might have n, and maybe k of them are spent. So the other outputs are unspent.

GARY GENSLER: I'm saying there's 340 million-- if I did my data search correctly-- and I'm fallible, so I might not have. But if I did my data source correctly, there was 340 million previous outputs. 290 million

of them are gone.

AUDIENCE: OK, so then you should say transaction outputs, because those are different than transactions.

GARY GENSLER: Yes. Except for it was easier to put TXS. But yes, Alin's clarification is, I believe, accurate.

AUDIENCE: [INAUDIBLE] so people can understand that there is a difference between a transaction and a transaction output.

GARY GENSLER: In essence, what Alin's saying is, there's currently 54 million transaction outputs in the UTXO, which also says outputs. There had been, in the past, another 290 million outputs that have already been spent. Are we together?

So there's a scripting language. There's a little bit of computer code. I said there was no prerequisite to take any computer science before you were here. And my own computer programming is so old, because when I was programming, it was in Fortran and APL. And you can look that up. It's kind of like around with cuneiform and you know the Rosetta Stone.

But Satoshi Nakamoto decided to put a little bit of computer programming inside. And I'm not going to get the count right, but there's several hundred, but not several thousand, little operations and codes that you can use in the Bitcoin script. It's not Turing complete, which means you can't do a lot of the things that you can do in all the rest of computer science. But it's more secure.

In essence, it has fewer attack vectors. It's harder to bring down a little bit. It's a programming code, as I said. For those interested, it's called stack-based, where you sort of move the code over one at a time as it's being performed. And it gives some flexibility.

And back to Emily's question about why there was lock time, or Shimon's, scripting code allows for some conditionality, that it appears that Nakamoto was trying to give some ability to condition a transaction on events, but not so much conditionality, so much flexibility, that he needed a Turing complete. So he kind of, I'm going to say, chose a midway place.

I believe, you could have created Bitcoin and say there was no scripting language. It was just going to be a straight instruction, moving this input to another output. Created a little bit of computer code, but not a lot. That's what I think of the economics and the marketplace for this.

And next Tuesday when we talk about smart contracts-- and I promise you, there's a reason

for the craziness of my talking about Turing complete and scripting code. Because next Tuesday, we'll be talking about smart contracts where they're much more flexible. And so this is sort of the foundational-- and you don't need to know anything more about computer science than you want, unless you go with Tom down that rabbit hole and spend more time reading.

So there's four different types of, I call them script types. They're not actual script words, but you will read about these from time to time. And I just wanted to cover these four. The UTXO, remember, is about 54 million transactions. And there's been a nice academic paper that I didn't assign that was written earlier this year that investigated the whole 54 million, all of the unspent transactions.

And this is how it broke down. 81% are transactions that send to a hash of a Bitcoin address. Eight, nine years ago when Satoshi created this, that was not the most popular instruction. But it's basically sending an output to the hash, the compression, the commitment of a Bitcoin address.

We're now up to 18%. This didn't exist three and four years ago, really. But 18% go to a conditional script. It's a hash of a conditional script. So somebody saying, Emily, it's not even about time. It's like, you can only get it when all these other instructions that are in the scripting language happen. And I'm going to hide the conditions in a hash of it.

And then only 0.1% goes the way that he first envisioned nine years ago, directly to a Bitcoin address. So it's either to a hash of a Bitcoin address, a hash of a conditional script, and a little less than 1% now go to multiple signatures. Meaning, you need two out of three or three out of five. Or believe it or not, this academic paper shows that some say 0 out of 1. Now, it's hard to believe that somebody mistakenly programmed something to go to 0 signatures, but apparently somebody did.

So I just wanted to give you a sense there's some flexibility in the computer code, not a lot of flexibility, but just enough that you can do things that are really helpful. And they're going to solve a lot of challenges for Bitcoin. Hugo mentioned layer 2. We're going to be talking about layer 2 later in the semester, where there's a whole way to put technology on top of Bitcoin. And it's because the scripting language is there that you can do that. Any questions on script? I know I'm trying to cover a big, weighty topic in 120 seconds or less. No?

So just back to the whole-- this is just a review. What have we've talked about? There's that

little graphic again. It's just a bunch of blocks. That's what a blockchain is. Though today, we realize that underneath the blocks, we have another chain. I often think of two chains-- the chains of blocks. In Bitcoin, there's about a half a million blocks. But underneath that, there's all the transactions that are, in fact, chained, as well. 54 million of those outputs have not yet been spent and 290 million outputs have been spent.

But underneath about a half a million blocks, there's been 340 million outputs, so to speak. It creates a database. Bitcoin is a transaction database. Next Tuesday, we'll talk about an account-based database in Ethereum. But it could be a ledger which is transactions or a ledger which is balances. Satoshi Nakamoto decided to do transactions here. In some ways, I believe it's because it was fewer attack vectors. Probably a little bit more secure, but I'm not entirely sure. And until you solve the riddle as to who Satoshi Nakamoto is, we won't know the answer. Of

Course, hash functions we talked about, and digital signatures, and a consensus protocol. So I like to think of it in three buckets, whether it's for a dinner party conversation or digging into three lectures. It's the cryptography itself. We did that last Thursday. And if you have to remember anything, it's only two cryptographic primitives-- hash functions and digital signatures. How many people think they kind of roughly have what a hash function is? All right, so I lost half of you.

[LAUGHTER]

All right, is there anything I can do for Lauren's table? I didn't see a single hand go up. Are you reading your Facebook page or are you listening to the class? You've got your computer open. What's your name.

AUDIENCE: Matthew.

GARY GENSLER: Matthew. All right, that might have been that you weren't listening to the class. Thank you. How can I help in what a hash function is? My promise is to bring everybody along. Nobody at your table said you even roughly got what a hash function is. I'm not trying to embarrass anybody. I'm trying to work this through. Nicholas, so give me a baseline. Did you read any of the readings? Maybe not. OK.

AUDIENCE: I have, yes.

GARY GENSLER: You have, OK. Hash functions came along decades ago to help facilitate database management. Sometimes it's called a registry. It's taking a lot of data and shrinking it down, compressing it, shrinking it, to maybe a series of numbers. I think of it sometimes as a zip code for information.

Down in Baltimore, Maryland, I'm in 2120-- well, I grew up in 21208. It was my parent's zip code. I won't say my current. We're being videoed.

[LAUGHTER]

And so I think of it a little bit like that. So a hash function that has nothing to do with bitcoin came along to take a bunch of data and create a registry. But through that, it also became a way to do a commitment. Yes, your first name?

AUDIENCE: Dana.

GARY GENSLER: Dana?

AUDIENCE: Yeah, Dana. What goes into the hash function and comes out as a hash, that's what I don't understand.

GARY GENSLER: So what goes in is any set of data. Today, that could be an entire movie. It could be a picture of everybody in this room. Initially, it was mostly alphanumeric data. But because, in computer technology, all data can be broken down to a series of registries of 0's or 1's-- computers started with-- literally the first one started with registries that were either turned on or off. If they were on, call that a 1. If it was off, call it a 0. I'm not sure which way it goes. I keep looking at Alin.

And so all data can then be brought down to a series of 0's and 1. And if you put four 0's and 1's in front of each other, 2 times 2 times 2 times 2, 2 to the fourth is 16, all of a sudden, you see if you keep going 2 to something, you can get a lot of data. So sit back to answer your question Dana, when we talked last week about *The New York Times* crossword puzzle-- *The New York Times* may, if they wish, take the solution of their crossword puzzle and hash it. And then Stephanie?

AUDIENCE: Yeah.

GARY GENSLER: Stephanie likes to do *The New York Times* crossword puzzle. And she wants to know if she

properly completed *The New York Times* crossword puzzle. *The New York Times* could say to her cell phone, we're not going to really give you the answer, but we'll give you the hash of the answer. And then when she's finished and she pushes a button, her application could say whether her answer properly hashes to theirs.

AUDIENCE: [INAUDIBLE]

GARY GENSLER: Please. We're trying to learn here together.

AUDIENCE: In the case of a blockchain, it's whatever dated you loaded to the blockchain, and then in Bitcoin, it's just the transactions. Is that right?

GARY GENSLER: So in Bitcoin and blockchain, they use hash functions in several big ways. Everything you said was correct, except for the one thing when you said, it's just. Because they actually use hash functions in the middle of the proof of work. Because the hash pointer points-- block 3 points to block 2 and there's hashing. They use the hash function to compress a bunch of data, what I call the Merkle Tree, but it's taking 1,500 or 2,000 transactions and squeezing it into one hash.

So they're hashing all of these things up. It uses hash functions in the midst of the Bitcoin address. So the hash function is like electricity in the middle of it, almost. It's probably used six or eight places, and some I don't, in any way, know myself or need to understand. Nicolas, how are we doing? Did we get a little closer?

AUDIENCE: Yes.

GARY GENSLER: Lauren, did we get a little closer?

AUDIENCE: Yeah.

GARY GENSLER: Matt?

AUDIENCE: Oh, yeah.

GARY GENSLER: You're there.

AUDIENCE: I'm not there yet, but I'm closer.

GARY GENSLER: Stop by. Send me an email. It's gensler@mit.edu. I'm here like four days a week. Ben.

AUDIENCE: So I think the time that I really understood hash functions was when I saw someone do a live

demo. It's a website called [INAUDIBLE] Brain Wallet. But you type in text, and in real time, it converts it into a hash. So

GARY GENSLER: Say the website again, Ben.

AUDIENCE: It's brainwallet.io.

GARY GENSLER: Brainwallet.io-- a recommendation.

AUDIENCE: You can also just Google Brain Wallet blockchain. And you can type in text, and you see in real time it converts it into a Bitcoin address. If you change one letter, or make one in uppercase or one in lower case, it changes in real time. And it's just, you put any text in, you put a password in, and it turns it into a blockchain address. And that's all a hash is. It translates text into a hash.

GARY GENSLER: Or a whole movie.

We talked about the network consensus, how to actually agree on the state of information with no centralized authority. You don't have a central bank or a commercial bank or a Facebook or a parental unit, if you wish. It's all of us out there on the playground figuring it out together somehow.

AUDIENCE: Sorry, I have a quesiton here. For the proof of work, my question is, for example, I make a transaction, does it mean I have to wait for 10 minutes for the transaction to be completed? Or for example, when we do Venmo, it's like instantaneous. I can immediately get the results.

GARY GENSLER: Anton's question is, does it mean I have to wait 10 minutes? Venmo and so many other payment practices can go more quickly. The answer to you is, yes. And that is one of the commercial challenges to blockchain as we know it in Bitcoin. There are certain approaches to that, layering in technology on top of, they call it layer 2 or lightning network. We're not going to dive into lightning network.

But everybody should hold onto Anton's question. It's the right question, that if all of you bring your critical reasoning to this class about markets and about commercial realities, a little bit about the law and a little bit about technology. Because that's what we're trying to do. It's like, oh, well does this really matter? Will it work? Hugo.

AUDIENCE: So just a point of contention here--

GARY GENSLER: Contention?

AUDIENCE: A little bit.

GARY GENSLER: Oh, very good. I like that.

AUDIENCE: So if you know the person that you're transacting with, you can accept the transaction with 0 confirmations. As long as it gets into the mem pool and has a reasonable fee attached to it, then it will eventually get included on a block, and that's probably good enough for most people.

GARY GENSLER: So what Hugo is saying is, another approach is to take counterparty risk, that Anton's-- back to Anton's question-- does it mean you have to wait 10 minutes? The actual technical answer to that is, no, you don't have to wait 10 minutes, unless you want final settlement, if you want finality with no counterparty risk, no commercial risk.

Hugo is saying, well, if I'm willing to take some economic or commercial counterparty risk, which is, in finance, you take it all the time, then maybe I can do it in less than 10 minutes. And in fact, even Starbucks, when Starbucks accepts your credit card swipe, they're taking a little bit of counterparty risk from the payment processing company First Data. I don't mean to say that it might not be also from Visa and the banks. But I'll just say the payment system has some counterparty risk. Because final settlement in our payment system doesn't happen within seconds.

So the actual answer-- thank you, Hugo. Clean me up again. You should do this all the time. Everybody should clean me up. It's that final settlement can happen. And so you have to find other solutions, whether it's some commercial arrangement with counterparty risk or other technical commercial arrangements. Shimon?

AUDIENCE: Well, I'll make a counterargument, which is that, 10 minutes is not final settlement, right? Because it could be forking. So it's basically the probability of the finality goes up with time, which is associated with how many blocks are attached to [INAUDIBLE].

GARY GENSLER: So Shimon's point is that, even in 10 minutes, your probability of finality is not complete. Because the block might not be the block that's included in the longest chain. And many people have said, you maybe should wait three blocks or six blocks. I think the longest-- I'm going to use the term loosely-- orphaned chain has been five blocks long. And in Bitcoin, what's the longest orphan?

AUDIENCE: It was an accidental fork. It was 20 or more blocks. Due to some crazy things that miners were doing, they accidentally forked a blockchain.

AUDIENCE: OK, and what year was that?

AUDIENCE: So look up March 2013 fork. And there's another fork after that, in 2015 maybe.

GARY GENSLER: Yeah, somebody's been down the rabbit hole.

[LAUGHTER]

All right, there's some still probabilistic risk. Aviva, and then we'll move on.

AUDIENCE: What's a fork.

GARY GENSLER: So I don't have the chart up. But if you remember, there was the slide that showed the longest block. It was in black. And it had little purple blocks. That's a fork. There's some forks that end up being that both chains continue for a long time. They're called hard forks. And there is something called-- Bitcoin and Bitcoin Cash have come out of that. Most, the way that Alin was using it, are discarded. I'm sorry, behind you, remind me of your first name?

AUDIENCE: Erin. I don't know. Let me know if it's not the right time to ask this question. But I'm getting a bit confused between the most important things we now need to know, and the differences between the technology of mining Bitcoins versus just transacting on the blockchain. What are the major differences we need to know?

GARY GENSLER: Very good question, Erin. Erin's question of, what do I need to know about mining, what do I need to know about transaction, is it one and the same? I apologize. They overlap, but they're not the same. So think of a Venn diagram. But it's a very good question.

The essence of mining is creating an incentive structure where there is no central authority to validate and put a new set of transactions or data-- I'm going to say broadly, data-- into the ledger, into the accepted state of what reality is. So mining helps with that. That's that whole process. In essence, who gets to decide the next block of data? Transactions are included in the data, but it's not identical. Mining is really critical, but it's not the only component.

In terms of transactions, then you have to actually think of, well, there's this other thing going on. Well, there's been 340 million of these in the Bitcoin network so far. And has it been used

already? Has it been spent? Does it have an appropriate digital signature? If there's a time lock on it, is there a condition? Might there even be this little bit of scripting code that puts other conditions, like there has to be multiple signatures? Has it been double spent?

It was a very good question. They overlap a lot. One thing you can just remember is, mining is about that there's been a half a million blocks. Transactions, there's been 340 million. So there must be something else going on in all those transactions. Does that help a bit? Kelly?

AUDIENCE: Since we're talking about all the technical features and how they overlap, one of the questions was, what part of blockchain is novel to Satoshi? Is the novelty in bringing it all together, or is it one specific thing? Because the paper talked about the ledger and creating the incentive, and then sort of solving the whole Byzantine Generals Problem. But I don't really understand. Was there a specific thing that unlocked the--

GARY GENSLER: So Kelly's question, which is the heart of the study questions is, what makes the whole Satoshi paper novel? Is it just bringing it all together, or is there something more? I'll give you a hint. I think there's one other-- I think that the genius can be just in bringing together things. That in itself can be sheer genius.

AUDIENCE: There's also the part that, creating the value in the currency. But I don't know if that's--

GARY GENSLER: Right, so creating an incentive structure within there. Others? Derek.

AUDIENCE: Yeah, I have a question.

GARY GENSLER: Question, or answer to Kelly's question?

AUDIENCE: No, I had a question.

GARY GENSLER: All right, I'm going to hold your question, Derek, just for a second. Who's going to help me with-- because it's central to the study questions.

AUDIENCE: Just another thing to add-- the proof of work that Satoshi did on the consensus to [INAUDIBLE] it's also novel.

GARY GENSLER: Yeah. But novel, though, didn't Adam Back already do some of it in hashcash. So its application was novel. I come out where I think the genius is bringing it all together, and using Adam Back's proof of work in a way that really addressed double spend. Adam Back was not dealing with a double spend issue. He had different challenges. It was about email spam.

Frankly, it didn't even work with email.

AUDIENCE: [INAUDIBLE] we weren't counting [INAUDIBLE] work as a completely novel thing, his article discussed how it was already published. So I guess it's the application.

GARY GENSLER: It's the application specifically to the double spend. Now, Patrick Murck, would you answer it then? This is somebody who ran the Bitcoin Foundation, but he's a lawyer, you know?

PATRICK MURCK: I think that's absolutely right. So usually-- and I think they address it in that particular paper-- when somebody says, what was a thing that was different about Bitcoin from everything else, the answer is Nakamoto Consensus, right? And Nakamoto Consensus, being the incentive structure pulling everything together and aligning everybody to actually create trusted signing parties for this database, without having to actually trust or identify those parties. And that's something that really hadn't existed before.

And so that's really novel. That's sort of the breakthrough that I think you can attribute to that particular white paper. I also use this as a way to give a clean definition of blockchain, which is a badly abused term, as I'm sure you'll discover through the rest of this class. It's saying, to me, a blockchain is something that is born from Nakamoto Consensus.

Blockchains, as they discuss in that paper, have existed for decades. That's not even a novel data structure. But using that to form Nakamoto Con-- that's the thing. It always sort of comes back to that. Anyways, maybe a longer elaboration than you wanted.

GARY GENSLER: Good, there we have it. You now know that you're in a class that has guest speakers. I do want to say on the guest speaker point-- and Derek, I cognizant that you have a question, but we have 12 minutes or so. Next Tuesday, Larry Lessig, who sometimes floats into this class, has agreed to guest lecture with me. And so we're going to co-do smart contracts.

And let me just say a little bit about Larry. You sort of see him here. He bicycles over from Harvard. He's a constitutional scholar that's a remarkable constitutional scholar. And even though he came to be a full professor at Harvard, they stole him away from Stanford actually, where he was a full professor, too, readily. But he's extensively written. Anybody in here a *West Wing* fan, the television series *West Wing?* He is the only-- do you know that Larry Lessig was in West Wing?

AUDIENCE: No.

GARY GENSLER: Now you do. Well, Larry was. And Christopher Lloyd played Larry Lessig in one episode. But you'll go back and you'll find the episode. And Larry has a funny story about watching the filming of it. But Larry is a constitutional scholar over at Harvard. He clerked for Justice Scalia on the Supreme Court. He clerked for Posner over in Chicago.

He knows a lot about contracts. And so I asked him if he'd help teach smart contracts next Tuesday. So Larry's going to-- we're going to Mutt and Jeff it up here next Tuesday. Watch out, Patrick. You might be up here one day.

This is not a class that we're going to have a lot of guest lecturers. Later in this semester, I hope, we're still in confirming Jeff Sprecher, who's the chief executive officer of Intercontinental Exchange, runs the New York Stock Exchange. Jeff is probably joining us on, I think it's November 15. But I really want to stay to the content and so forth. Derek, what's your question?

AUDIENCE: I can follow up with you on that.

GARY GENSLER: OK, follow up. All right, and then we just did transactions today. Remember, the hash function is *The New York Times.* We're in a little better place with Lauren's table now. All right, good, good.

My goal is not to embarrass anybody when I ask these questions. My goal is that we all come along on this journey, that we somehow have some basis. Because it does relate to understanding the commercial reality and the economics. We talked about the time stamping and the blocks, the Merkle Trees, which is not a deep part of it, and of course, digital signatures.

Part of the reason I replay this each time is because, in politics, I, of course, learned that repetition is a really important thing.

[LAUGHTER]

But I also think it's true in academic settings. And then Bitcoin addresses, and that's just a cleanup, that it's not an identical to a public. And then the proof of work, and back to the questions. Nakamoto Consensus is, yes, all of this and an incentive structure, but it's this proof of work. And to Erin's question, proof of work is a little bit different than the transactions that we talked about, but there's a lot of overlap. And then it creates the native currency. And I've corrected this slide to 2140, of course.

The network is really critical, too, and that there's all these different actors on a network, 10,000 nodes and this many light nodes and the miners and the mining pool operators. And they all have their separate economics. And so if anybody wants to come and get office hours, talk about those economics, please come on in.

If there's nothing you remember from the reading, I've now read this paper probably six times to kind of slowly get it through my head. But every time I read the Clark paper, I go, wow, that really helps me. Because it's not like Satoshi Nakamoto just flipped his fingers and there it-- it was on the backs of a lot of cryptography, a lot of technology earlier.

But this is the chart I turn back to, and it's sometimes helps me. Ah, there's time-stamping, there's digital cache, there's proof of work, and how these things. Maybe 10 years from now, they'll look back and Nakamoto's stuff will just be built upon. That's the central question. That's what some of our colleagues are doing over at the Digital Currency Initiative or over at the Computer Sciences Lab. They're saying, can they build upon this and take it to another level?

Right now-- and you'll see throughout the semester-- there's not a lot of full scale applications of this technology. But it might just be in a whole line of this. Yes, and I can't remember your first name, Aviva?

AUDIENCE: I'm Aviva. And that is the other Indian woman.

GARY GENSLER: That's the other Aviva.

AUDIENCE: That's the other Indian woman.

GARY GENSLER: Yeah, yeah, it's important. Out of 100 people, we can have two Avivas, you know? We could even have two Aviva's if there's two.

AUDIENCE: [INAUDIBLE] name's Priya.

AUDIENCE: I'm Priya.

GARY GENSLER: Pria-- oh, I'm sorry. Thank you.

AUDIENCE: So I was just thinking about, as one of the applications of the hash function-- so does the hash function actually replace the data? So I'm thinking now that everyone's saving data in the cloud, so can you save a hash function instead of your actual data, and then so it can be

compressed?

GARY GENSLER: Very good question-- my summary of it-- though others' probably would be more expert. My summary is, you get a choice. You could do either. So let's take it in blockchain rather than in the cloud. You can choose to save in a blockchain just hashes, and have the full picture somewhere else. Let's say you were going to do a whole database of--

AUDIENCE: A library.

GARY GENSLER: Of what?

AUDIENCE: I'd say like a library.

GARY GENSLER: A library-- and so there's 100,000 books in the library. You could hash all 100,000 books, and then store the hashes in the blockchain and not the books themselves. And that would form a blockchain of the commitments to those books. Or you could actually, I guess, put the books themselves into the blockchain. Now, I saw some shaking heads in the middle. Alin from the Digital Currency Initiative.

AUDIENCE: The way I understand this is, the answer is no. You can store the hash. That doesn't replace the data. The storing of the hash allows you to prove that you have the data. But the fact that you store the hash doesn't mean that you store the data.

GARY GENSLER: But Alin, there's a two-part question. You shouldn't get rid of the book, because hashes are one way. You're not able to take the hash and recreate the look. You can't take the hash and recreate *The New York Times* crossword puzzle. But you don't need to store them in the same place. Thank you, because it's two parts the question. You could store the hashes in the cloud and store the books somewhere else. But you still need to store the book, maybe.

So who is Satoshi Nakamoto? We have just a handful of minutes, but can every table-- each table's going to take four minutes. And amongst yourselves, decide who is Satoshi Nakamoto.

So how are we doing? Who's your answer to Satoshi Nakamoto?

AUDIENCE: We would say, probably multiple people, led by Hal Finney.

GARY GENSLER: OK, so the first one is, multiple people, probably led by Hal Finney.

AUDIENCE: NSA.

AUDIENCE: Something within the government or a government.

GARY GENSLER: So table number 2 is, government actor, US or foreign.

AUDIENCE: I don't know if it matters, but maybe US.

GARY GENSLER: US, but it might not matter. How are we doing over here?

AUDIENCE: Dorian Nakamoto.

GARY GENSLER: Dorian Nakamoto-- so you're going with the *Newsweek* story. Pria, sorry about the name thing before. Your table, who--

AUDIENCE: A bunch of crypto punks.

GARY GENSLER: What's that, a bunch of crypto--

AUDIENCE: Punks.

GARY GENSLER: Punks.

AUDIENCE: Plus economists-- it's like a group of people.

GARY GENSLER: So a group of crypto punks and economists. And how do you spell crypto punks, though?

AUDIENCE: Cipher punks.

GARY GENSLER: Cipher punks, cipher punks, actually. Where are we here?

AUDIENCE: NSA.

GARY GENSLER: Oh, the NSA, all right.

AUDIENCE: People with incentive and the capability.

GARY GENSLER: Oh, so incentives and capability, you think it's NSA.

AUDIENCE: MIT.

GARY GENSLER: MIT, oh!

AUDIENCE: We said, a guy named Gary Gensler.

[LAUGHTER]

GARY GENSLER: There is a word for that, but I can't say that on tape. Kelly, Anton, two Alins what do we have here, Jihee.

AUDIENCE: Let's go with Nick Szabo.

GARY GENSLER: Nick Szabo, who wrote the first paper on smart contracts. So Aviva is Nick Szabo. My hash table--

[LAUGHTER]

GARY GENSLER: Who do you go for?

AUDIENCE: We actually did have him, Szabo.

GARY GENSLER: All right, you can say another table for Nick Szabo. Put another vote next to him. Here?

AUDIENCE: We're going with you, Gary.

GARY GENSLER: No, no, come on.

AUDIENCE: We think it's Craig Steven Wright.

GARY GENSLER: Craig Wright, the Australian. Oh, my god. Oh, Patrick Murck's table is going to go last. Here?

AUDIENCE: Bill Belichick.

GARY GENSLER: Bill Belichick.

AUDIENCE: Alan Greenspan.

GARY GENSLER: Alan Greenspan. I actually know Alan. He's really talented, but I don't think Andrea would let him do this. Here, who do we have?

AUDIENCE: [INAUDIBLE]

GARY GENSLER: Who?

AUDIENCE: [INAUDIBLE], me.

GARY GENSLER: No, no, but who-- you're saying you invented it? No, no, this table.

AUDIENCE: This table is saying he invented it.

GARY GENSLER: Nick Szabo, so another for Nick Szabo. So does anybody want to tell us why it's the NSA? Oh, Patrick Murck, I'm sorry. What's this table?

PATRICK MURCK: Well, I said, if I-- so I don't know. But if I did know, I would say that I don't know, and I would create as much obfuscation as possible. So I think I was the worst person to have at a table for this. And I did them nothing but a disservice in their hunt for Satoshi. But I'll let somebody else speak. No, I don't know.

GARY GENSLER: But if he did know, he would say he doesn't know. Derek, who did your table go for?

AUDIENCE: We said Craig Wright.

PATRICK MURCK: You can see my influence.

GARY GENSLER: Oh, my gosh. So let me ask this, because it's just for fun, one minute. Somebody said that it was the NSA. Do you want to say why?

AUDIENCE: Because, arguably, they have the most advanced cryptography in the world. And if anybody was doing this, to have a system where all the dark money in the world was flowing around instead of $100 bills, you would create this and create it in a way where you could hack it backwards and figure it out. And they have the capability.

GARY GENSLER: Wow. Hugo.

AUDIENCE: More [INAUDIBLE] money is going through [INAUDIBLE] right now than it is through Bitcoin.

GARY GENSLER: So Hugo would say that, if it was the NSA, it didn't work out for them too well. And those of you who said Craig Wright, I heard some others in the room that said, no. So who said Craig Wright? Which two tables said Craig Wright? Isabella and Ben, why did you pick Craig Wright?

AUDIENCE: So I read a bunch of it. And basically, people analyzed the English used in the email, and they think it traced back to Australia. And then we [INAUDIBLE] from there.

GARY GENSLER: All right, so just the language analytics for Craig Wright. And those who said it can't possibly be Craig Wright, who did that? Alin?

AUDIENCE: Yeah, so he started a website. He said, oh, here's cryptographic proof that I'm Satoshi

Nakamoto. But he actually botched it. Like, if you are Nakamoto, you can prove you're Nakamoto by spending the first coin. But he couldn't do that, so come on, man.

GARY GENSLER: So Alin says, he failed the test. He didn't spend the first coins from 2009. Three tables picked Nick Szabo. Why'd you pick Nick Szabo, just any one of the three tables? Because we're going to talk about him in the next lecture. No?

All right, look, this was a bit of fun. I just thought it would be worthwhile. Because the only person in the room that really knows who Satoshi Nakamoto is isn't going to tell us. [LAUGHTER] But you're welcome back any time. Thank you. We'll see you next Tuesday. Remember, Larry Lessig is here, so please do the readings. Please, let's have a good time.