2025 Financial Stability Conference, Financial Stability in a Time of Rapid Economic and Technological Change

Panel Session: Technology

Host:
Peter Zimmerman, Federal Reserve Bank of Cleveland

Moderator:
Til Schuermann, Oliver Wyman

Panelists:
Hilary Allen, American University, Washington College of Law
Lewis Rinaudo Choen, Cahill, Gordon & Reindel LLP
Timthy Massad, Harvard Kennedy School

Peter Zimmerman:

If I could invite you to take your seats, please. Welcome back. Our final panel of the conference is going to be a discussion on the theme of technology moderated by Til Schuermann from Oliver Wyman.

Til Schuermann:

All right, thank you. Thanks so much for having us on this panel, for organizing this panel. And it is, in some sense, so well-placed after the papers that we saw this morning, as you'll see from the discussion. So the panel is about technology in the context of financial stability. We're going to pick up a lot of the themes that you've already heard about both yesterday and this morning, and hopefully shed a rich perspective that's additive to what you've already heard. We're going to go in alphabetical order. So let me introduce the panelists and after the introduction, each of them and each of us will give five, six minutes of overview introductory remarks on what they want to talk about. And then we'll start a discussion that will also hopefully involve all of you.

So, Hilary. Hilary is a professor of law at American University in Washington D.C. She's focused on financial stability regulation and on new financial technologies. Lewis Cohen is a partner at Cahill where he co-chairs their digital assets and emerging technology practice. He works on blockchain technology, crypto assets and tokenization across all aspects of capital markets. And then Tim Massad, to my immediate left, he served as chair of the CFTC under President Obama, prior to that as the assistant secretary for financial stability at the Treasury Department where he oversaw TARP. He is now at the Kennedy School at Harvard and spends his time working on financial regulation and FinTech issues. So with that, Hilary.

Hilary Allen:

Thank you. So at a conference like this, in a panel like this, I thought it would be helpful to go really big picture and talk about the political economy of Silicon Valley. Because what Silicon Valley does is it sells stories and dreams about the future and unfortunately in the last decade, the reality has not always

matched its stories. However, those stories have often succeeded as a smoke screen to hide the real innovation, which is finding a way around the rules that everyone else has to play by, in other words, regulatory arbitrage.

So I'm going to read you something from something I published over the summer called FinTech Dystopia, which I think describes a lot of what Silicon Valley does these days. First, develop a business model that centers a particular technology. Tell some stories about how that technology will solve a legitimate problem, preferably using the words democratize and disrupt. Bend or break some laws with that business model and profit from not complying with the law. Get away with bending or breaking the law and with harming people along the way because lawmakers and regulators are too timid to stop "innovation." Get big enough that you can convince lawmakers and regulators to change the law so that you never have to comply with it. And those who are harmed have no recourse because you haven't actually solved the problem and your business model isn't good enough to survive if you have to follow the same rules as everybody else.

So really that describes how the crypto industry works. We've all heard stories about how blockchains are decentralized and the crypto industry has been able to secure special regulatory treatment because of those stories, but those stories aren't true. A system can be technologically centralized, which is what blockchain is, but that does nothing to ensure economic decentralization. At every level of the crypto stack, whether it's the core software developers, the validators, the DAO operators, the stablecoin issuers, the oracles, the exchanges, you find significant concentrations of economic control. In other words, people acting as intermediaries.

But this blockchain technology creates real inefficiencies because of its technological decentralization. And so the industry is increasingly dispensing with blockchains wherever it can operating what we call off-chain. So those in the industry have a vested interest in repeating the blockchain-based decentralization narrative to avoid financial regulation, but it doesn't really bear out in reality.

Those in the AI industry have a vested interest in spinning narratives about super intelligence or the ability to achieve huge productivity gains in order to justify their noncompliance, in this case with environmental laws for data center construction and copyright laws. The industry concedes that having to comply with copyright laws would kill the industry.

So these narratives that the AI industry gives us, they oversell gen AI tools which have no actual intelligence, no ability to reason, they're statistical tools. LLMs predict the most statistically likely set of words that respond to a given prompt, but the response can be spectacularly wrong and/or entirely fabricated. One widely cited independent study from last year found that even the best models can generate hallucination free text only about 35% of the time. And many of us are familiar with the MIT report that said that enterprise adoption has resulted in 95% of the organizations getting no return on that. And this is the case at a time when the AI industry is burning through billions of dollars to subsidize the use of these tools, people aren't actually paying their true cost.

So why is this political economy relevant to financial stability? Well, most obviously if tech innovation is largely regulatory arbitrage, then FinTech is going to undermine financial stability regulation. Another thing to note is that Silicon Valley has kind of a conformist herd mentality that tends to produce bubbles. And Silicon Valley, no one there has any real incentive to prevent a financial crisis, and we see in fact that the AI industry is already happily angling for bailouts.

Venture capitalists benefit enormously from ZIRP, from prolonged periods of low interest rate environments because they attract a lot of investment as people seek yield. So they may not mind a financial crisis if they get ZIRP afterwards. There's also an exit mentality that is very common there. Basically you're looking for exponential growth and then out of there as a venture capitalist. I'll be gone, you'll be gone, we might remember from the 2008 financial crisis. That mentality is not compatible with stability.

And then it gets weird. In Silicon Valley there are a lot of ideologies that people ascribe to about the thing we need to focus on is whether our brains in jars can survive on Mars in a thousand years. If that's your focus, you're really not going to care about financial stability in the here and now. Then there's Silicon Valley's lack of expertise in finance. They move fast and break things. They don't bother to invest to learn why finance is the way it is. And that runs the risk of inserting a lot of new operational risks into our financial system too.

I think I've spoken too long, so I'll wait and talk later about the operational risk, but I'll hand on to my panelists.

Til Schuermann:

All right. Thank you, Hilary. We're off to the races. Lewis.

Lewis Cohen:

Well, thank you, Hilary. That's definitely a point of view. I'm reminded of the illustration of the old crone if you look at it one way and the lovely young lady, if you look at it another way.

Hilary Allen:

Who're you calling an old crone?

Lewis Cohen:

No, neither one, but that we can look at the same sets of facts and draw radically different conclusions, right? That is indeed the illustration. And I think that's good, and I said early to any number of people, I think it's very important to approach everything with a skeptical eye and that adds tremendous value.

The points, Til, that I want to touch on, and as you mentioned, I'm a practitioner, I'm a lawyer in this space. And given by my whatever hairs are left being gray, you can see I spent a lot of time working in the traditional financial markets and many of my clients are very traditional large investment banks, commercial banks, investment fund managers who very well understand not only the financial regulatory environment but the importance of meeting and complying with it both as a matter of principle in terms of supporting their overall approach and their investors' expectations, and also the value we all get in a society by having a compliant approach.

I had a call just this morning with a very large investment fund thinking about vaults that are used to deploy crypto assets across a wide range of DeFi protocols and we spent an hour talking about compliance issues and where the problems and concerns are. So certainly it's the case that the vast bulk of any market participants with whom I'm familiar pay close attention to these issues.

I think the points I want to talk about really are what does attract people to this? And one thesis is that, hey, there's just a lot of bad people out there who like telling stories and tricking people and running away and getting away with it. And for sure, those people are out there, undoubtedly. Does that really explain the widespread and global interest in these technologies. And ask yourselves those questions, I don't have the answer.

I can tell you though that the idea of automation through blockchain-based systems, whether they are decentralized or not, and I think we probably can have a good conversation about where decentralization applies and does not apply because I think you make some very valid points. But the idea of automation is something that is very, very attractive and interesting to a lot of people. And automation in financial systems means not working through traditional parties.

I think one of the things the crypto sector has done very poorly, I would say is attempt to demonize intermediation. And one of the main themes you'll see or you're undoubtedly aware of is boy, rent seeking intermediaries, how bad are they? And that's just silliness. As I point out to people, intermediaries that add value are service providers and they're people that we want. There's nothing wrong with intermediation.

I think where the concerns are and the complaints are, are intermediaries that work within heavily constrained boundaries that don't allow the maximum amount of competition, but nor do they deliver the kinds of promises of stability and protection that people are really aching for. And so they're open to exploring automated systems that work outside of those bounds.

I gave some folks yesterday, an example of something that I thought about. I was at a Best Buy store. And I was buying some large piece of equipment, 7, $800 and went up to the cash register. And what's the first thing they say to you when you go up to the cash register at a Best Buy? Would you like protection with that, sir? No. No, I would not like protection. I can evaluate the risk of owning this and I'm making the conclusion that 69.99 is not a great bargain for me. So, no, thank you.

What crypto allows is a financial environment in which an increasing number of people have the agency to go to the cashier at Best Buy and say, "No, I don't want to do that." And we can worry about whether these people are well-informed and how informed they are. But working against the general interests of the people I would say is very concerning and where we see these trends.

I also want to highlight briefly what I think is in many ways one of the most interesting aspects as a lawyer in these systems and that they're a-legal. They do not rely on the functioning of our existing legal system. And as someone who's been invested for now pushing 40 years of his professional career in the legal system, I'm fascinated by systems that are self-effectuating. I wouldn't call them automated and automated is not really the right term, but they're self-effectuating. And that is of tremendous interest to people. If you could lend money to folks, have all the commercial terms understood and agreed, and whatever the outcome is, it's deterministic and self-effectuated. That to me is a fascinating concept.

I'll leave you with my general plea as someone who endeavors to be about as down the middle as one can be, and that is this is a trend that is not going away. And as a result, and we saw in the prior administration, attempts to let's stamp that out, were actually counterproductive and in many ways hardened the system. I think trying to understand what the motivations are behind all those people that are holding Tether, that are dealing with DeFi and doing all these things and building a regulatory framework that adapts to them, that creates incentives for socially valuable behavior is the most important work that we can do over the coming years.

Til Schuermann:

Excellent. Thank you so much. Tim.

Lewis Cohen:

Good morning. Thank you first of all for inviting me here. I'm going to talk about stablecoins. We've had a lot of discussion about stablecoins. I'll try to be additive, not repetitive. But just by way of my background, I come at this from a regulatory standpoint, what should be the regulatory policy? And I've been in that space since 2014 effectively when as chair of the Commodity Futures Trading Commission, we declared Bitcoin a commodity. And I think the first time I testified on the weaknesses in our regulatory system, vis-a-vis digital assets, was 2014. Been talking about that ever since. We're finally getting around hopefully to fixing it. And I testified several times this year on both stablecoins and market structure.

On the GENIUS Act, my overall view is it could have been better. But we're still better off having passed it because I think it is better to bring this within a regulatory framework both to address the risks and to enable the private sector to develop the opportunities. Crypto market structure legislation I'm a bit more worried about, but we'll see if we get into that. So I'm not going to make any predictions about how big the market's going to be. I'm rather just going to list a number of things that I'm thinking about in the short term that will affect the regulation of this and the development of the market.

We're clearly in the implementation phase of the GENIUS Act and in particular, the capital and liquidity and risk management rules will be critical I think, to how banks think about their role in this space. Another very important issue in that implementation phase will be this question of payment of interest. The act prohibits stablecoin issuers from paying interest. Some of the bank organizations are pushing for a broader prohibition on other intermediaries from effectively paying interest and stablecoin issuers paying marketing incentives to firms like Coinbase and so forth, and then those firms paying interest. We'll see where that lands. I'm frankly skeptical that the OCC will prevent that. I think they may very well take a view that that's outside of our jurisdiction.

The issue of achieving a yield, of getting a yield on stablecoins is also important because of the fact that people who own stablecoins are lending them in various ways to facilitate other people's leveraged acquisitions of crypto. And I think that might be relevant to the discussion we had earlier of Rashad's paper, but we don't know how much activity there is in that regard because of the lack of transparency about leverage in the crypto market. But I think it's clearly relevant. There's a new paper that argues it's relevant to maintaining the peg on stablecoins. And the market structure debate will play into that in terms of the potential exceptions for DeFi protocols, which are one of the things that concern me.

Another issue in the implementation phase will be how federal regulators view state rules and foreign rules. Because of the way the GENIUS Act is set up, you can be licensed under a state regime. That's supposed to only be for small issuers, but at the very last minute of the development of the act, there was an additional provision that could allow states to continue to be the only supervisor of a larger state issuer.

And plus then on the foreign side, I believe the act at the end of the day kind of got to the right place, but it could have been a lot better. It's a bit murky on exactly what must a foreign issuer comply with. There's a reciprocity standard, there's a comparability standard. We'll have to see how that's interpreted. We should have done this very simply. We should have said, if you are going to issue a

dollar-backed stablecoin, you have to be registered in the US, you have to comply with our rules. We can argue about how we would've enforced that, but we should have at least set that as the standard.

In terms of use cases, we can have a long discussion about what those use cases are going to be. But a couple that I'm keeping my eye on is the use of stablecoins as collateral. ICE and CME, our derivatives exchanges have already said they're exploring taking stablecoins as collateral. The CFTC is working on that also. That could be a use case that grows very quickly. The use of stablecoins as the cash leg in repo transactions I think will also be something that we will see. The broader tokenization of stocks and bonds I think is a big use case that people see in the future. I think that may take a little bit more time before we see a lot of activity there.

And of course in terms of use cases, we'll have to see what banks do. Will they offer simply to manage stablecoin reserves, provide custody for their customers, or will banks get more aggressive? We're seeing, of course some banks like JP Morgan develop their own deposit tokens. We can get into a discussion of the difference between a deposit token and a stablecoin, but I think that will be important.

I want to say a couple words about redemption then of stablecoins because everybody thinks in terms of the reserves, which is important. But of course most stablecoin holders don't have a right to have their stablecoins redeemed. They must sell them in the secondary market. And you could have any number of things which cause people to perhaps be more concerned about the value of their stablecoins and create a spike in redemption requests, not just the value of the reserves, but an accounting problem with a stablecoin issuer, or a managerial problem, an operational problem. And not just with the stablecoin issuer, but with the blockchains on which the stablecoin is transferred. USDC is on 28 different blockchains.

And then when you think about that secondary market transaction to get out of a stablecoin, you have to think about the fragmentation of that liquidity across many different blockchains. You could have a problem on one blockchain that causes people to want to get out of their use of the stablecoin on that blockchain. And of course you've got a number of different exchanges where that redemption could take place.

And so I like to say stablecoins are very cool. We can transfer them in an instant. Redemption is a TradFi transaction. Even if I'm selling on a secondary market, someone somewhere is redeeming that stablecoin unless there's obviously great secondary market demand. How quickly can those treasury securities be liquidated? How quickly can the issuer get out of a repo? How quickly can it transfer the money? All those things will come into play.

And of course, layer on top of that, psychological factors of how people are perceiving that risk and whether they're getting more worried. Maybe it's a problem that's fairly isolated with a small stablecoin. But given the newness of all this, will people start to think, "Gee, I better get out of this stablecoin too"? We saw with Silicon Valley Bank of course, how quickly a run today can occur given social media, given the kinds of communications we have.

I want to say just a word about what I call national security risks, meaning not just AML, but preventing the financing of terrorism and our use of the financial system for sanctions. Stablecoins are, in my mind, a bearer instrument and we have an account-based financial system. And we've used that to achieve these objectives of AML, CFT and sanctions, meaning we rely on banks and other intermediaries to know who they're transacting with or to block someone's transactions or even block a financial institution from having access.

When we think about stablecoins and the ability to transfer those without going through an intermediary, that creates a whole new ballgame. And I don't think the GENIUS Act sufficiently addressed that. Yes, blockchain has advantages because we can see all the transactions, we can ring-fence someone if we know they're a bad actor, we can prevent them more easily, but I think we will need to develop new tools. Lots of discussion about that. The Treasury has a process going on for innovative techniques on that. And whether that's zero-knowledge proofs and digital identity or whether it's building compliance into the smart contracts or whether it's more aggressive monitoring that we would require of stablecoin issuers, I think all those things should be on the table. Let me stop there.

Til Schuermann:

Excellent. Thank you, Tim. So after two discussions on stablecoin, I'm going to focus my remarks on artificial intelligence, in particular, their use and adoption in banks. But I'm going to parse this through a very particular lens. I spend most of my time speaking to risk executives, particularly CROs of banks. And so a problem that I've been noodling on and working on with my clients is how to use AI for better risk management. And some of the themes that you have heard here will come through this.

And it's useful to start by just recognizing that the chief risk officer, a CRO's job has become ever more and more complicated, more complex. There's more risks. The world is becoming more complicated. Things are moving faster. So all of this falls on the plate of a CRO. And as a result, there's a very natural question that you would ask is with this new technology that is actually quite good at aggregating and dealing with a very wide range of information, how could we leverage that to improve risk management itself?

So I want to start with the narrower, perhaps more obvious applications and then get a little bit wider and perhaps a bit more creative. So very tangibly, where has AI already proven to be useful? So perhaps let's start with high-volume repeatable processes. For instance, transaction monitoring, like anti-money laundering, a lot of interesting work going on there. Improving the efficiency of the task and the effectiveness of the transactions monitoring itself.

KYC or know your customer during customer onboarding is another area. Here there is a bit of an arms race going on also. AI has proven to be useful to mimic and impersonate individuals, which makes the KYC process itself much more difficult. And so that you need here as in other places, AI to help you deal with the AI. And improving both just the effectiveness, the efficiency of the KYC process, but in the face of more creative counterparts, also upping the ante in this arms race.

Research and report writing intensive processes. So for example, in credit underwriting, there is a lot of research that happens in the credit underwriting and monitoring process. Reports get written left, right, and center. And this is another area where AI has already proven to be quite useful.

Any complex, manually intensive process like risk and control self-assessment, a tedious task, absolutely critical for running a bank, especially when there's plentiful data and very clear frameworks and RCSA is one good example.

Another one is evaluating control effectiveness where AI has already proven to be quite useful. So one way you can think about this is banks have this enormous control ecosystem that has grown up over decades. And if you were to look at it today, you would never build it the way that it is today. It just has grown up that way and it is often very complicated and a mess and full of redundancies and duplications

and controls that are no longer actually being used. And so, one really useful thing that you could do and have done is to let the AI loose on this ecosystem and come back with recommendations about how to get rid of redundancies, consolidate, automate, and so on.

And then the next step in evolution here would be something like a control co-pilot that some banks are already experimenting with. So I'm going to put on a new control and this co-pilot is going to help me both design it and make sure that it is not in conflict with or redundant of other controls that are already in place.

So where is this moving? It's moving increasingly towards semi-autonomous or agentic approaches. So for example, a credit agent that assists very actively in underwriting. All of this is going to make and has made the importance of governance and risk management of the AI itself increasingly important.

So let me now scope out just a little bit from, I've given you some examples of some very specific things that are being done. These are pretty increasingly widespread applications. Let's step back or a step forward perhaps a little bit about what else you could do. So let's come back to the recognition of that the CRO's job is just getting absurdly complicated and AI is really actually quite good in getting better at detection simply because it's scanning a very wide range of data. LLMs in particular are very good at summarizing and synthesizing. It's one of the things that we use them most, I certainly use them a lot for that.

So here's a problem, though. Information compression for a risk manager can be somewhat problematic because as a risk manager, you care not what is expected, you care about the unexpected, the surprises, the deviation from the expected. One person's outlier is another person's warning. And so in this way, LLMs suffer from a similar problem as any other statistical model, it re-reminded us that these are just statistical models, in that they are very happy in the dense part of the distribution and are slightly less happy and a little bit more fragile when you get to the edge of the distribution. Of course as a CRO, you're particularly interested in the edge of the distribution. So it's a little bit of a catch-22.

Now to be sure these models are getting better and better at all of this. And the fact that they are able to use such a wide range of data and information, and including not just numerical and text but also audio and video, they have an informational reach that is difficult for a human to duplicate. So having in this way a CRO assistant agent is not a silly idea at all. I'm not sure we're quite ready for Chat-CRO yet, but you could imagine that an AI agent is probably not going to be able to vote formally on a bank risk committee, but the agent could be integrated as an advisory member of the risk committee.

Let me stop there. Hopefully that has sparked some interest. Now I wanted to turn to some questions of our panelists. One of the prerogatives I get as the chair is I get to ask some questions before others do. And so I have a few. I actually wanted to go back to you, Hilary. You had sort of teased us by saying, "Oh, I want to talk about ops risk, but we ran out of time." So ops risk is very dear to my heart. I want to hear about ops risk.

Hilary Allen:

So all these new technologies bring with them new operational risks. So you actually started, there's a lot of new ops risks associated with AI, for example. And so AI tools are only ever as good as their data and actually I have a quibble with you that these tools are getting better. They can never get better than the data available to them. And when you're thinking about things like financial stability, we actually only have one market timeline when we're thinking about all the interactions of different institutions

and markets. And so I actually don't think we're even remotely in a big data situation when it comes to financial stability and figuring out where the risks are.

But the data also can be an attack vector. So there are new types of cybersecurity risks like data poisoning where people can actually poison the data in the models, and that's a way of attacking things. And another, while we're on the topic of cybersecurity, I think we really need to think a lot about what we're really doing by building the financial system on blockchains. Blockchains are so vulnerable to all kinds of cybersecurity problems. Most people don't anticipate this, but there are four or five individuals who are responsible for maintaining the Bitcoin blockchain and we don't really know who they are or who pays them. We're really going to build a financial system on this?

Ethereum is based on the Ethereum Foundation, but the Ethereum Foundation goes to great lengths to say, "Oh no, we're not actually responsible for the code. No, no, no, you can't come after this." Even though there was an article that came out recently where the Ethereum Foundation insider said, "Look, yeah, it's all just Vitalik Buterin." So he's not regulated, but he's like the one person we're depending on for the Ethereum blockchain. So if they make mistakes, there's holes, they're not regulated, they're not accountable, those holes can be exploited.

It's also true not just of the blockchains themselves, but the smart contracts. All this automation we're doing using smart contracts, they're all programmed by people too. And you know what? They often just cut and paste software from other places without really understanding it. And also increasingly, they're vibe coding. They're using AI to code and recent research shows that the AI-coded stuff has vulnerabilities in it like at least half the time.

There's a broader problem here, which is that financial stability regulators, financial regulators generally are used to dealing with the economics and then punting on the technology and just assuming that it will work the way they are told it's going to work. And we're getting to a point where that's not a tenable approach anymore. You cannot take industry claims about how this technology works at face value. There are so many operational vulnerabilities here and these operational vulnerabilities are not necessarily going to be idiosyncratic.

So something I've explored at my work is that we think of systemic risk as passing through credit channels. But it's quite possible that we could actually start seeing between different kinds of financial institutions, interoperability of financial systems being the vector through which a problem is transmitted from one financial institution to another. So as we have open banking pushes to link banks to FinTechs to banks to FinTechs, have we just created a through-line for an operational problem at one to go all the way through the chain? So I think these are real risks that we need to be focusing on.

Til Schuermann:

Thank you. Perhaps-

Lewis Cohen:

Just a couple of thoughts in response, Hilary, because kicking off with the idea of telling stories and then telling more stories, there's to my mind a little irony there. I think it's worth bearing in mind when you say, for example, the Bitcoin blockchain depends on four people.

Hilary Allen:

It was in the journal.

Lewis Cohen:

Well, then it must be true. The Bitcoin blockchain has a code base that's operated by tens of thousands of validators. Changes to that code base need to be adopted by those validators. The core developers can make suggestions and there is an elaborate process by which those suggestions are evaluated and considered. To do a hard fork or a foundational change requires a tremendous amount of work. I suspect you're very aware of this and it is just a stretch by the enormous measures, in fact, I would say a falsity to say there's four people that it depends on and likewise, other major chains like Ethereum. And people would not be putting trillions of dollars on something that is just about to tip over. It doesn't really make common sense. So I think it's important just when we talk about these things to have a fair understanding.

But are there ops risks? Yes, my goodness, there are ops risks all over the place and that is a very valid statement and they include some of the things, Hilary, that you've mentioned. I think the important thing I would assert as you go through this is not to imagine, well, I hope these blockchain systems go away and then the world would be a better place. It's rather how do we understand what those ops risks are and how are we evaluating them and how do we support the people that are trying to make sure that these systems work well through research development and investment? I think that's really the direction.

Tim Massad:

If I can weigh in? There's a little bit of truth in what they both said, right? Because there is a small group of programmers sitting at an office at MIT, but there also are tens of thousands of people who would have to validate what that change in code is.

I think one of the things that's interesting though about this space is the moves by some institutions to develop new blockchains which are more centralized, more permissioned, and we're seeing Circle has announced Arc, Stripe has announced Tempo. There are several others. And it's quite interesting, particularly because for so long, the blockchain crowd was very against the walled gardens of banks, we didn't want that. But now we are seeing these movements toward blockchains that maybe have centralized validators, a little bit more permissioning, a little bit more governance. And it will be very interesting to see how those evolve and where we land.

Lewis Cohen:

Just quickly, I want to add one thing because, Hilary, you didn't bring up the Godzilla of ops risks, which you should have, which I would support, and that is quantum. Blockchains have tremendous susceptibility. Blockchains are based on cryptography and the world of cryptography is in the process of dramatically changing, and I would absolutely hand to you that is a huge Godzilla ops risk. Now how is that going to play out? We don't know. Does it also affect traditional banking systems? But I just want to support that because it somehow got left out, but it is a very legitimate ops risk.

Til Schuermann:

That is indeed the Godzilla of ops risk in this space, absolutely. So actually, Lewis, I wanted to ask you a question and that is, you talked a lot about automation and the importance, proliferation of automation. I don't know if you mentioned smart contracts, but perhaps you were thinking about that also. So as a lawyer, you spend a lot of your time I think dealing with disputes and in that space there are no backsies. So how worried should we be about that? Is this a feature or is this a bug of smart contracts?

Lewis Cohen:

Indeed, I did not use the term, Til, smart contracts. At this point everyone has heard the aphorism, they're neither smart nor contracts. And indeed that's the case. I do think automation captures the concept better. It is code having been deployed to ideally a decentralized and neutral system. As you point out, Tim, not all blockchain systems are either decentralized or neutral. So it's a very valid point, but it is code that does that.

And you're right, Til, to say that for many of these systems there indeed are no backsies within the system. Some do have that, and I think again, Hilary, it'd be a valid criticism to say that there are undisclosed back doors in many smart contracts and that is a deeply concerning thing. There are a lot of concerns, but ultimately much of what is out there does work on a self-executing basis, the result of which cannot be returned.

I don't know that this is either a good or a bad thing. It's something that we must adapt risk parameters to. So there are many things that we do that having occurred, you cannot go back. That doesn't mean you shouldn't do them. You should understand and have processes, procedures and systems. And of course many large and regulated entities, BlackRock being at the top of the list, engage with permissionless blockchains all the time and have developed very effective tools to manage those risks. This does not mean that you cannot be careless or foolish and lose large sums of money, but last time I checked, you can be careless and foolish and lose lots of money in lots of different ways. So I think that's worth bearing in mind.

I think also in terms of what these systems are, and Tim, you bring up these other chains, what ultimately attracts people is the neutrality of the system. I think a concern about a bespoke stablecoin system that is to promote one particular provider's chain is it's not neutral. And I think ultimately capital loves neutrality. It loves fluidity, it's what brings capital into the space, but we have to watch this. This is an evolving area for sure.

Oh, I'm sorry, one last thing. I wanted to get the law in here. Just because you have no technological backsies, Til, it's very important to understand the legal system can provide recourse where someone who has exploited someone else can be identified. The case of Mango Markets, which was a DeFi system where there was an exploit by a guy named Avi, whatever his last name is, it'll come back to me. And he sought to assert a code as law kind of approach. He said, "Well, the system works this way and I'm going to exploit it." Ultimately, the judicial system is out on what exactly he did, but many people have been prosecuted for misleading others in the ways they use the code. So you may not have backsies on the code, but you may have recourse against people who exploit the code in ways that are deceptive or misleading.

Til Schuermann:

Thank you. Did you want to add something to that, Hilary?

Hilary Allen:

Yeah, I'd like to weigh in a little bit on the automation stuff. I'd also like to weigh in on the previous comment about all the nodes on Bitcoin and Ethereum watching what the core software developers are doing. Cybersecurity researchers have looked at this, some commissioned by DARPA even, and found that the vast majority of nodes don't participate and all kinds of bugs that have been put in there by the core software developers have gone undetected and sometimes been exploited. So it's an unrealistic expectation to think that all those nodes are really watching. Most of them are pretty passive participants.

So on automation more broadly, I mean this is the promise that we're getting in so many places from smart contracts to AI, et cetera. The idea is that this is always good, efficiency is where we're at. I think it's really interesting to think about this through the frame of complex systems because the financial system after all is a complex system and what you learn is that efficiency is a trade-off for robustness. There comes a point where you are undermining the fragility of the system.

And I think it's worth thinking about when do we get so efficient that it's actually counterproductive in terms of undermining the fragility of the system? And this is a question we started asking during the pandemic actually. The 2020 pandemic, supply contracts, is it better to start building at home even if it's less efficient so that it's more robust?

And with all this automation, we're getting rid of weekends, we're getting rid of after hours. Those were times that worked as a kind of circuit breaker. They were a pause. You could do an emergency rescue of a financial institution, you could shut down a bank, and we're getting rid of all of that. And I do wonder if we will come to regret not building in some pauses. And maybe, as we look at these new technologies, we need to think about different ways of creating circuit breakers.

So one of the things I suggested in my book Driverless Finance, which I published a few years ago, was maybe we need to have smart contracts consult an article maintained by the government or regulators that would basically tell smart contracts not to execute in certain situations to create a circuit breaker.

But I don't want to imply by that, that we always have to accept what's happening in technology as a framing thing. A lot of this conversation is like, "Well, this is happening and we just have to adapt and there's nothing we can do about it." That's a choice. Inevitability is a narrative that tech people love to use. Nothing is inevitable. If it was inevitable, they wouldn't be fighting so hard to get the legal changes that would give them the business model they wanted. If the law couldn't stop them, they wouldn't care. So I just want to put that out there as we think about this. Automation absolutely is happening. It's introducing new risks. It's not inevitable. Maybe we want it, maybe we don't.

Til Schuermann:

Thank you. Well, one thing that is inevitable is I'm going to ask Tim a question. So I want to actually come back to the paper that was right before the break, which among many other things reminded us that Treasury is really quite bullish about the size of the stablecoin market. I think 2 or 3 trillion are numbers that I've heard, and I think one of those was cited in the paper.

And with that coupled the empirical result that the beneficial yield impact was going to be something around ... I can't see the authors, but they'll correct me if I'm wrong. Oh, there you are ... 6 to 8 basis points. So that's not small, and I just wanted to get your thoughts on that. How realistic is this? How plausible? And maybe, what would we need to see have happened, believe in order for that to happen?

Tim Massad:

Well, yeah. I mean look, I think about this question of how big will the market grow in terms of the various use cases? And I don't have any brilliant way of forecasting that any more than any of you, but I like to sort of break down the use cases and really think them through. Today, stablecoins are used mostly for crypto trading. That's obviously going to continue. They're used somewhat for remittances. And I think in corridors where the conventional channels aren't very good, that's going to increase. They're increasingly being used by people in foreign countries that have weak currencies, weak financial systems. I think we'll see that grow.

But then you get into kind of the much bigger use cases of consumer payments and business-to-business payments, and I think that's the one that's much harder to predict. On the business payments, for example, there's a lot of reasons why you wouldn't want to use a stablecoin if you're the CFO or the treasurer of a company. I mean, there are certain risks in sending 50 million over Ethereum versus using CHIPS or versus using Fedwire. And do you really want instant settlement because maybe your entire systems are based on end of day settlement and instant settlement changes that a lot? You've got to think about liquidity to manage that.

Nevertheless, if you have some big players move into this space, Amazon and Walmart are making noises about having their own stablecoins, that could change things. Obviously Mastercard and Visa aren't sitting on their hands. They're very aggressively looking at this. And often when you talk to them, it's more about stablecoins will be the rails that people won't necessarily even know they're using. And I advised PayPal at one point and that's how they were thinking about it in part that, look, the technology is cheaper, it is faster, and maybe we'll just get to a point where it's providing some rails that we don't fully realize.

On the consumer side, I mean look, we all like our credit cards. They give us lots and lots of features that stablecoins do not give you and stablecoins today are clumsy to use. But again, if Starbucks starts taking stablecoins and Amazon has its own, we may see that change as well.

Lewis Cohen:

Or if you have a credit card that runs on stablecoins, right?

Tim Massad:

Or if you have a credit card ... Yeah.

Lewis Cohen:

The features are distinct from the rails, right?

Tim Massad:

Yes, they are. So I don't make predictions about market size. The secretary of the Treasury's forecast and the Citibank forecast, they're kind of in the same ballpark. We'll see.

Til Schuermann:

Thank you. Lewis, I wanted to ask you a question about GENIUS Act. And in particular as we move from statute to actual rulemaking, what are some of the things that you would especially watch out for, want to be considered also from a financial stability angle, but not only? Are there two or three things that you think are especially important to pay attention to?

Lewis Cohen:

Yeah, thank you. And I think in particular, Tim, you brought out some of those core points, but I'll maybe add some emphasis there. I think you're absolutely right, Tim, to call out the issue around redemption, the process of redemption and exactly how liquidity is going to be measured. The GENIUS Act somewhat punted that to rulemaking. It is a difficult question to say balancing the return versus pure available liquidity and what the demands are. They generally have not been very high for redemptions, but that changes under financial stress. And I think managing that and most importantly, giving the holders the confidence not to run because they believe that they will be able to exit if they need to. So how that works is going to be of course, particularly important.

I think it'll be interesting, you alluded to the state-federal dynamic. Our country has always been bounded by federalism and the idea of states as experimenters. It'll be very interesting to watch and see how that plays out. Some of the important proponents of the GENIUS Act, including Senator Lummis of Wyoming is a big proponent of the ability of states to innovate. So it'll be very interesting to see where that goes and how that plays out.

And I think also, Tim, you alluded to something I would call out as well, not just the idea of a foreign dollar-based stablecoin issuer, but there are many and growing numbers of non-dollar stablecoin issuers who can and will likely have an impact on our financial system as non-dollar, particularly the most major currencies, euros, yen, et cetera, increasingly other currencies are moved into the stablecoin framework and therefore tradable. And that is going to be interesting. The GENIUS Act is woefully lacking in how exactly we think. Are they completely illegal? Can they be allowed under certain circumstances? They obviously cannot have reserves and dollars because they're non-dollar stablecoins. So there are a lot of things that I'm watching to see how this will play out.

I'll just add quickly, Tim, I can just tell you from the practitioner's point of view that many large corporates are looking actively at stablecoins in their cross-border business. We are anticipating that to be a very significant trend, again, and I'm very happy to say wisely or foolishly, that they're looking at.

And then I'll add just one point of confluence everywhere. I'd still agree with you, Hilary, we'd share at least one bete noire. I do agree with you that it's ridiculous to see the crypto industry go whining to the government, the people that they were working against to say, "Oh, please, you must fix this to make our systems work." I would absolutely share that with you. I don't think the crypto industry needs or should be soliciting help from the government, but they do that and they didn't ask me.

Tim Massad:

If I can maybe add in. I agree with a lot of what Lewis has said. And on the state-federal issue, I certainly recognize the importance of the dual system, the importance of innovation at the state level. So I'm not against that. I think what concerns me though is that this whole sector is so new that you could have a small issuer at the state level under slightly different rules and something bad happened to that issuer, which makes people nervous more broadly about stablecoins. Just because we don't have enough experience with them, we're not yet at a place where we could say, "Oh yes, they're backed by the government in this way." Because they're not and does that affect the psychology of this whole market?

Til Schuermann:

Thank you. As you can tell, we could be talking about this for a long time, but I realize that we have just six, seven minutes left. So I would love to pass the microphone to Mr. Mark Carey.

Mark Carey:

Congratulations to Pete and Joe for another fantastic panel. Thank you all very much. I have two unrelated questions. My view and I think that of many in the financial stability community is that today, stablecoins, crypto, whatever, are not really a threat to financial stability because they are some combination of too small and too disconnected from the regular financial system. How do we know at least a few months in advance when it's getting connected enough and big enough to be a threat?

And then my unrelated question is, arms race, AI versus AI. Seems reasonable that sometimes the good guy's going to lose. How should the good guy set a threshold and say, "I lost." And what's the fallback positions? Because if you're trying to figure those things out in real time without any forethought, it seems to me the cost of losing is going to be much bigger. Are people thinking about that? Thank you.

Tim Massad:

I'll take the first one. Look, it would be great if we had those metrics and knew exactly, but we don't, you know that. There's no silver bullet here. And I'll answer it simply by when I was at treasury during the financial crisis, someone said, "Well, we spend a lot of time looking for financial instability. The problem is financial instability usually finds us." We're not going to know. We have to regulate this as it evolves. We're not going to know exactly what the use cases are to an earlier point that was made. We're not going to know how big it's going to become. And regulation is always catching up and that's the position we're going to be in.

I think a lot of it goes to, do we take steps to make this within the singleness of money? How do we think about its connections to fed settlement systems? And the skinny account proposal of Governor Waller, as was said, is only for eligible institutions, but some stablecoin issuers are seeking bank charters presumably in part to position themselves for that. Is that a good step? Do we want to see it evolve that way? I think those are the questions we're going to have to answer.

Hilary Allen:

If I might weigh in, I wonder if we might already be there. Crypto is still not big, but if you think about how leveraged our financial system is entirely, particularly outside, like in the non-bank financial sector, and you think about how much of it is tied together by narratives about technology. I mean the narratives around the AI and narratives around crypto, they're not that different. And what supports so

much of this sentiment driven stuff is the story. And if the story starts to collapse about both in a place where we have a highly leveraged financial system, to my mind it's a little bit of a tinderbox. So it's not to say that crypto in and of itself is too big and too interconnected, but just as part of the larger system that we're looking at, I'm already worried.

Lewis Cohen:

Yeah, no, I wouldn't say I'm necessarily already worried, but I think we are. It is the right time to be doing events like these where you're seeking to understand this. I think that's what you can do. And we sort of eluded, Tim, to your time at TARP. We managed to screw things up really well without any blockchain 20 years ago. It's not that. I think it's seeking understanding, listening to different voices. And doing what you're doing here is the best work that you can do.

Til Schuermann:

Arms race. So the arms race between the good guys and the bad guys is as old as banking, I would argue. So it's a very well-known issue and very much explored in fraud. Fraud actually, particularly credit card fraud was one of the early adopters of neural networks to try and detect in real time. So a couple of more specific reactions.

So first, whenever you implement a new system or upgrade an old one, there's a kind of red team, blue team approach that's done. So one party tries to break and the other party tries to build, and it's from the breaking that you learn how to improve better. So it is an incremental step towards staying ahead, but it's also a step towards understanding what the damage could be that you don't necessarily know ex-ante unless somebody more clever and perhaps more motivated than you achieves in breaking it.

Second is the pretty careful examination of false positives and false negatives. So misclassification costs are really asymmetric in this. For example, in know your customer, you would like to onboard really lucrative clients that are going to give you a lot of business. But if you're wrong about that client, it could also be really, really damaging because who knows who you onboarded and what their business is and where they got their funds and what they're going to do with their funds.

And so thinking very carefully about and modeling a little bit more formally, being a bit more formal about what those misclassification costs actually are, are also a little bit of a step further in perhaps staying ahead of the arms race. But there ain't no foolproof answer to this guy, this one. I see a negative sign in front of the timer here. So a very subtle way of saying-

Hilary Allen:

I think we're done.

Til Schuermann:

Let's thank the panel. And thank you all for participating. Who do I turn over ... Joe. Excellent.

Joseph Haubrich:

Just a few closing remarks as we conclude the conference. First, we'd really appreciate it if you could take a few moments to complete our survey and share your thoughts so we can improve this conference

for next year. On behalf of the Federal Reserve Bank of Cleveland, I and Pete would like to thank all our presenters for their valuable time, the excellent papers presented over the past two days and the fine discussions. We also want to thank our distinguished panelists and moderators for facilitating some great conversations as you just saw.

Special thanks to President Beth Hammack for opening the conference and to our keynotes, Professor Itay Goldstein and Vice Chair Philip Jefferson. We're grateful to you, the audience both here and online for attending and contributing many insightful questions. And I hope you had a lot of good conversations in the breaks.

With a high number of excellent paper submissions, Pete and I were supported by a dedicated team of paper reviewers as well as an outside scientific program committee. We had over 140 submissions and we had to narrow it down to six. From the Cleveland Fed, the reviewers were Paola Boel, Chengcheng Jia, Nick Fritsch, Lara Loewenstein, Tom Phelan, Ned Prescott, and Jan-Peter Siedlarek. Our outside scientific committee consisted of Will Cong, Victoria Ivashina, Pab Jotikasthira, Anton Korinek, Nag Prabhala, Gregory Nini, Gregory Udell, Anthony Lee Zhang, and Alex Zhou.

And that was in choosing the paper, but also there's a lot of behind the scenes work that a success of an event this size depends on the efforts of numerous individuals who are behind the scenes. So we really extend our gratitude to our conference and AV teams for their support. You can see the AV guys, give us a wave or something. Great. Great, thanks. And ensuring everything runs smoothly, Diona Roberts and the conference events team, Asher Rench and the AV team. Lastly, thanks to Diane Roberts, who I'm sure you've run into because she's been putting out fires all conference long for their crucial role in organizing the speakers and facilitating the smooth operation this year and the event year after year. We look forward to seeing you at next year's Financial Stability Conference. Thanks for your participation. We hope to see you next year.