Acting Comptroller of the Currency Michael J. Hsu
Remarks to the American Bankers Association (ABA) Risk and Compliance Conference
"Tokenization and AI in Banking:
How Risk and Compliance Can Facilitate Responsible Innovation"
June 16, 2023

Thank you for inviting me to the ABA's first combined Risk and Compliance Conference. It is an honor to be here as you call on your risk and compliance communities "to unite to protect banks from increasingly interconnected and complex threats." I applaud your effort to break down silos and approach things holistically.

Today, I would like to talk about a topic that badly needs such an approach: rapid innovation.

In particular, I would like to focus on two innovations that are evolving quickly and have the potential to be highly impactful on banking: tokenization and artificial intelligence (AI). The benefits of each are potentially quite significant, as are the risks—to consumers, to safety and soundness, and to financial stability.

There is a saying: The better a car's brakes, the faster you can drive it safely. In other words, strong controls *enable* sustained high performance. Too often risk and compliance are seen as nettlesome hindrances, roadblocks to getting to market, or drags on innovation and profitability. Some would say it is better to "move fast and break things," create "minimally viable products," "fail fast," and "rapid prototype" one's way to a market leading position.

In some domains, that approach can work. In banking and finance, however, it tends to end badly, as shown by the experience of the 2008 financial crisis with derivatives and last year's crypto winter.[1]

In banking, the *responsible* approach to innovation is the better way: by progressing in tightly controlled stages where the risks can be identified, measured, and managed at each stage, by building the brakes and the engine at the same time, and by working with regulators, instead of around them. This takes discipline and time. It requires engagement by, and trust in, risk managers and compliance professionals from the get-go through every step of the process. While this may slow things down initially, it helps to ensure that innovations *can be trusted* by the public and regulators to be safe, sound, and fair. In short, responsible innovation plays the long game. I want to discuss today how that approach can be adapted to today's fast-paced environment.

First, though, I want to spend some time talking about the promise and perils of tokenization and AI—two areas where the pace and scope of innovation present special challenges.

Tokenization

In order to discuss tokenization, I have to discuss crypto, as the underlying blockchain technology is where most tokenization efforts are currently focused.

[1] Regarding derivatives, refer to Gillian Tett, *Fool's Gold: The Inside Story of J.P. Morgan and How Wall Street Greed Corrupted Its Bold Dream and Created a Financial Catastrophe* (2010). Regarding crypto, refer to Mark, Julian and Gerrit De Vynck, "'Crypto winter' has come. And it's looking more like an ice age.," *Washington Post* (December 18, 2022). Refer also to remarks by Acting Comptroller Michael J. Hsu at the Blockchain Association, "Cryptocurrencies, Decentralized Finance, and Key Lessons from the 2008 Financial Crisis" (September 21, 2021).

I have long been a crypto skeptic.[2] The crypto industry remains immature and rife with risks, despite several years in the mainstream spotlight, billions of dollars of venture capital investment, and millions of hours of code commits. In 2022, losses from fraud exceeded $1 billion, losses from scams exceeded $2.5 billion, and losses from hacks exceeded $3.8 billion;[3] one of the largest stablecoins imploded; and multiple crypto platforms failed due to outright fraud, poor risk management, or both. In light of these risks, the OCC, Federal Reserve, and FDIC issued two interagency statements reminding banks of supervisory risk management expectations regarding crypto activities and exposures.[4]

Public blockchains, which support the vast majority of cryptocurrencies circulating today, appear to suffer from a key design flaw: "trustlessness."[5] The goal of having a "trustless" or "trust-minimized" blockchain requires a decentralized consensus mechanism, such as proof of work or proof of stake. These mechanisms are inefficient and create a trilemma between decentralization, security, and scale—achieving all three simultaneously is not possible with a

[2] Refer to remarks by Acting Comptroller of the Currency Michael J. Hsu to the Harvard Law School and Program on International Financial Systems Roundtable on Institutional Investors and Crypto Assets, "Don't Chase" (October 11, 2022).

[3] Refer to Federal Trade Commission, "New Analysis Finds Consumers Reported Losing More than $1 Billion in Cryptocurrency to Scams since 2021" (June 3, 2022); Department of Justice, Office of Public Affairs, "Justice Department Seizes Over $112M in Funds Linked to Cryptocurrency Investment Schemes" (April 3, 2023); and Chainalysis, "2022 Biggest Year Ever for Crypto Hacking with $3.8 Billion Stolen, Primarily from DeFi Protocols and by North Korea-linked Attackers" (February 1, 2023).

[4] OCC News Release 2023-18, "Agencies Issue Joint Statement on Liquidity Risks Resulting from Crypto-Asset Market Vulnerabilities" (February 23, 2023); OCC News Release 2023-1, "Agencies Issue Joint Statement on Crypto-Asset Risks to Banking Organizations" (January 3, 2023). Notably, cross contagion from crypto to the traditional banking system has been limited. The only bank failure attributable to the crypto winter has been that of Silvergate, a state-chartered bank, which self-liquidated in March 2023.

[5] Refer to Vitalik Buterin, "Trust Models" (August 20, 2020), in which he states that "[o]ne of the most valuable properties of many blockchain applications is *trustlessness*: the ability of the application to continue operating in an expected way without needing to rely on a specific actor to behave in a specific way even when their interests might change and push them to act in some different unexpected way in the future."

public blockchain.[6] To grow and manage the trilemma requires either ponzi-prone "tokenomics,"[7] highly technical workarounds,[8] or both. As a result, the crypto industry remains largely self-referential and disconnected from the real world. Moreover, the non-permissioned nature of public blockchains makes them attractive to criminals and others engaged in illicit finance,[9] and full compliance with anti-money laundering rules is extremely difficult for crypto intermediaries to achieve.[10]

By contrast, centrally operated, *trusted* blockchains have the potential to deliver security and achieve scale efficiently. Embracing the need to trust a blockchain operator—and forgoing trustlessness—eliminates the need for decentralized consensus mechanisms and the associated tokenomics. It enables the technology to solve settlement problems more efficiently and securely at scale, without the need for hype. Such "trusted blockchains" are also easily permissioned, making full compliance with AML rules achievable.

The greatest promise for blockchain technology today may lie in its potential to improve settlement efficiency through tokenization of real-world assets and liabilities on trusted blockchains. Settlement occurs when a transaction is deemed final. Typically, there is a lag between when the terms of a transaction, such as price and quantity, are agreed upon and when

---

[6] Vitalik Buterin, *Proof of Stake: The Making of Ethereum and the Philosophy of Blockchains* (2022).

[7] Vitalik Buterin, "The Revenue-Evil Curve: a different way to think about prioritizing public goods funding" (October 28, 2022).

[8] Bank for International Settlements (BIS), "Annual Economic Report" (June 2022). Refer to Vitalik Buterin, "Why sharding is great: demystifying the technical properties" (April 7, 2021).

[9] U.S Department of the Treasury, "Illicit Finance Risk Assessment of Decentralized Finance"(April 2023).

[10] Refer to OCC News Release 2022-41, "OCC Issues Consent Order Against Anchorage Digital Bank" (April 21, 2022); New York State Department of Financial Services, "Notice Regarding Paxos-Issued BUSD" (February 13, 2023).

all of the transaction components are performed, and obligations are fully discharged. That lag is due to the multiple entities and multiple steps that are typically needed for reconciliation and verification.

Tokenization of real-world assets and liabilities has the potential to improve settlement efficiency by minimizing those lags and thereby reducing the associated frictions, costs, and risks. For instance, if you want to sell shares of stock with today's technology, you have to send an instruction to a broker and then a whole host of other steps have to occur across multiple entities before that transaction is deemed final, usually two days later.[11] Each of those steps takes time and carries risk. With tokenization, the instruction, transaction, and settlement can theoretically be collapsed into a single step, removing those frictions—provided, of course, that the technology is interoperable with central bank money and real-world settlement systems.[12]

Some have estimated that tokenization of real-world assets could save 35 to 65 percent across the settlement value chain, including, for instance, cost savings of up to $5 billion for equity-post trading.[13] Tokenization of fiat currencies for cross-border payments also holds the promise of reducing frictions, costs, and delays.[14] Importantly, tokenization does not require

[11] Refer to Depository Trust & Clearing Corporation, "Guide to Clearance & Settlement."

[12] Organisation for Economic Co-operation and Development, "The Tokenisation of Assets and Potential Implications for Financial Markets" (January 17, 2020); Securities and Exchange Commission, Final Rule, "Shortening the Securities Transaction Settlement Cycle," 88 Fed. Reg. 13872 (March 6, 2023); BIS Bulletin 72, "The tokenization continuum" (April 11, 2023).

[13] Finoa, "Cost disruption in the issuance market: The case for tokenization" (October 2, 2020); Frederick Van Gysegem, "Tokenization: The future of financial markets?" (December 13, 2021).

[14] Refer to BIS, "Nexus: enabling instant cross-border payments" (March 23, 2023); Joint report by the BIS Committee on Payments and Market Infrastructures (CPMI), the BIS Innovation Hub, the International Monetary Fund (IMF), and the World Bank, "Exploring multilateral platforms for cross-border payments" (January 18, 2023); Federal Reserve Bank of New York, "Facilitating Wholesale Digital Asset Settlement" (discussing the Regulated Liability Network U.S. Proof of Concept); Hugh Son, "JP Morgan is rolling out the first US bank-backed cryptocurrency to transform payments business" (February 14, 2019).

decentralization and trustlessness. In fact, decentralization leads to fragmentation and imposes severe limitations on scalability. The Federal Reserve's Hamilton Project noted this in its Phase 1detailed report[15]—a finding that has been reinforced by national bank pilot projects that the OCC has reviewed as part of our supervisory process.[16]

Importantly, the legal frameworks—and risk and compliance capabilities—for tokenizing real-world assets and liabilities at scale need further development. Specifically, ownership and other property rights are not clear, especially in bankruptcy and in cross-jurisdictional situations.[17] Are tokens simply representations of real-world things, like a bank statement, or are they a distinct bundle of legal rights and obligations, like a deed? If the latter, how is ownership of a token established, recorded, transferred, perfected, contested, and resolved *in real-world legal systems*? What is the legal relationship between a owning a token and owning the underlying real-world asset or liability? How is that legal relationship enforced and how does it operate in bankruptcy? What is the process for un-tokenizing an asset or liability?

[15] Refer to Federal Reserve Bank of Boston, "Project Hamilton Phase 1 Executive Summary" (February 3, 2022).

[16] OCC Interpretive Letter No. 1179 (November 18, 2021) clarifies and elaborates on aspects of prior interpretive letters addressing cryptocurrency and trust activities and discusses that those activities are legally permissible provided the bank can demonstrate, to the satisfaction of its supervisory office, that it has controls in place to conduct the activity in a safe and sound manner. Specifically, a bank should notify its supervisory office, in writing, of its intention to engage in any of the cryptocurrency activities addressed in prior interpretive letters and should not engage in the activity until it receives written non-objection from its supervisory office. The supervisory office will evaluate the adequacy of a bank's risk management systems and controls, and risk measurement systems, to enable the bank to engage in the proposed activities in a safe and sound manner and in compliance with all applicable law.

[17] Refer to Uniform Law Commission, "2022 Amendments to the Uniform Commercial Code"; Juliet M. Moringiello and Christopher K. Odinet, "The Property Law of Tokens," 74 Florida Law Review 607 (2002); Law Commission, "Digital Assets."

Clarifying the ownership and other property rights of tokenized real-world assets and liabilities is foundational. It will inform the broader risks and associated risk management and controls needed to transact with tokens in a safe, sound, and fair manner.[18]

Programmability is an amplifier, further expanding the range of potential benefits and risks of tokenization. In theory, programmability could further reduce settlement frictions by making certain payments automatic when specific conditions are met. In the crypto space, these are referred to as "smart contracts." While the concept of smart contracts is fairly straightforward, there have been practical challenges with implementation, including with so-called oracles and coding vulnerabilities.[19]

In sum, to the extent settlement efficiencies can create real value for businesses, households, and financial institutions, demand to tokenize real world assets and liabilities is likely to grow over time. Today, trusted blockchains are better positioned than public blockchains to facilitate that growth at scale securely and in a safe, sound, and fair manner. In time, future innovations may reveal that non-blockchain-based systems may prove even better suited to the task. Regardless, the legal foundations for tokenization need to be developed. That will inform the controls and risk management capabilities required to support innovation in that space. Being attuned to the risks and building the brakes along with the engine will help ensure

[18] The American Law Institution and the Uniform Law Commission approved amendments to the Uniform Commercial Code (UCC) in 2022 to provide rules for the transfer of and security interests in certain digital assets. States have begun to adopt these changes. The UCC does not address ordinary ownership interests in digital assets, and many digital asset structures remain subject to significant legal uncertainty, including ownership interests. Refer to Uniform Law Commission, "2022 Amendments to the Uniform Commercial Code."

[19] Dylan Yaga, Peter Mell, Nik Roby, and Karen Scarfone, "Blockchain Technology Overview," National Institute of Standards and Technology Internal Report 8202 (October 2018).

that tokenization innovations can be sustained and trusted over time. I will come back to this after touching on AI.

Artificial Intelligence

To date, banks have generally approached machine learning and AI adoption cautiously. Use cases have ranged widely from customer chatbots to fraud detection to credit screening. Banks broadly have been attentive to the need for controls when using machine learning, including with regard to fair lending, compliance and adhering to model risk management practices.[20]

But the fear of missing out, especially regarding generative AI, may gain traction given the hype and breakneck pace of change. The buzz from OpenAI's release of ChatGPT last November went parabolic this spring with the leak of Meta's large language model, Google's release of Bard, and DIY releases like AutoGPT.[21] The market has taken notice, with "AI" mentions during second quarter earnings calls with investors nearly double the five-year average.[22] My own observation is that, for now at least, recent press reports of generative AI adoption by banks have been based more on speculative inference and, perhaps, attracting clicks than on reality.

[20] See OCC Comptroller's Handbook booklet "Model Risk Management" (August 2021); OCC Bulletin 2011-12, "Sound Practices for Model Risk Management: Supervisory Guidance on Model Risk Management" (April 4, 2011).

[21] Refer to Sawdah Bhaimiya, "ChatGPT may be the fastest-growing consumer app in internet history, reaching 100 million users in just over 2 months, UBS report says" (February 2, 2023); GPT-4 Technical Report, "Open AI" (March 27, 2023); Dylan Patel and Afzal Ahmad, "Google 'We Have No Moat, And Neither Does OpenAI'" (May 4, 2023); Bernard Marr, "Auto-GPT May Be The Strong AI Tool That Surpasses ChatGPT" (April 24, 2023).

[22] John Butters, "Highest Number of S&P 500 Companies Citing 'AI' on Q1 Earnings Calls in Over 10 Years" (May 26, 2023). Nearly one in five S&P 500 financial companies cited "AI."

For banking, the potential benefits of more widespread adoption of AI are significant, but so are the risks. The use of AI has the potential to reduce costs and increase efficiencies; improve products, services and performance; strengthen risk management and controls; and expand access to credit and other bank services. But AI also presents significant challenges.

Alignment is the core challenge. AI systems, which are generally based on neural networks, are not programmed explicitly like most software. They require training, and their outputs are not predictable.[23] While this is part of their magic, it also creates a fundamental problem: since AI systems are built to "learn," they may or may not do what we want or behave consistent with our values.[24] This alignment problem is inherent to all AI systems and is the focus of intense research.[25]

This alignment problem, in turn, creates a significant governance and accountability challenge. The more an AI system learns, the further it gets from its initial programming. This creates "opportunities for plausible deniability" should things go wrong.[26] In addition, like most companies, banks generally must rely on third parties to develop and support their AI capabilities. Within a bank and among its AI vendors, who is responsible for an AI system's performance and results? Who can and should be held accountable for misaligned, unexpected,

---

[23] OpenAI, "How should AI systems behave, and who should decide?" (February 16, 2023), notes that "the process is more similar to training a dog than to ordinary programming."

[24] Refer to Richard Ngo, Lawrence Chan, and Sören Mindermann, "The Alignment Problem from a Deep Learning Perspective" (February 22, 2023).

[25] Brian Christian, *The Alignment Problem: Machine Learning and Human Values* (2020); Jan Leike, John Schulman, and Jeffrey Wu, "Our approach to alignment research" (August 24, 2022); DeepMind, "Safety and Ethics." Refer to Defense Advanced Research Projects Agency, "In The Moment (ITM)" (March 14, 2022) (seeking proposals to enable trust in defense-related AI decision-making).

[26] Robin Feldman and Kara Stein, "AI Governance in the Financial Industry," Stanford Journal of Law, Business, and Finance Vol 27, No. 1 (posted October 10, 2022).

and harmful outcomes? To govern AI adoption and use AI prudently, banks need to be able to answer these questions clearly as the scope and complexity of their AI initiatives grow.

AI systems also present unique bias and discrimination challenges. The issue of biased training data is well known. (Google's early experience with automated photo captions unknowingly labeling pictures in highly inappropriate and racist ways in the early days of image recognition is a good reminder.) Bias challenges with supervised and reinforcement learning in the consumer lending context have also been flagged and are being discussed.[27]

Stepping back, though, a deeper fairness issue lurks. Even if an AI system could achieve complete color-blindness in decision-making at the individual level, it would still yield unfair outcomes at the group level if baselines across groups differ. The AI community has been grappling with this "impossibility theorem" for some time in the criminal justice context.[28] Banks and regulators should prepare for similar discussions as AI adoption among banks expands. The compounding nature of money, wealth, and financial health—and the impacts on mobility and persistent inequality—adds further complexity to this debate.[29]

Banks and regulators must also grapple with generative AI's capacity for enabling fraud and the spread of misinformation. Fraud has been increasing across all forms, from traditional

[27] Refer to Emily Flitter, *The White Wall: How Big Finance Bankrupts Black America* (2022).

[28] Jon Kleinberg, Sendhil Mullainathan, and Manish Raghavan, "Inherent Trade-Offs in the Fair Determination of Risk Scores" (November 17, 2016); Kailash Karthik Saravanakumar, "The impossibility theorem of machine fairness: a causal perspective" (January 29, 2021); Moritz Hardt, Eric Price, and Nathan Srebro, "Equality of Opportunity in Supervised Learning" (2016); Machines Gone Wrong, "Getting Started."

[29] Some AI researchers have begun to look to philosophy as a potential guide. See Laura Weidinger, Kevin R. McKee, Richard Everett, and Jason Gabriel, , "Using the Veil of Ignorance to align AI systems with principles of justice" (April 24, 2023); DeepMind, "How can we build human values into AI?" (April 24, 2023).

check fraud[30] to sophisticated synthetic identity[31] and synthetic media[32] fraud. The ability of AI agents to mimic human communication and the low cost of scaling AI agents increase opportunities for fraud. The speed and sophistication of such developments warrant close monitoring and coordination.[33]

In addition, the potential for AI and social media to facilitate the creation and dissemination of harmful misinformation is also concerning.[34] For instance, last month a fake Bloomberg Twitter account posted a fake picture of black smoke near the Pentagon, which was then shared by verified Twitter accounts, triggering a brief sell-off in equity markets.[35] Banks and regulators will need to update playbooks and strengthen defenses against such actions in the near future.

The value of a risk and compliance approach to rapid innovation

How should banks and regulators approach rapid, potentially transformative innovations like tokenization and AI prudently?

[30] Amy Besci, "Check Fraud Running Rampant" (March 2023).

[31] Tad Simons, "Trends in synthetic identify fraud" (April 21, 2023).

[32] Department of Homeland Security, "Increasing Threat of DeepFake Identities."

[33] William Dixon, "What is adversarial artificial intelligence and why does it matter?" (November 21, 2018); Marian Radu and Joel Spurlock, "CrowdStrike Advances the Use of AI to Predict Adversary Behavior and Significantly Improve Protection" (May 23, 2023); Consumer Financial Protection Bureau, "Chatbots in consumer finance" (June 6, 2023).

[34] Bradley Honigberg, "The Existential Threat of AI-Enhanced Disinformation Operations" (July 8, 2022); Karen Hao, "How Facebook and Google fund global misinformation" (November 20, 2021).

[35] Donie O'Sullivan and Jon Passantino, "'Verified' Twitter accounts share fake image of 'explosion' near Pentagon, causing confusion" (May 23, 2023).

It helps to bear in mind three principles: (1) innovate in stages, (2) build the brakes while building the engine, and (3) engage regulators early and often.

Innovating in stages requires discipline. The concept is simple: start with what can be controlled, expand only when ready, monitor carefully, adjust, and repeat. Fortunately, banks with robust new product approval processes are familiar with this approach. It is captured at a high level in the OCC's 2017 New, Modified, or Expanded Bank Products and Services guidance, which starts with adequate due diligence and approvals before commencing a new activity, and then touches on policies and procedures regarding risk identification and monitoring, effective change management, and ongoing performance monitoring and review systems.[36] Putting these principles into practice provides space for innovation to occur, but with guardrails and gates to prevent things from getting out of control.

To the extent a bank's innovation program involves algorithms or third-party vendors, the OCC's guidance on Model Risk Management and the recent interagency guidance on Third-Party Risk Management provide additional clarity on supervisory expectations, which should also help with promoting discipline and consistency in the face of rapid innovation.[37]

To build the brakes while building the engine, risk and compliance professionals need to be at the innovation table and have their voices heard. In the technology space, speed to market is an important factor in innovation. Slowing things down is seen as anti-innovative. Structurally

[36] OCC Bulletin 2017-43, "New, Modified, or Expanded Bank Products and Services: Risk Management Principles" (October 20, 2017).

[37] OCC Bulletin 2011-12, "Sound Practices for Model Risk Management: Supervisory Guidance on Model Risk Management" (April 4, 2011); OCC News Release 2023-53, "Agencies Issue Final Guidance on Third Party Risk Management" (June 6, 2023). Refer to OCC Comptroller's Handbook booklet "Model Risk Management" (August 2021).

and culturally, this casts the risk and compliance functions as barriers to innovation. In less regulated institutions, they tend to be ignored or pushed aside.

Those with experience know how this movie plot plays out in the banking space. A new product or service gets developed without any risk or compliance input. It launches and gains popularity. The bank becomes a leader. Problems appear. Financial, legal, and reputational costs mount. Finally, risk, compliance, and operations professionals are brought in to clean up the mess.

There is a better way: by giving risk and compliance professionals a seat at the innovation table from the get-go and heeding their input. Empowering them to identify risks and risk mitigants will help ensure that the products and services that result will be safe, sound, fair, *and trusted*. This is what supervisors and the public expect, and it makes good long-term business sense.

Asking for permission, not forgiveness, from regulators will help ensure the longevity of rapid and transformational innovations. The pressure to be a first mover and take advantage of network effects can incentivize firms to release first and engage with regulators later. This "ask for forgiveness" approach may work in certain technology contexts. But it doesn't work in banking and finance, where public trust is critical to long-term product success, and regulatory approval is a proxy for that trust.[38]

Regulators, of course, must be responsive, knowledgeable, and agile. This is why we recently expanded and upgraded our Office of Innovation to the Office of Financial Technology

[38] Refer to Bent Flyvbjerg and Dan Gardner, *How Big Things Get Done: The Surprising Factors That Determine the Fate of Every Project, from Home Renovations to Space Exploration and Everything In Between* (2023). The first product to hit the market is often not the one with staying power.

and hired a Chief Financial Technology Officer. Building a bigger and stronger team fluent in both financial technology and bank supervision will allow us to keep up with developments more easily, to engage banks and fintechs more actively, to educate examiners and policy staff more effectively, and to collaborate with peer agencies more regularly.

Conclusion

Rapid innovations like tokenization and AI present special opportunities, risks, and challenges for banks and regulators. While banks need to be adaptive and dynamic to thrive, they also need to safeguard trust by approaching innovation responsibly and purposefully. The risk and compliance professionals at banks—including all of you here today—play an invaluable role in making that a reality. And you do so not by simply saying yes or no to a new product or service but by developing the necessary expertise and bringing your experiences and perspectives to bear in rapidly changing environments.

The OCC recognizes that rapid innovations also require a more responsive approach by regulators. We are committed to being agile and credible on financial technology developments so that we can balance prudence with innovation and growth. Freezing the banking system in place is not an option nor is blindly embracing all innovation for innovation's sake. We must be able to navigate a more nuanced path, where responsible and purposeful innovations can be brought to market and a combination of controls, culture, and common sense can prevent irresponsible innovations from emerging.

Thank you again for inviting me to speak today. I look forward to engaging on these issues.