PROFESSOR: I'm excited, because I'm going to get the chance to co-teach today with-- I would say one of the students, but it's not really one of the students. But Larry Lessig has consented to join us in a few minutes. So I'm going to be breezing through a little faster than usual. And then we'll co-teach this.

Blockchain and Money. Here we are. We're at smart contracts. Everybody seems to be coming back, which is a sign of your interest more than it is in my teaching. But I thank you for being here.

We made it through the last three classes together on bitcoin and the basics of that technology. And in one class, we're going to try to chew off a bit on smart contracts, both the technology side, a little bit on the markets, and then the law that Larry is going to take us through.

And so as I said, I want to start with a little administrative, because we are on the sixth class. I'm going to review a bit about the projects very quickly.

We're going to do smart contracts, the design. What design features? Yes, we're going to go back a little bit about hash functions and Merkle trees but not too much. DApps, which are basically decentralized applications, and token sales. Larry's going to take us through legal issues, and then we'll sum it all up.

So let me just, real fast on the administrative side again-- class participation, 30%. That's why we're all here together. That means, hopefully, reading the assignments and participating.

About half of you have participated, so I guess I'm going to go with a little bit more cold calling starting Thursday. I'm not going to do a bunch of it today, because Larry and I are joining. So you can ease off. But really be conscious. If you haven't been participating, try to get in and join the conversation and discussion.

The two individual write-ups, I think we have seven. But it's quite possible some of you have submitted already. It's just meant to be critical business reasoning. We are in a business school. To the extent you just summarize some readings, I'm sure we'll give you a pass on that.

But that's not what I'm looking for. I'm really looking for critical reasoning and thinking from a business perspective of, why does this matter? What are its strengths or its values in terms of business reasoning and critical reasoning?

One by the 10th class, one by the 23rd, always before class. What it likely means is we'll be getting most of these on the 8th, 9th, and 10th class. I know how that works and so forth. And that's OK. That's OK. But I'm just reminding you of that.

In terms of the group research paper, again, Sabrina and Thalita stood up a Google App-- I think it's in Google, but-- where you can go in and team up in teams of three or four. It's not required to do this by the eighth class next Tuesday, but I'm strongly suggesting it to figure out who your teams are and not sort of wait till the second half of the semester.

And I'd like to encourage everybody to choose an area for your use case by midway. Again, you're not going to get graded if it takes you another class or two to figure it out. But I just think it's much better if you know your teams, you know what your use case will be.

If it's not about finance-- one group has already asked me if that's all right. I just want to know more detailed what it's going to be. I'm probably going to say yes, but it needs a little bit of preapproval if it's outside of finance. So any questions about the requirements? I just wanted to--

So the study questions. Today's smart contracts and basically how they compare to regular contracts. And what are the tokens that are used within that ecosystem? And what are the platforms?

In a very similar sense to the internet, we have the internet. And then above the internet, you have, you might say, applications-- Facebook and other applications. Well, this, too, has a series of platforms and then decentralized applications potentially on top of that.

And basically, a quick touch on decentralized applications. Later in the semester, we're going to take two sessions on initial coin offerings. And thus, we're going to talk a lot about token economics. So this will be just the first taste test, and then we'll come back to it later.

And then the readings, hopefully, everybody read through "Smart Contracts." I thought the Chamber of Digital Commerce, even though this is almost two years ago, this paper was a very helpful sort of flavor for what folks in commerce are thinking and what developers were thinking. And I love that Nick Szabo wrote the introduction to it. And it's interesting to see and question, why is it that it's two years later, and many of those use cases are still being discussed but haven't fully been adopted?

And then the "State of the Dapps," and then who are the competitors to Ethereum? So don't you feel good? I haven't asked anybody a cold question yet.

And then the optional readings, I don't know. Did anybody actually go back? They're optional. Did anybody go back and read either Szabo's original piece from 20 years ago on smart contracts? Oh, a few of you are kind of into that rabbit hole of blockchain and ether.

Brotish what did you think of-- it's 20 years ago he wrote this thing on-- Nick Szabo wrote this thing.

AUDIENCE: Actually, I spent more time on the Ethereum white paper.

PROFESSOR: All right. So what did you think about the Ethereum white paper one?

AUDIENCE: Yeah, I think it was pretty good. It gave me a very good overview of the world potential of the [INAUDIBLE].

PROFESSOR: Yeah. And what's interesting is even if you didn't do it for the class and you find yourself more and more interested in this over the next couple of months or even later, going back and reading the Ethereum white paper, it's not highly technical in the first, I don't know, 10 or 15 pages. It really gives a history of bitcoin. It talks about distributed applications and largely written at the time by a 19-year-old, as well. It's a remarkable thing.

And then one of Larry's colleague, or maybe it's two of them, but De Philippi paper, as well, on the regulatory issues. So let me talk a little bit about smart contracts and laying groundwork before Larry gives us the law.

A smart contract is a set of promises specified in a digital form. I'm going to say four things. It's just a set of promises in a digital form. So it's not handwritten out.

It includes protocols. What's a protocol? Andrew.

AUDIENCE: Standard operating procedure.

PROFESSOR: Standard operating procedure. I like that. Anybody else give me another word for it, maybe? An algorithm.

So a set of promises in digital form. But it can include math, basically, if you wish or standard operating procedures-- if-then statements and so forth.

And the parties then perform against these promises. And guess what? Nick Szabo wrote that in 1996. And I thought it was still probably the best definition of smart contract.

He coined the phrase 22 years ago. He might actually be Satoshi Nakamoto. Three of the tables in here, you all voted that it was Nick Szabo.

So I thought that's kind of the best definition if you've got to just-- kind of a root. Now, I would also say, however, that smart contracts may not be so smart. A lot of people have come to be calling them dumb contracts that are just algorithms that perform a function.

So don't think of them as artificial intelligence. That's another class provided next semester by Simon Johnson. Think of them almost as just dumb contracts. And in a sense, they're mechanizing what might otherwise be done amongst and between humans.

And smart contracts may or may not be really contracts. And that's why Larry's going to speak to it. So remember, even though Nick Szabo calls it smart contracts, they may not be smart, and they may not be contracts.

So a little bit about the technical features. Remember our three ways we did this. What are the big technical features that we studied? I'm sorry to do this. Anton, what are the three big buckets? Remember, we took three classes and three buckets of information. It can be one to three.

AUDIENCE: Cryptography.

PROFESSOR: Cryptography. Great. You got one. Two other people will give me the others.

So cryptography. Guess what? Bitcoin and Ethereum all have the same cryptography. It's not identical. But for the purposes of design features, it has cryptographic hashes, timestamps, block headers, Merkle trees. Though Ethereum has more than one Merkle tree, and bitcoin has one. And it has digital signatures and addresses.

So everything we talked about three lectures ago about cryptography, both forms of blockchains. Anybody want to give me what our second bucket was? Geramo.

AUDIENCE: Decentralization.

PROFESSOR: Decentralization. What else did we talk about? Eilon.

AUDIENCE: Consensus.

PROFESSOR: Consensus. So again, decentralized network consensus. Ethereum actually uses proof of work even there's some talk that Ether will move to proof of stake. But it's currently proof of work.

There is a native currency. It's ETH, or "eh-th," or E-T-H, or Ether, instead of bitcoin. And it has a network. The third thing that we talked about, Alpha.

AUDIENCE: Transaction format.

PROFESSOR: Transaction format. So we talked about transactions and script. Well, guess what? Ethereum does not have a transaction script or UTXO. So that's the one place that Vatalik Buterin, who designed all of this, said no, had to go a different way.

Instead of transaction inputs and outputs, there's something called state transitions. Isabella, ledgers. What are the two different types of ledgers that we talked about and set a class to?

AUDIENCE: Permissioned and public.

PROFESSOR: So permissioned and public are two different types of blockchains. Remind me your name again. Stephanie.

AUDIENCE: Balance ledgers and transaction ledgers.

PROFESSOR: All right. So balance ledger and transaction ledger. You can keep a list of transactions. And this goes back thousands of years. This is not a blockchain. Or you can keep balances.

Bitcoin is, in essence, a transaction ledger. Ethereum and many of the other smart contract platforms are balance ledgers. There's a lot of technological and mathematical reasons why, which I'd be glad to do in office hours.

But because of that, when you're moving from one set of balances, like-- is it Bo? Bo has $100 at Bank of America to Bo having $101. You need to have a transition. It's called a state transition, which would mean add $1.

So Ethereum is account based and, in fact, doesn't even have one programming language. There's six or seven programming languages you can write in, for those who are so inclined.

So I'm going to go through really quickly my analysis, and many other people's, but my sort of rendition of the difference between Ethereum and bitcoin. But stop me if there's a question.

So the founder. There's actually a founder. The mythology around Vatalik Buterin might not be as great as Satoshi Nakamoto. But a 19-year-old journalist who was writing about bitcoin for-- was it *Bitcoin Magazine,* if I remember where he was writing-- said, we can build something on top of it using Nick Szabo's thoughts about smart contracts, about six years after bitcoin.

He made it Turing complete. Does anyone want to remind the class what Turing complete is? Did I see a hand up? Yes. Bold of you. What's your first name again?

AUDIENCE: Alana.

PROFESSOR: Alana.

AUDIENCE: You could write pretty much any-- well, you can write loops, but you write any kind of program, like any form of logic is expressed.

PROFESSOR: So Alana says Turing complete means you can write loops. But what that really means for the business crowd is it means you can write a program to do just about anything. It's highly flexible.

I'm sure the technologist in here will say, well, maybe there's something you can't do with it. But the point in what Vatalik said is we shouldn't just limit it to a scripting language that was non-Turing complete that can just move a little bit of peer-to-peer value around, that he wanted to do basically a peer-to-peer virtual computer that could move code and complete code.

And over the years, it's being able to be written in a bunch of things. But Solidity is the main program language. And thus, it's account based rather than transaction based because of the loops. If you could loop and be Turing complete with transactions, there is a vulnerability in attack factors that he made it account based.

The transactions are stored in Merkle keys. But guess what? If you were really interested and wanted to learn everything about Ethereum, there's at least four key Merkle trees that get summarized up into the block headers.

There's the transactions, which, in essence, aren't transactions. They call them state transitions. There's the state itself, something called storage, which is really related to each one of the individual Ethereum accounts, and then, believe it or not, actually, receipts. There's written records of receipts from every state transition.

So there's a lot more complexity inside the Ethereum blockchain. They run about 14 seconds a block instead of 10 minutes. And that change is a bunch of the economics.

Proof of work, for some reason, which others can study. Vatalik decided to use a different hash function. It's still based on elliptic curves, I think, but a different hash function.

What about the economics? Well, it's called ETH or E-T-H. It's programmed in such a way that you can't use ASICs, purposely makes it that mining is more decentralized, and you don't have the big factories.

The entire hash community, the entire mining community, is much smaller. In fact, I think it's about-- what would that be? 200,000 times smaller. There's 260 terahashes per second as of yesterday. And the bitcoin mining community has 54 exahashes. That means lots more computers, a lot more electricity, a lot more gnashing of teeth about resources.

Bitcoin started in January of 2009. And nobody owned any bitcoin, whereas Ethereum started with a presale and an ICO, which we'll be talking about, about 72 million Ethereum.

Vatalik wanted to raise money he was maybe 19 years old. He looped in with a venture capitalist from Canada, Joe Lubin, who now runs ConsenSys. Lubin took about 10% or 9 and 1/2% of the offering. They put 9 and 1/2% in a foundation called the Ethereum Foundation. And the other 80% was sold to the public for $18 million.

We'll talk later in the semester as to whether that was really a securities offering. I've publicly said I think so, but that was in 2014. And in 2018, the Securities and Exchange Commission has said regardless of why it might have been in '14, it's now sufficiently decentralized that we'll consider it not a security.

But in essence, they raised $18 million and were off to the races. Oh, and the 10% that Joe

Lubin kept, if he still owned it, would be worth about $2 billion now. But he probably sold some of it along the way.

There are block rewards. The monetary policy in Ethereum, if you remember, it splits every four years. There's the block reward splits.

Ethereum was set up that it was five Ether per block. And then a year ago, they just announced they were going to change the software to three Ether per block. And a month ago, they announced they're going to change it to two Ether per block.

So the monetary policy of bitcoin is said to be immutable and fixed forever. But I would say that because Ethereum supposedly was fixed and now, twice, they've changed the monetary policy, there is a form that if all the miners and all the computer nodes decide, they can change the monetary policy. And Ethereum has shown that.

I think Ethereum's a bit more centralized and has more leadership, because Vatalik Buterin is an actual human who is willing to disclose who he is. And he still has the sort of founder following.

And Satoshi Nakamoto went-- he ghosted all of us, in a sense. And so thus, it's in some ways socially just more decentralized.

And then fees are voluntary in bitcoin. They're a necessary part to channel everything. Emily.

AUDIENCE: Going back to monetary policy, in practice, what does it actually mean for a difference between bitcoin and Ethereum that it's fixed but changing versus staying at the same rate?

PROFESSOR: So Emily asks, what does it mean in practice? In practice, bitcoin has a much slower growth rate or inflation rate, which is currently, if I'm not mistaken, about half. What's that? About 4%. But it's about half of the inflation rate at Ethereum, which is running in the 7% range.

Every one of the 1,600 live tokens that are right now Ott coins have separate monetary policies. And one could do a complete economic study about what it means. But in terms of Ethereum versus bitcoin, Ethereum has a higher inflation rate.

And secondly, because they've shown that they can form some consensus and change it, I think it sends an interesting question into that ecosystem as to how hard a monetary policy versus a more human-based, flexible monetary policy. Hugo.

AUDIENCE: So is it that the core developers of the Ethereum blockchain decide? I'm not familiar with how they make that decision to change the monetary policy.

PROFESSOR: So the core developers of any coin can propose to the various mining and nodes to make a change, including the monetary policy. Even in bitcoin, the monetary policy could change if there was a proposal from the core developers.

In the Ethereum case, they have done that twice. The core development of Ethereum is highly concentrated around the Ethereum Foundation. ConsenSys, the company that Joe Lubin runs, has some normative social standing in the community, as well.

But it's been part of proposals. And in reading the proposals, it goes back to Emily's question. The core developers have said we should bring down the inflation rate. There's an active advocacy to bring down the inflation rate.

AUDIENCE: So you go by updating your node software?

PROFESSOR: Yes, in essence. And it could lead to a hard fork, I believe. So that's the background. Let me just talk about the platforms.

We know about Ethereum. We've just chatted about it. Its actual current market value is $22 billion. While we're not going to spend a lot of time in this class this semester about market values, I thought it would give you a sense of how people think about it.

The other five that you did some reading about. EOS, whose market value is about $5 billion, is so new, because they just finished an initial coin offering in July. And they just went live in July. But they raised $4.2 billion. So my estimate, my prediction, is EOS is going to be real and going to be around.

They've taken $1 billion of that $4.2 billion and set up a Kickstarter sort of venture firm literally so that they could maybe support some of you. You could be knocking on the EOS venture firm's door and saying fund me. I've got a great idea.

And they'd have one condition, amongst others. You'd have to use EOS as the platform. So it's a self-reinforcing business model.

NEO is the other big one that I'd mention, which was started two years ago out of China, a lot of people think with the backing of the Chinese government. Even if not officially, certainly with the verbal and help of there. Some people think of it as the Ethereum of China, but it does use a different proof of work.

And those are the main ones. Ethereum Classic is there because there was a hard fork off of Ethereum after the DAO circumstance. Any quick questions about the platforms?

And NEO and EOS are thought to be a little bit higher throughput and faster because of the different proof of work that each of them have. So maybe they're more scalable than Ethereum long term.

AUDIENCE: [INAUDIBLE]

PROFESSOR: What's that?

AUDIENCE: [INAUDIBLE]

PROFESSOR: So Hugo is pointing out that neither one truly use-- NEO and EOS truly use decentralized proof of work. They use a delegated Byzantine fault tolerance.

This was from the reading. We're not going to spend time on it. But there was 12 use cases that the Digital Chamber of Commerce came up with. And we're going to study most of these, not all of these, later in the semester. Please tell me, Sean.

AUDIENCE: So from the growth perspective across different platforms, do you support multi programming language platforms as opposed to single-language programming platforms? Which one do you think has more potential?

PROFESSOR: The question is, do multi-language platforms have more potential or less than single-language platforms? I haven't done a real study. My gut tells me that there's some trade-offs. So a multi-language platform probably allows for more development of apps, just like on the internet, if you can have more app development. Though if you have only one single language, you might have fewer vulnerabilities, vulnerabilities either to attack or coming down.

So there's probably some trade-offs. And I'm more into democratizing capital markets, so probably my biases would be to the ones that have multi-language potential. But I can't say for sure whether it will necessarily win, because there are some trade-offs, if that helps.

So we'll take a view of all of these later in the semester. But what's interesting is none of them have yet taken off. And in fact, if you look at the dApps today, the decentralized applications which run on a decentralized blockchain, they generally have native tokens.

They don't have to have a native token, by the way. You can run a dApp based on Ether. You could run a dApp on an underlying token. But they almost always have their own native token.

This is a list that I pulled off the internet yesterday similar to your reading. These are the actual dApps that are working the highest-- gaming, gambling, exchanges, and finance. The most active dApp is a gambling site that only has 1,500 users a day.

In the last 24 hours-- I pulled this down yesterday, so that was a Monday. So this would have been Sunday night to Monday night. There was only 1,500 users to the most active gambling site. CryptoKitties that some of you might know had 418 users in those 24 hours.

These are not economy wise use cases. You would see numbers that were hundreds of thousands. Or if it's like Facebook, there's two billion members. And probably in any 24 hours, there's a half a billion to a billion people that check in on Facebook. So these are pretty limited at this stage.

But it has led to something called initial coin offerings, which we're going to study a bunch later in the semester. Initial coin offerings raise money to build a network. But the tokens are usually issued before they're usable. And a token is some native currency to be used on a network.

The development is open but highly centralized. The promoters usually give themselves some skin in the game or some vig. In the Ethereum initial coin offering, the Foundation kept 10%. Joe Lubin kept 10%. And the other 80% was sold to the public. But some keep 60% or 80% for themselves. I mean, it's a whole wide range of economic incentives and models.

And the tokens are usually fungible and transferable. And thus, you can sort put them on an exchange and try to sell them and promote them. And again, we're going to come back. But I thought if we're talking about smart contracts, they tie into initial coin offerings. Daniel.

AUDIENCE: If the tokens aren't functional, what goes into their evaluation?

PROFESSOR: That is an excellent question. Daniel says, what goes into the valuation of something that is not functional? And there are many things that go in.

Ultimately, it's in the anticipation of the potential profit and appreciation in the future. So if you were just to have a laundromat, a corner laundromat here in Cambridge, you probably would only pay for the laundromat token what you thought the value was to do your laundry, $0.75 or whatever the-- frankly, I don't know what the tokens go for in Cambridge. You're going to tell me what a laundromat token goes for?

But if it's prefunctional and the laundromat has not been built yet and you have confidence it will be built, you'll probably discount back. You might pay $0.50 instead of the $0.75, ultimately. If you think it's going to be a really popular laundromat and it's going to be the place to be seen by all MIT students and you think that token might one day be worth $5, then you're starting to speculate on the community's interest.

So these tokens, if you really believe in them, you're trying to pay for what others will pay for them in the future. And the economic equilibrium would be discounted. So thus, you're buying it because you think they'll appreciate in value.

AUDIENCE: Couldn't you make an argument sort of following numismatics, how people assign some aesthetic value to physical coins? So, too, you could have an impulse beyond speculation [INAUDIBLE].

PROFESSOR: Your first name is?

AUDIENCE: Isaac.

PROFESSOR: Isaac. Isaac says maybe there could be a numismatic or other value to it. It's possible. I mean, certainly, CryptoKitties caught into the whole collectibles wave.

Let me try to wrap up so that I can hand it off to Larry. So there's been $28 billion raised per one website, Elementis. Others that track it think it's only between $20 and $25 billion. There are no official arithmetic and no official records.

But the $28 billion raised in initial coin offerings, this is a cut of a neat video that I just took the last slide of from Elementis. You can watch it in a minute and a half.

And over the years, it's geographically dispersed with blue being Oceana, Australia, and so forth, green being Asia, North America being orange. But the biggest ones, EOS raised $4.2 billion. Telegram, $1.7 billion and the like. These are not small figures.

There's been at least 4,500 proposed initial coin offerings. Many of them didn't raise any money, but over 2,000 to 3,000 have raised money. I'm going to use the 3,000 figure. Less than half of them are even live today.

There's one study that shows that 59% fail within the first nine months. There are other studies that say between 1/4 and 3/4 are scams. Christian Catalina here has a study which I think is probably the most valid and reliable, which says 25% are scams or frauds. Statis has one that says 80% might be.

AUDIENCE: You said 59% fail. Can you talk more about what "failure" means here? Does that mean it just goes to 0 or there's a technological deficiency?

PROFESSOR: Can I hold that until later when we're going to dig into these in the class? But broad definition of fail, so it's not just technology. It means that you can't even find the website anymore. They took your money, and they ran. Or they still have a website, but it's not live. It doesn't seem like there's a development team any longer. So multiple definitions of failure.

So that brings us to legal issues. And as Larry brings up his computer, let me just introduce our guest lecturer, Larry Lessig, who's an esteemed Harvard professor of law. He was at Stanford. He started something called the Center for Internet and Society. You clerked for Justice Scalia, so you must have some real views on what's going on this week, then.

And this incredible appellate court judge, Posner. And Larry also-- his first of-- whatever you're up to, 9 or 10 books now?

LARRY LESSIG: It's something. I don't know.

PROFESSOR: But his first was code and the law that I referenced in our first lecture. Larry is going to take it away.

LARRY LESSIG: OK, great. So I'm really happy to be able to say that I've taught business school students at MIT. I mean, I'm a tech wannabe. But I have never been allowed to be officially here, so this is exciting.

But what I want to do is really address what I've experienced as misperceptions about the nature of the law as it might interact with the issues around digital contracts. So I teach contracts. Contract law is one of the subjects which I've taught since I started teaching. And so I want to frame four points for you about how to think about contract law as it relates to these potential digital contracts.

But the first thing to do is just to make sure we understand we're all talking about the same thing. OK. So here's what the core of contract law teaches us contracts are. Contract is a promise or performance given in exchange for a promise or performance.

"Given in exchange for" is really critical. That's the quid pro quo that's sometimes referred to as the consideration for the promise. But notice here, this is mapping out four different possibilities. You can have a promise in exchange for a promise. I promise to pay you $10,000 if you promise to sing an opera for me tomorrow.

Or it can be a promise for a performance. I promise to pay you, Andy, $5 if you sing a song for us now. So it's the performance I want. I don't want a promise from him, because we know what Andy's promises are worth.

Or it could be a performance for a promise. I'll sing if you promise to pay me after I'm done. Or the really interesting one for our purposes is a performance for a performance. I'll sing if you pay me $5,000. I didn't want a promise from you, because I don't trust you. You're business school students. So I just want the money. But I'm not promising to do anything. I'm actually going to do something for you.

Now, that's the one that we're going to think about in the context of digital contracts. Oh, I'm sorry. Let me just fix one thing here. Actually, I was going to make three points, but then I decided I was going to make four. So let me fix that. Four points about contracts.

So the first point about contracts, so think about this case. All right. It's not quite digital, but it's a physical contract machine in the sense that it's a performance for a performance. If you drop a dime into this machine, then out will come Dr. Pepper or something else.

OK. So there's no promises involved. And we understand there's a mechanism that's to produce this result. And obviously, these have been here for a long time. And these mechanisms provide real value, because to the extent you don't have to hire somebody to stand there handing out Dr. Peppers, you can lower the cost of delivering Dr. Peppers and increase the market for Dr. Pepper.

So this is the motivation-- lower the transaction costs of engaging in a particular kind of contract, which is performance for performance. Now, when you look at that contract, you should ask yourself, what are the terms of this contract?

All right. So some of them are express, and they're pretty obvious. So this says $0.10. It says if you pay $0.10, you will get the Dr. Pepper. Or that's what you kind of expect.

There's a great cartoon I couldn't find where you come to a machine that says deposit $0.50. Deposits $0.50, and the light comes on. It says, thank you very much.

Right. So you think you know what this contract is, but that joke hints that maybe you don't know what that contract is. But the express terms of the one we expect go with a statement, the machine. But then there's a whole bunch of implied terms.

So one implied term if this machine is in the United States is that when you take the Dr. Pepper out and you drink it, it's actually going to be safe to drink. It's actually going to be Dr. Pepper. It's actually not going to make you sick.

And none of that is written on the Dr. Pepper machine. That's instead a term, a contract term, that gets created by the law and gets imposed or wrapped around the delivery of that drink.

OK. That's their first point. The second point is to think more about what these implied terms imply. Because if these implied terms are implied by a legal system, then that means the legal system has an interest in your contract. Legal system is not undisinterested in your contract.

So we should always think that our contract is going to have two parties. We call them the promisor and the promisee. I've told you we've had contracts that can be performance. "The performancer" isn't really a word. But let's just say promisor and promisee.

But there's always a third party, which is the state, who is in the middle of the contract in the sense that the state will police many contracts and decide whether the state likes the contract or not. And if the state doesn't like the contract, then the state won't enforce the contract. Or the state might actually punish you because of the contract.

So for example, the state cares about the kinds of contracts. You can have contracts for the sale of tables. You can't have contracts for the sale of people. But you can sell dogs for reasons I can't understand. But the point is we are deciding which type of things can be sold and which kind of things can't be sold.

The state cares about the effect of the contract. If the contract is to render your corporation vulnerable to bankruptcy, the state might have an interest in deciding whether that contract will be enforced or not or whether it'll be allowed or not, whether it's permissible under bankruptcy laws to engage in that contract because of the risk that it's going to create.

The state's going to care about the terms of the contract. So if you're selling your labor in a state with a minimum wage law, the state's going to care. Does the term that specifies your wage equal or exceed the minimum wage?

And states can obviously care-- the most important thing for the state is whether and how the state taxes the transaction in the contract. So when does it tax the transaction? What is the event that's going to manifest it?

And of course, the contract can try to play with that sort of deal with whether it will be taxed. And the state will care about how the contract deals with it.

OK. So the point is to fight against the first real bias that especially, let's say, tech people and maybe business tech people bring to the idea of contract law, which is that contracts are not about the state. They're about private parties.

That's not true. They're about private parties and the state. And the state is always going to be there.

Now, so if I say to you, I'm trying to sell my parents' house. I can't sell it. So if I say to you, I'll offer you $10,000 to anyone who will burn down my parents' house. You're trying to accept that contract. You're raising your hand, so you're trying to accept. I want to say officially it's a joke so nobody gets any uncertainty about this.

Now, you're going to ask a question, because I didn't want you to accept. Because if you accepted my offer, then that's it. I'm stuck. So now it's clear it's not really an offer, and I can ask you a question.

AUDIENCE: So you said contracts cannot be between two parties. They have to be between two parties and the state.

LARRY LESSIG: No. So let me say it more clearly. Contracts always have the state present, so it's always between two parties or three parties or four. So you and I enter into a contract. Not this one, but another one.

But the state is in the room and deciding whether the state's going to allow the contract to happen. So most contracts, the state doesn't care about. But some contracts, the state's going to say, hell no, we're not going to allow it, like this one.

If you didn't get that notice it was a joke and you thought I was serious and you went and you burned down my parents' house so that we could get the insurance and not have to worry about selling the house, and then you came to me, and you said, OK, pay the $10,000. And I said, it was an obvious joke. And you went to a court, and you said, force Lessig to pay the $10,000. The court will say this is an illegal contract. I'm not going to enforce this contract.

So my point is the state, in a certain sense, is the censor of this contract. The state is in the room when we make this contract. And the state's judgment about it will decide whether we enforce it or not. Is that clearer?

AUDIENCE: So you're not saying the state has to be there.

LARRY LESSIG: I'm not saying the state is technically signing the document. But I'm getting you to recognize the fact that the contract is valuable to the extent it's enforceable. And the state is the essential agent in enforcement in the real world.

AUDIENCE: So I guess that's my question, because it seems like nowadays, we can have contracts where the enforcement is not the state. I can put a contract out there that says, hey, if you can factor this number, give me the prime factors of it, I'll give you 10 Ether.

LARRY LESSIG: Yeah. And what I started with when I was showing you this picture was to say, actually, that's been true for a while, right? So in what sense is the state here?

Well, the state is here if when you put the dime in and you get the drink out and the drink doesn't have Dr. Pepper but it has gasoline in it, the state would come in and say, whoa, wait. You've breached the implied term that said that this was safe to consume.

So the state is in this contract, too. And so what I'm trying to lead to or get to the place where we say, is there ever a place where the state is not there, which is what I think your blockchain-like invocation is. So that's a question we're going to get to in a second.

Here's another contract. We'll offer you $50,000 to lobby Congress to pass HR102. This contract looks pretty normal to us. You can imagine lobbyists have a contract like this all the time.

In fact, in the middle of the 19th century, the Supreme Court ruled this contract was an illegal contract. You weren't allowed to hire people to lobby Congress, right? So again, the background norm of what is appropriate or not for the contract controlled what type of contracting was allowed.

OK. So that's about the type of contract. But then think about the terms of the contract. And so now, I want to get you to recognize the way in which the terms that the law wants a contract to have can be defeated or not by technology.

And the way I'm going to get you to think about that is to think about not contract law but something that will create the intuitions I want you to have. Think about copyright law. Everybody knows copyright law, right? I hope you know something about copyright law.

So copyright law is a basic contract with the state. But the state says, if you create something, then you're going to get an exclusive right to it or exclusive rights, a set of rights-- an inclusive right to copy, an exclusive right to sell it, exclusive right to make derivative works of it-- for a period of time-- and in America right now, that's your life plus 70 years-- subject to fair use, meaning the law says you can't control every use of my copyrighted work.

If you want to take a book of mine and quote a section and write a review that says, see how idiotic Lessig is? You can do that. And I can't wrap the book in a contract that says you're not allowed to quote it for purposes of criticizing. I'm just not allowed to do that.

So copyright law, imagine this bundle of rights that it was offering. But now imagine something called DRM, Digital Rights Management. All right. So DRM is a set of code that we can wrap copyrighted material in in the process of making it available to others across networks and whatever else.

It's pretty trivial to see the way DRM could, in effect, destroy the limitations on the term. You can wrap it, encrypt it, make it so that my ability to control it will be my ability to control it, conceivably, as long as machines are running. If it's a Microsoft-based system, four years later, it won't be workable. But the point is, in principle, it could be forever.

Same thing with fair use. You can imagine it being wrapped in a way that disables the capacity to engage in fair use.

So I make tons of presentations all the time where I need to capture video. And I was astonished to discover the latest round of this operating system basically makes it incredibly difficult to rip video for the purpose of capturing even two seconds of it.

So if you have a video program that is capturing your screen, this operating system will now disable it for any period of time that you're trying to capture the screen. They've built the technology so that, now, there is no capacity, technical capacity, to engage in fair use of copyrighted material on the Apple platform.

Now, you might say, why should they be allowed to do that if the law intended that the contract gives you the free use of fair use? Why should they be allowed to do that? But that's the battle that's been going on about DRM ever since the beginning of the beginning of copyrighted work on the internet.

So my point is to get you to realize the way the code becomes part of the law of this contract. And you have to ask yourself the question whether that law is respecting the law of the sovereign, the law of the jurisdiction.

So when Apple and Disney get together and they sell this technology and they sell movies across the iTunes platform that make it practically impossible-- there's not even code. I mean, if you go out there and you look, you can find everybody who says, yeah, with this version, nobody's yet found a way to break it.

So right now, we're in a world where, right now, it's not possible for me to capture three seconds to put into a presentation. And the issue that raises is, to what extent is that consistent with copyright law if the technology now disables you from doing exactly what copyright law wants?

So this is the trade-off to think about, the relationship between the policy that the law wants and the policy of the technology. And there's no reason to believe the policy of the technology will always be consistent with the law. And to the extent it's not consistent with the law, it challenges the law. It says to the law, OK, come out and get me.

Now, that obviously is implicated in the context of smart contracts, because the biggest fear about smart contracts is that they enable a kind of transaction that can hide from the policy of the law. So the question for the law is, what will you do to step in? And this is, I think, where your question was going. How does the state appear in the middle of that contract?

But let's take one more step before we get to that. OK. That's the second point. Here's the third point.

There's often this intuition that, especially technologists, people have about what the particular aim of contract law is. So in the very beginning of me writing about the law of cyberspace, somebody from MIT-- I won't name any names-- it wasn't Andy-- showed up at the Harvard Law School and said, I've solved the problem of contract law.

I said, what do you mean? He said, I have a system that will eliminate risks in contracts. And he was really disappointed when I said, you know, the objective of contract law is not to eliminate risks. The objective of contract law is just to allocate risk, to figure out who has the risk, so each of us can figure out what to do in light of the risk.

So if I say I will buy 10,000 bushels of corn from you at $350 a bushel-- turns out that is the price of corn right now. He always looks up things on the internet. I figure I should look it up before I present it. So $350 is the price of a bushel of corn right now delivered September 1.

What that's basically doing is it's allocating the risk of the price of corn. So if you're a farmer and you don't want to face the risk the price of corn is going to fall to $3, you enter into this contract. If you're a buyer, you accept this contract. But if the price of corn falls to $3, well, you're out of luck.

So the point is it relocates the price change, reallocates the risk of price change, also reallocates the risk of delivery. So if I've got all this corn, I can place it in a certain place to shift the risk of delivery so that, once again, I use the contract to shift my risk of storage or my risk of delivery and you on the other side. So the objective of contract law, number one, is risk allocation. Number one.

But allocation matters only if-- trying to say only if for me-- only if there is a system to process the breach of a contract, only if you've got a technology, let's say, for processing the breach. So if I have a contract with you-- 10,000 bushels of corn, $3.50, on September 1-- and you don't deliver, that's a breach.

My risk has only been reallocated if there's some way for me to enforce the contract at that point. So it requires the system. And the system we ordinarily take for granted is a legal system.

And I say we take it for granted, meaning some people can take it for granted, like people in well-developed legal contexts. But that's also to emphasized other people can't take it for granted-- so for example, people in developing worlds. They can't take the legal system for granted. They can't assume that if the contract is breached, they go into a court and say, enforce the contract or give me damages. Or if you've got a contract between somebody in Rwanda and somebody in Alaska, then there, too, there's a question of whether we've got sufficient infrastructure to develop.

So the point I want to emphasize at the end of this little intervention is to suggest that this fact that it takes for granted the system of enforcement shows the real potential benefit of this class of contracting devices. Because if we think about this as a representation of a well-developed legal system and we think of first-world countries as having those and we compare third-world or developing world countries, which don't have these well-developed legal systems, you might say that first-world countries are better off relative to third-world countries, because they have the legal infrastructure to enable this risk allocation that will enable all sorts of market transactions to happen which otherwise wouldn't happen.

But if we imagine infrastructure like blockchain-like infrastructures or Ethereum infrastructures to enter the mix, providing a technical infrastructure that doesn't require judges and lawyers but just requires code, then that can substitute for the legal infrastructure, provide the infrastructure the contract needs at a much lower cost, and thereby enable people to contract who otherwise wouldn't rationally contract, because they could never count on the infrastructure of the legal system to deliver what they need. OK. So the point is this picture is trying to say that one key value of these technologies is that they will be a substitute for a failed legal system or a legal system that's not yet developed. They will provide the infrastructure of a legal system or the legal systems.

AUDIENCE: How can they really do anything? Because you can't make that contract like, I will pay you $3.50 per bushel on September 1 in Ethereum, because you're making a statement about the real world. The Ethereum blockchain cannot verify that I gave you the bushels.

LARRY LESSIG: OK. So I've got two slides to get to your example [INAUDIBLE]. OK.

AUDIENCE: There's ways to do it, but they're very risky, I should say.

LARRY LESSIG: Right. But let's bracket it for just-- I'm not sure if it's two, but it's n slides. But n is less than 100, I promise. So just hold one second, OK?

So if you say that one function here is to substitute for a failed legal system, that suggests that the other key opportunity here is to enable contracts where the transaction costs right now are otherwise too high. So this is a key opportunity to think of places where if you can lower the transaction costs of the contract, you will enable a contract which otherwise can't exist right now.

So I'm on a scientific board for an insurance company. So I was meeting the president last week. And he was all excited about a new product which they were investing in, which was going to provide flight delay insurance. And this product was going to be completely blockchain driven.

And this is what I'm trying to get to your point. It would trigger payments in a completely automatic way based on the information that's being reported from the n different sites that are reporting information about flights.

So I buy the contract. It says, if my flight is delayed more than an hour, I get paid $200. And automatically, as he put it, it's a no-touch product, by which he meant no human needs to touch this product for this contract to be enabled. It's a kind of product that never would have been available before, because the transaction costs of engaging it were way too high.

But now that we've lowered the transaction cost and have an infrastructure of trust, which is what the blockchain is providing here, there's a huge market that now is available for a contract that otherwise just wasn't there before. Now, that market depends on making a couple assumptions. You're not saying that there's 100% certainty that everything in that market is working the way it's supposed to work.

But the point is you don't need 100% certainty for the vast majority of these kinds of contracts. If it gets it wrong every once in a while, that's good enough for government work or good enough for airplane work. And so that's going to be sufficient to enable the market, recognizing that even in the legal system market, guess what? It doesn't always get it right either.

But it doesn't always enforce the contract well either. In fact, the costs are much, much higher to fail in the legal system. OK.

So two kinds of transaction costs. One system transaction cost suggests that where you have less developed legal systems, the blockchain is going to provide a real opportunity, because you're going to lower the transaction costs for those systems. And the other is just contract transaction costs. There'll be a huge explosion of markets where, right now, the contract transaction costs are so high, and we can lower them and thereby enable a certain kind of transaction that otherwise wouldn't be there.

OK. Final point I want to make. The other thing technologists always love to say is the great thing we will do when we do contract technology is they'll solve the clarity problem. Every term will be perfectly clear. Because you write those contracts out, and there's all sorts of ambiguity and vagueness, and it's a total mess. But when we've coded all of our contracts, our smart contracts, then we'll have perfect certainty for every single outcome, and that will be great.

And the point I want to suggest to you is that, often, obscurity is a real value. Obscurity is what you want, because here's a way to see it. So imagine this is a decision tree. And it's really small, because I just stole it from the internet. And it doesn't have anything to do really with what I'm talking about here.

But imagine a really complicated decision tree like this, which is to represent all the possible things that could happen with our deal. So I want to buy the house. But what happens if the house gets hit by a meteor? Or what happens if you go bankrupt? All of these possible outcomes.

And in principle, we could say we should be negotiating every one of these blue dots. We should be saying, what happens if this happens? OK, then this is what you get, and this is what I get. What happens if that happens? What you get, what I get. OK.

So imagine this blue dot here has a 0.002% chance of happening. So you know the chance of that happening is practically zero. And so what's the reasonable amount of time you should spend negotiating that term? Zero, right?

Especially because if this term is something you know he's really worked up about and you could never come to an agreement about that term, it would be ridiculous that the whole contract fall apart because of this 0.002% possibility. So what contracts do all the time is they create these fuzzy or vague or ambiguous places as a gamble.

It's like, OK, we'll go forward. We're going to just gamble that this 0.002% outcome won't happen. Most of the time, in fact, you can work out how often it doesn't happen, right? So most of the time, that would be just fine.

And if it turns out to happen, then what we'll do is ask somebody-- namely, a judge-- to figure that term out. We'll say, what should that term be interpreted as? It was ambiguous, so what should the answer be? And the judge will look at it. And judge will say, well, it's fair that you win or he wins.

So the point is there are many times when you ask the question, should you negotiate a term ex ante? And the answer to that question is no. And in those contexts, an ambiguity is a way to negotiate it ex post, meaning after the fact, ex post, by using the court.

So as we think about these digital smart contracts, this is why smart contracts are referred to as dumb contracts. They're smart contracts for the equivalent of dropping a dime in and getting a Dr. Pepper, the sorts of things where the possibilities are really small and narrow, or, like my CEO was really excited, is your plane late? Yes, I get $50. No, I don't. Things where it's relatively clear.

But there's a really important conceptual question about what happens when we're trying to use them for the kinds of contracts where what we want is ambiguity. Because if the very terms of deployment of the platform demand specifying all of the outcomes in this tree, then your basic thing is a whole bunch of contracts you're just not going to be able to have in this space, because the cost of specifying that tree will be higher than the benefit of those contracts.

So it's a weird sense in which, on the one hand, I've said to you that this technology can lower the transaction costs of contracts. But for this kind of contract, it can actually increase the transaction costs of contract. Because for this kind of contract, if it reveals the ambiguities we need to negotiate about and those negotiating ambiguities are just too costly for us to negotiate, then it's going to block us from having that contract. It forces us to see the 0.002%, and you and I have to come to terms on it.

And we don't yet have a good way to fake ambiguity. I mean, the legal system fakes ambiguity, because we just say, oh, yeah, yeah, we didn't see that. They saw it. He knew it when they wrote the contract. But they don't have to admit they knew it.

But the code has to admit it knows there's an ambiguity. And that's a hard thing to self consciously prevent.

OK. So I've given you four ideas. Happy to take questions or abuse. Usually, I get abuse from business school students, but OK.

AUDIENCE: So what if you can code into a contract the easy scenarios and then say else-if--

LARRY LESSIG: Go to court.

AUDIENCE: --go to court or some multinational court that is the Ethereum court or whatever.

LARRY LESSIG: Yeah. And even the Ethereum court will have to have a court above it if it wants to avoid government saying, if you have anything to do with Ethereum, we're going to punish you, right? So this is the sense of which I wanted to suggest, to go back to your first question, that if you think about it as layers of an onion, peel layers back enough, and you're going to, in the end, have to get to a state in some sense, a state as an enforceable mechanism.

And that enforceable mechanism doesn't have to be for every case. Again, 99% of the time, you drop the dime in, you get the Dr. Pepper. But there's a contingency where you drop the dime in, and out comes a bottle of gasoline. And then you need to go to somebody and say, you breached this contract. And that person--

AUDIENCE: But if it's a contract between somebody in Alaska and somebody in Rwanda, you still have the question of which state you go to. What's the jurisdiction? So I feel like there would have to be some extranational extra-state.

LARRY LESSIG: Yeah. So you will see in these types of contracts is there'll be a whole bunch of boilerplate that specifies choice of law, which turns out to be a relatively easy thing to do right now, choice of jurisdictions. For most countries, it's pretty easy. There are standard ways to do that. All of that will plug in automatically. But again, all of those are outside of the code. All of those are law.

AUDIENCE: Comment and a question. So I don't trust Vatalik or other software engineers that they have the legal understanding and capacity to write legally binding contracts. So I trust the government or I trust the court. I don't trust a software engineer to write a proper code to protect me or my counterparty. So what is your take on those smart contracts?

PROFESSOR: Can I add to that? Not only your take on whether to trust but what the courts in Europe and the US right now do if somebody says, I wrote the contract, and here's the code.

LARRY LESSIG: Well, so when you say-- let me just me understand the question better. I'm sorry. Your name is--

AUDIENCE: Hugo.

LARRY LESSIG: Hugo. The way Hugo described it, I think, is nice, with a whole bunch of conditional statements, which is the code. So the code says, if the plane leaves more than 30 minutes late, then transfer $100 to his account. So you don't trust Vatalik's system to be able to implement that conditional?

AUDIENCE: Yep. I don't understand-- I mean, I don't know the code. I don't know if it's breakable. I don't know if Jean can log in and change it.

LARRY LESSIG: I'm sure she can. But the point is, for most people, this is true of everything. When I say to you, I'm a lawyer, I'm going to write the contract so you can sell your car to Andy, you can have the same questions. You can have the question whether Andy is going to have a way to flip the price so instead of $10,000, it's 15,000.

So this uncertainty is everywhere. It might be Vatalik would say, actually, there's a more robust way to verify my code than Lessig's contract code. Because Lessig's contract code is written in English, and we have all sorts of-- but my code, you can have independent people who verify it.

So at the level of conditionals, I'm pretty confident. What I'm not confident about is-- and I had the great pleasure in December of 2015 spending a weekend with them, watching that group. And it's this weird kind of-- he is like the messiah figure, and there's 12 people sitting on the floor around him listening to his every bit of wisdom.

So it was inspirational and scary at the same time, because you see how much money is resting on this messiah's structure. But I have a lot of confidence in their ability to do the conditionals. But I'm not so confident that they yet thought through how it plugs into the bigger legal story.

And that's part of what I was trying to pitch to them, that's what I'm trying-- to him, and that's what I'm trying to pitch to you, that it's never going to be the case. I was at this conference in Australia where I met them. And so many of the people there were speaking the way people spoke about the internet 20 years ago.

It's like, oh, there's the real world. We have governments. But we're going to create-- like John Perry Barlow speak. We're going to create this virtual world where there is no governments, where we just live free of government.

And it's so fucking naive about the way this stuff works, because it's always embedded in a real world which has a real government. And that real government is not going to look the other way if you're doing lots of damage or not paying your taxes. So the question isn't whether. The question is just how and how much.

PROFESSOR: Can we go back there?

AUDIENCE: Yeah. So I have a question about, what kind of implications do you think this technology has to broaden access to legal services in general, like letting people know when they're being taken advantage or being able to provide more standard versions of really common contracts, like employment contracts or lease contacts and things like that? Do you think that this is going to be a game changer for those?

LARRY LESSIG: Absolutely. I mean, you've got to muster the political will to break the monopoly lawyers have in this space. And I'll tell you, we're going to fight hard against it. But there is no reason for 90% of what lawyers do to be done by lawyers.

Just like if you buy a house and you have to have a lawyer who sits there and basically signs documents for you. You're like, why? And the answer is because the law has been written to require that person to sit there and sign documents. And why? Because the people who get paid to sign documents have corrupted the law.

So there's lots to clean up. But if we can clean it up, absolutely. 99% of this stuff ought to be automatic. And then let's get the lawyers to focus on the hard corner cases, not on everything that should be automatic. And that certainly should be true not just within a jurisdiction but across jurisdiction.

AUDIENCE: Can I return to your insurance examples? I got the idea that you could write a smart contract that would pay you automatically if the plane was late. But then you said it puts it on a blockchain. Can you connect why he put it on the blockchain as opposed to just putting it on his disc and letting your credit card get credited? I mean, where did the blockchain enter into that? And why did he need a blockchain in order to maintain that statement?

LARRY LESSIG: I think that the thing that he thought he was getting out of the blockchain is to increase the verifiability of third parties of the actual payments according to the data. So if I say to you, I'm going to be paying you $500 if your plane is an hour late and we have the data out there about the planes being late, if he did it inside of his insurance company, I wouldn't have any way to know that he paid you $500 for the plane being late.

But if it's in a blockchain, there's at least conceptually a way in which we could be doing this-- not that I'm reviewing it to you, but we could be signaling--

AUDIENCE: That doesn't follow. So that depends on who maintains the blockchain. And then at the same time, it returns that. Suddenly, everybody knows the cash flow of that insurance company, which is likely not something he wants to do.

LARRY LESSIG: Well, the cash flow of the insurance company's bigger than authenticating the truth about certain types of contracts.

AUDIENCE: Well, let us know the cash flow of that part of the business. So I mean, he may not want that. I may not want everybody to know what planes I'm flying. So you've implied that there's now a public blockchain that does that to everyone to verify.

LARRY LESSIG: Yeah. All I mean to argue-- and I didn't interrogate him far. I was just taking his statement that he's doing. So I'm trying to think, why would he want to do it? Because I had the same kind of question you wanted to.

And it's just that if you are trying to create credibility around your claim-- but do I have a reason to trust this insurance company that, in fact, it's going to be doing this? Then there's some transparency that this enables-- not necessarily the transparency of your credit card number or your name or the flights that you're taking, but that there was somebody who was on this who had a contract, and we then made this kind of payment.

That would be a potential value that he has. Now, if there's no value from that, then you're right. The overhead of the blockchain or public or private or whatever is too high, and he just could do it inside.

And for certain companies, like if you went to a credible insurance company, the credible insurance company, you probably trust that credible insurance company. But again, if you're a not credible insurance company, if you're a startup and you are out there in the market and you're saying, give me your money and I'll pay you if the plane's late, people are going to say, why should I trust you?

And you're like, well, here. You don't really have to trust me. Here's the data. Here's the evidence in a more credible way than if I just published a report on my website that I'm doing what I say I'm doing.

PROFESSOR: Let's try to--

AUDIENCE: He has to escrow the $500.

PROFESSOR: Andy, let's try to get a couple more questions. But my hunch is that it's probably a permission rather than permissionless blockchain. And it may be the insurance company wants to ride on the buzz of blockchain. But it's possible, also, that he thinks that there'll be more trust, that consumers will trust that if it's called a blockchain.

But you did an interview. You can pick who you want to--

LARRY LESSIG: Right here.

AUDIENCE: So proof of performance, could this whole smart contract solve it? So for instance, some countries will receive-- and I was talking to Leonardo about it in Cargill, in his company. They deliver wheat to some countries. And proof of performance is always delayed. And hence, it becomes a private issue. So could smart contracts solve something like that?

LARRY LESSIG: Yeah. If you had an alternative way to credibly represent a fact-- and again, this is kind of connected to Andy's point. Is there an alternative way? And is this the alternative way?

Then you lower the transaction cost of that kind of contract, because I'm going to trust the contracting process more if I'm confident that, in fact, the fact that I'm not late doesn't penalize me, or you don't penalize me claiming I'm late. So to the extent you lower the cost of verifying facts in the world, you increase the opportunity for certain contracts to happen who otherwise wouldn't happen. And that's the only trade-off that I'm trying to emphasize by emphasizing the transaction cost part of these contracts. You had a question here?

AUDIENCE: Oh, yeah. I was just saying maybe one of the benefits of applying blockchain here would be not for one-off transactions but for the insurance company, perhaps, to have an aggregate thousands of transactions where they've shown performance. And they can use this for commercial reasons to show that, yes, people get paid when they purchase our insurance and get credibility for particular products.

LARRY LESSIG: Yeah. You would frame that as it would have to be that that would be a value it was providing. Otherwise, to Andy's point, there would be no reason to adopt this.

PROFESSOR: OK. Go on the back right. I don't remember your name

AUDIENCE: Kyle. So with, I guess, easier access to these derivative contracts, do you foresee a world where there's a lot more leverage in any type of market outside of financial markets? And do you foresee this creating kind of a risk in that way?

LARRY LESSIG: Well, I mean, this is your expertise, right? Because, I mean, we already saw in the derivatives market the fact that the choice by policymakers was to allow it to be an invisible market and not to regulate that market. It created all sorts of risks that sensible people might think shouldn't have been there.

And I think the same potential is here, which is, again, to come back to the point, don't expect there not to be government here. I mean, to the extent people realize this risk and don't have as much political corrupting power as Wall Street did in our system, we should expect governments [INAUDIBLE].

PROFESSOR: I would say yes. Even on bitcoin, you can create something called discrete log contracts to do contracts for differences or derivatives. But with smart contracts, you can put a lot of leverage into the system. And transactions can move quickly.

So I think the state will have an interest, particularly if it grows. We probably only have time for two more questions. And I'm still wondering, how do courts currently look at these as a matter of law?

In the late 1990s, I was honored to work with Senator John McCain on something which became the e-signature law. I was just playing point for the US Department of Treasury. It was really John McCain's law Congress was doing. But I'm wondering how the courts today would see these contracts. Do we need something like an e-signature law to have code accepted beyond what e-signature accepted?

LARRY LESSIG: No. I think the e-signature infrastructure is going to be 99% of what this system is.

PROFESSOR: You mean that which I worked on 20 years ago?

LARRY LESSIG: Yeah. You solved 99% of the problem.

PROFESSOR: Little did I know.

LARRY LESSIG: Here, too. Yeah. I mean, that's why I wanted to wrap this around the idea of a soda pop machine, right? So it's nothing new, in some sense. Contract law has always dealt with machines that are delivering on obligations.

It's just a more sophisticated set of proofs you're going to have to make in a court. But it's the same underlying plot.

PROFESSOR: One more question. We're MIT. We're supposed to end five minutes early.

LARRY LESSIG: Oh, OK.

PROFESSOR: I don't know what you do at Harvard.

LARRY LESSIG: I don't remember.

PROFESSOR: It's Harvard Law.

LARRY LESSIG: Right here.

AUDIENCE: So I have a little bit of the opposite question from Elon, which is a lot of the contracts you're talking about, simple contracts, right? You've got individuals on one side. You've got large companies, like your insurance company, on the other.

The insurance company can't, in fact, go through the entire decision tree and decide what every term is in their favor. And the law deals with that all the time.

But here, you have another problem, which is now, it's going to be OK. It's going to be written in computer code. How are the judges going to deal with that? Now it's a language that is going to be even tougher to deal with that problem.

LARRY LESSIG: Great question. And the answer is-- so this is actually another version of your question. The answer to that is nobody knows right now.

And so this issue gets raised in a lot of parallel contexts. For example, there's a Supreme Court Justice from California who's doing a lot of work about the question of black boxes that predict whether you are likely to commit a crime again. So if you're convicted of crime, the question is whether you're going to have parole. The parole process is supposed to decide your likelihood of committing a crime.

So these companies have built these black boxes where you spit in every bit of data. And it comes out and says yes, you're a criminal, or no, you're not. And then the lawyers come forward, and they say, well, I want to interrogate the black box. I want to know what--

And the courts are completely confused about this. Because on the one hand, they say, no, no, this is their trade secret. But on the other hand, they're like, wait a minute. You can't decide whether I have liberty or not based on these black boxes that just spit out numbers, right? So I've got to be able to interrogate them. Right.

So this is the most important innovation that's got to happen in the law. Lawyers have to become technically sophisticated to be able to read code like they read legal contracts. They have to have a conceptual understanding of what code can do so they can think creatively about code like they think creatively about language, right?

And one of the most important innovations that we, like the Berkman Center and people like that, are trying to push into the legal environment is to insist that just like lawyers now all study economics, because that's a core way of thinking about the law, we also should study basic code so we can think about this modality of regulation. Not expect people are going to be writing code, but at least that they can think through it.

So I completely agree. That's a fudge space that I didn't talk about at all. But I think it's a really important problem, thinking about whether the legal system is going to be able to deal with it. Because if none of the lawyers understand it, yeah.

Let me just end with one story about that. So when I first started doing this work, talking about code and-- I went to Paris 20 years ago, and I gave a speech to some lawyer group. And I sat down after the speech. And the chairman of this legal group sat down next to me.

And I introduced myself. And he stood up, and he grabbed my card. And he crushed it. And he threw it to the ground. And he said, I am not a technician.

And his point was he, as a lawyer, could never accept the idea that what he needed to understand was code. That was forbidden. It was beneath him.

And I think it's a hugely important cultural problem to integrate this form of knowledge. Because if we don't, then the problem you're talking about is really a huge problem. But I think we can, because we've seen lots of--

PROFESSOR: So I want to thank you on behalf of the class, Blockchain and Money.

[APPLAUSE]

I also want to say you're much better than Christopher Lloyd. And if anybody wants to know the joke, watch that *West Wing* episode that Christopher Lloyd plays Professor Lawrence Lessig. So thank you. See you on Thursday.