VIA REGULATIONS.GOV

August 9, 2024

Director Moses Kim, Office of Financial Institutions Policy
U.S. Department of Treasury
ATTN: Uses, Opportunities, and Risks of Artificial Intelligence in the Financial Services Sector
1500 Pennsylvania Avenue, NW
Washington, D.C. 20220

RE: Uses, Opportunities, and Risks of Artificial Intelligence in the Financial Services Sector (TREAS-DO-2024-0011)

Dear Sir or Madam:

The Crypto Council for Innovation ("CCI") appreciates the opportunity to submit comments on the U.S. Department of Treasury's Request for Information on Uses, Opportunities, and Risks of Artificial Intelligence in the Financial Services Sector ("RFI").

CCI is a global alliance of industry leaders in the digital assets space with a mission to communicate the benefits of digital assets and demonstrate their transformational promise. CCI members span the digital asset ecosystem and share the goal of encouraging the responsible global regulation of digital assets to unlock economic potential, improve lives, foster financial inclusion, protect national security, and disrupt illicit activity. CCI believes that achieving these goals requires informed, evidence-based policy decisions realized through collaborative engagement. To that end, CCI provides our comments and recommendations to the RFI.

Executive Summary

CCI's response to Treasury's RFI discusses the current and potential applications of AI in financial services, particularly within the digital assets space, while also addressing regulatory and compliance considerations. The response aims to highlight the potential of AI and blockchain technologies in transforming financial services, while promoting the responsible use of AI. Specifically, CCI's response elaborates on the following key themes:

1. **Use of AI in Financial Services:** Financial institutions, including digital asset firms, are employing AI for various purposes, such as enhancing products and services, risk management, capital markets, internal operations, and regulatory compliance. Furthermore, AI and blockchain technologies can complement one another, specifically in two main ways: (i) the use of AI to enhance blockchain-based services and (ii) the use of blockchain to address inefficiencies and risks within AI technologies.

2. **Risk Management and Compliance:** AI can play a critical role in managing risks in digital asset transactions by enhancing security, detecting fraud, and ensuring regulatory compliance, particularly with Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) standards.

3. **Challenges for Small Financial Institutions:** Smaller institutions face barriers to accessing AI due to limited resources and data availability, necessitating partnerships with other technology service providers to leverage AI effectively.

4. **Opportunities and Benefits:** AI can provide significant benefits, including improving service offerings, enhancing fraud detection, and increasing financial inclusion for underserved communities. It can also improve compliance with fair lending and consumer protection laws, particularly when blockchains are used to bolster AI models.

5. **Potential Risks and Risk Management:** There are various risks associated with AI, such as bias, data privacy issues, and the potential for fraud, especially with emerging AI technologies. It is crucial that AI models are explainable and transparent to ensure compliance and accountability.

6. **Regulatory and Supervisory Recommendations:** CCI emphasizes the need for responsible regulation that fosters innovation while managing risks. For guidance, U.S. regulators should evaluate the AI policy activity of other jurisdictions, such as the EU, and identify pathways for a risk-based approach to regulating AI.

A. General Use of AI in Financial Services

Question 2: **What types of AI models and tools are financial institutions using? To what extent and how do financial institutions expect to use AI in the provision of products and services, risk management, capital markets, internal operations, customer services, regulatory compliance, and marketing?**

Just as traditional financial institutions have begun to utilize AI to enhance their products and services, identify risks, and streamline operations, among other things, so too have digital asset firms. Many digital asset firms have already begun to explore the synergies between blockchain and AI, whereby one is deployed to enhance the other. The intersection between these two emerging technologies can be separated into two main categories: (i) AI for blockchain and (ii) blockchain for AI.

- "AI for blockchain" refers to the use of AI to enhance blockchain-based products and services, such as the use of AI to facilitate digital asset trading or identify potential threats to the security of blockchains.[1]
- "Blockchain for AI" refers to the use of blockchains or other distributed ledger technology ("DLT") to address inefficiencies and risks within AI-based tech, such as promoting the privacy and integrity of data inputs to large language models.

For purposes of Part A of the RFI, this comment letter will focus on "AI for blockchain" use cases as it more accurately addresses the question of how financial institutions (including digital asset firms) expect to use AI for a variety of reasons. Part B, which addresses the potential risks and opportunities associated with AI, will elaborate on "blockchain for AI," or the use of blockchain-based technologies to mitigate the risks and bolster the opportunities presented by AI.

a. Provision of Products and Services

Crypto firms have deployed AI to improve services and offerings. For instance, AI can be used to efficiently search and sort through on-chain data, which can then be used to create help tools for service providers and consumers alike, including data analytics boards, intent-based trading platforms,[2] and

[1] *See* Mohamed Baioumy and Alex Cheema, *AI x Crypto Primer*, https://alexcheema.github.io/AIxCryptoPrimer.pdf/.

[2] Intent-based trading allows a user to rely on a third-party, such as an AI bot, to execute intricate transactions on the user's behalf. This differs from the traditional trading in the digital asset space where a user must specify every detail of each transaction, such as the exact steps and parameters (e.g., "do A then B, pay exactly C to get X back"). Intent-based trading simplifies this process by allowing a user to simply tell the third-party the intended outcome and then rely on the sophisticated third-party to execute the details (e.g., "I want X and I'm willing to pay up to C"). *See An overview of intent-based architectures and applications in blockchain*, CoinTelegraph (Mar. 8, 2024), https://cointelegraph.com/learn/intent-based-architectures-and-applications-in-blockchain; Quintus Kilbourn, Georgios Konstantopoulos, *Intent-Based Architectures and Their Risks*, Paradigm (June 1, 2023), https://www.paradigm.xyz/2023/06/intents.

customizable bots for on-chain games.[3] AI can help to sift through, interpret, and generate actionable insights from vast amounts of information available on-chain. This, in turn, can be used to create useful dashboards for consumers.

- For example, Dune Analytics provides a powerful platform that allows users to query, analyze, and visualize data across more than thirty blockchains.[4] Such tools are useful for digital asset firms and consumers to better understand the types and quantities of activities that are happening on-chain.

b. Risk Management

AI can be used to help improve the security of blockchains. The immutable nature of digital asset transactions makes certain breaches and hacks on blockchain protocols irreversible. Accordingly, blockchain platforms and the smart contracts overlaying them need to be secured from the start. AI technologies can be deployed to stress test protocols and new solutions before they go live.

- Firms can deploy AI to analyze historical blockchain data and detect fraudulent activity, enhancing the security and reliability of digital payment systems. Companies like OpenZeppelin,[5] ChainPatrol[6], and CertiK[7], for example, have already begun to use AI in this way.
- Blockchain analytics firms utilize AI/ML for fraud and risk detection for on-chain activity, allowing platforms to flag and mitigate illicit activity.
    - One example is that of Dorsa, a blockchain security start-up, that uses AI models to audit and monitor smart contracts.[8] They have developed a variety of tools, including reinforcement learning agents to extensively test the security of a smart contract. The tools developed by Dorsa can help both developers and auditors to improve the security and the reliability of smart contracts.
        - While skilled human beings can already write secure smart contracts, this process is more efficient with AI.

c. Capital Markets

Cryptocurrency traders or high-frequency trading firms can use AI-based tools to more efficiently facilitate trading. Traders seeking to connect to an exchange's API can quickly generate testing scripts

[3] Mohamed Baioumy and Alex Cheema, *AI x Crypto Primer* (February 29, 2024), p. 8, https://alexcheema.github.io/AIxCryptoPrimer.pdf/
[4] Dune Analytics Documentation, https://docs.dune.com/home (last visited July 29, 2024).
[5] OpenZeppelin Documentation, https://docs.openzeppelin.com/ (last visited August 1, 2024).
[6] ChainPatrol Documentation, https://chainpatrol.io/docs/introduction (last visited August 1, 2024). *See also Maika Isogawa, Webacy Teams Up With ChainPatrol to Expand Ecosystem Coverage*, Webacy Blog (July 30, 2024), https://world.webacy.com/webacy-teams-up-with-chainpatrol-to-expand-ecosystem-coverage/.
[7] CertiK Blog, https://www.certik.com/resources (last visited August 1, 2024).
[8] Mohamed Baioumy and Alex Cheema, *AI x Crypto Primer*, https://alexcheema.github.io/AIxCryptoPrimer.pdf/.

before fully deploying the technology.[9] These scripts allow them to carry out technical tests that ensure they can connect to the exchange in a reliable manner.

d. Regulatory Compliance

In general, AI can assist in complying with AML/CFT regulatory requirements by automating the generation of reports and alerts. It can also help in interpreting large volumes of regulatory data to ensure that firms stay updated with the latest compliance standards. Additionally, AI-driven tools can facilitate more efficient communication between regulated entities and supervisory authorities.[10]

AI-based analytics tools can specifically aid digital asset firms in complying with AML/CFT requirements and standards by detecting activities and patterns that indicate illicit activity, and therefore allow firms to respond accordingly, all while bolstering a risk-based approach to AML/CFT compliance.

- For example, blockchain analysis firm Elliptic, in partnership with MIT-IBM Watson AI Lab, developed a novel AI-based technique to spot transactions made by ransomware groups and on darknet marketplaces.[11]
    - Elliptic worked with a crypto exchange operator to learn whether its technology could be useful in identifying money laundering, achieving positive results. Specifically, the technology identified numerous accounts that showed signs of probable money laundering activity and flagged them accordingly.
    - Rather than focusing on illicit wallets, the researchers trained their model on "subgraphs," which represent bitcoin transaction chains. Some of these transactions involved money laundering. By focusing on subgraphs rather than wallets, the model could analyze the broader "multi-hop" laundering process.
    - By scanning ledgers of transactions and data on wallets, machine learning can spot signs of illicit payments and help lead investigators to the actors behind them. According to Elliptic co-founder Tom Robinson, the ability to view past transactions on blockchains makes cryptocurrencies more amenable to AI-based financial crime detection than traditional financial assets.

***Question 4*: Are there challenges or barriers to access for small financial institutions seeking to use AI? If so, why are these barriers present? Do these barriers introduce risks for small financial institutions? If so, how do financial institutions expect to mitigate those risks?**

[9] *Id*. (Providing an explanation of a Perps AI, a firm that has developed a crypto trading network built on top of AI agents, which provides, among other things, AI generated trading recommendations.)
[10] FATF, *Opportunities and Challenges of New Technologies* for AML/CFT (July 2021), https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf.coredownload.pdf.
[11] Elliptic, *Our New Research: Enhancing Blockchain Analytics through AI* (May 1, 2024), https://www.elliptic.co/blog/our-new-research-enhancing-blockchain-analytics-through-ai.

In order for the broader financial sector to fully benefit from AI, smaller financial institutions will likely need to partner with third-party technology vendors and need the regulatory clarity that such partnerships done responsibly are encouraged; on the latter point, ambiguity regarding regulatory expectations can chill adoption of AI technologies and related partnerships As Treasury pointed out in its March 2024 report, "Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Services Sector,"[12] there is a widening gap between large and small financial institutions when it comes to in-house AI systems. Large institutions are developing their own AI systems, while smaller institutions may be unable to do so because they lack the internal data resources required to train large models. Additionally, financial institutions that have already migrated to the cloud may have an advantage when it comes to leveraging AI systems in a safe and secure manner.

Training AI systems, such as large language models, requires a significant amount of computing power and data. Right now, only the most well-resourced institutions can afford to maintain the servers needed to support the requisite level of compute power and access the necessary amount of data. Institutions can acquire large amounts of training data by paying to scrape it from the Internet or by accessing existing repositories of data gathered from the consumers of their products/services. These methods favor large, well-resourced institutions that can pay for troves of external data. However, it is important to note that such methods can also raise important consumer protection concerns because they force consumers to (often inadvertently) cede data to large institutions that neither have the consumers' best interests in mind, nor offer any compensation.

B. Actual and Potential Opportunities and Risks Related to Use of AI in Financial Services

a. <u>Actual and Potential Opportunities and Benefits</u>

***Question 5*: What are the actual and expected benefits from the use of AI to any of the following stakeholders: financial institutions, financial regulators, consumers, researchers, advocacy groups, or others? Please describe specific benefits with supporting data and examples. How has the use of AI provided specific benefits to low-to-moderate income consumers and/or underserved individuals and communities (e.g., communities of color, women, rural, tribal, or disadvantaged communities)?**

As described in Part A, AI aids digital asset firms in analyzing historical blockchain records. Not only is this useful for enhancing blockchain-based products and services themselves, but it is also an effective way to detect illicit activity and mitigate financial exclusion. AI-based analytics tools are useful for financial institutions more broadly because they can automatically monitor, process, and analyze transactions to detect suspicious activities in real-time. These technologies can help to distinguish illicit activities from normal transactions, reducing the need for initial human review and allowing for quicker responses to potential threats.[13]

---

[12] *Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Services Sector, U.S. Department of the Treasury* (March 2024), https://home.treasury.gov/system/files/136/Managing-Artificial-Intelligence-Specific-Cybersecurity-Risks-In-The-Financial-Services-Sector.pdf.

[13] FATF, *Opportunities and Challenges of New Technologies* for AML/CFT (July 2021), https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Opportunities-Challenges-of-New-Technologies-for-AML-

The use of AI to improve the detection of illicit activity will also prove beneficial to regulators. AI technologies can update risk models in real-time to account for new and emerging threats, ensuring that the AML/CFT measures are always current and effective. AI can further boost compliance with regulatory requirements by automating the generation of reports and alerts and interpreting large volumes of regulatory information to ensure that firms remain compliant with the most up-to-date standards.[14]

In terms of consumer benefits, AI tools can generate more accurate and comprehensive assessments of potential fraud or customer risk by continuously updating customer profiles with new data. This helps in better decision-making and can reduce instances of financial exclusion. AI can also categorize customers into risk levels during onboarding and monitor their activities for patterns that may indicate AML/CFT risks.[15]

AI can also improve the efficiency and accuracy of certain complex tasks, such as writing code. This is particularly important in the context of blockchain networks in which transactions are immutable and irreversible. Given the finality of blockchain transactions, it is important that the smart contracts—the programming commands that dictate the execution of transactions—be designed properly from the start, and without bugs that would make them vulnerable to attack. While high-quality manual coding is essential to achieving good outcomes in programming, AI has the potential to greatly improve this process, including through audit functions. Secure and properly functioning protocols, which rely on accurate code, are beneficial to digital asset firms and digital asset consumers alike.

How has AI been used in financial services to improve fair lending and consumer protection, including substantiating information? To what extent does AI improve the ability of financial institutions to comply with fair lending or other consumer protection laws and regulations? Please be as specific as possible, including details about cost savings, increased customer reach, expanded access to financial services, time horizon of savings, or other benefits after deploying AI.

Financial institutions can leverage AI to aid humans in making critical financial decisions such as assigning credit scores and issuing loans. In some cases, AI may be better suited to make these decisions because it can process more data at a quicker pace. However, like humans, AI can also demonstrate biases in its decision making if it is trained with faulty inputs. However, as we will discuss further under Question 7, there are technical solutions to manage the complications around biases.

It is also likely that digital asset consumers will increasingly rely on AI agents to make financial decisions for them, such as how and where to invest. Accordingly, it will be important that we can trust these AI agents. Here, the trustless nature of blockchain networks and the underlying technology of cryptography may prove useful.

CFT.pdf.coredownload.pdf; New York City Bar, Artificial Intelligence and Machine Learning in Financial Services (Mar. 11, 2024), https://www.nycbar.org/reports/artificial-intelligence-and-machine-learning-in-financial-services/.

[14] *Id.*

[15] *Id*.

- As noted in our response to Question 2, digital asset firms can deploy AI models in order to help consumers decide what trades to make. However, if these models are not run "on-chain," or via the smart contracts that secure and verify transactions on blockchains, then there is no way for the smart contracts to confirm the veracity of the models' results. In other words, if the AI model is not run on the same blockchain as the trades themselves, then consumers cannot be sure that the AI model has generated sound and reasonable trading recommendations.

- A proof of concept trading bot known as Rockfeller Bot, or "RockyBot" sought to resolve this problem by putting the AI model on-chain.[16] Specifically, by utilizing zero-knowledge proofs, RockyBot gave users confirmation that the AI model conveyed verifiable outputs because it allowed users to query the model on a transparent blockchain. This would not have been possible without the combination of AI and blockchain.

b. Actual and Potential Risks and Risk Management

i. Oversight of AI: Explainability and Bias

***Question 7*: How do financial institutions expect to apply risk management or other frameworks and guidance to the use of AI, and in particular, emerging AI technologies? Please describe the governance structure and risk management frameworks financial institutions expect to apply in connection with the development and deployment of AI. Please provide examples of policies and/or practices, to the extent applicable. What types of testing methods are financial institutions utilizing in connection with the development and deployment of AI models and tools? Please describe the testing purpose and the specific testing methods utilized, to the extent applicable. To what extent are financial institutions evaluating and addressing potential gaps in human capital to ensure that staff can effectively manage the development and validation practices of AI models and tools? What challenges exist for addressing risks related to AI explainability? What methodologies are being deployed to enhance explainability and protect against potential bias risk?**

Blockchain technology has the potential to enhance the testing and governance of AI models, thereby helping to mitigate risks related to AI explainability and accuracy.[17] For instance, data analytics firm FICO has used blockchain to assist in auditing AI training models.[18] The following are some of the various applications:

- **Immutable Record-Keeping:** Blockchain can be used to record all decisions and actions taken during AI model development, testing, and deployment. This includes documenting the model's objectives, design choices, algorithms used, and testing procedures.

- **Transparency and Auditability:** By recording all steps of the AI development process on a blockchain, organizations can provide a transparent and auditable trail of their model's creation

[16] RockyBoy Documentation, GitHub, https://github.com/Modulus-Labs/RockyBot (last visited July 29, 2024).
[17] Isabelle Bousquette, *AI Has a Trust Problem. Can Blockchain Help?*, Wall Street Journal (Jan. 11, 2024), https://www.wsj.com/articles/ai-has-a-trust-problem-can-blockchain-help-ba3b26f7.
[18] Scott Zoldi, *How to Use Blockchain to Build Responsible AI: An Award-Winning Approach*, FICO Blog (Oct. 17, 2023), https://www.fico.com/blogs/how-use-blockchain-build-responsible-ai-award-winning-approach-0.

and evolution. This allows for easier verification of compliance with ethical standards and regulatory requirements.

- **Accountability:** Blockchain can associate specific tasks and decisions with individual team members, creating clear lines of responsibility throughout the AI development lifecycle. This helps ensure that all participants are accountable for their contributions.
- **Enforcing Development Standards:** Organizations can use blockchain to codify and enforce their AI development standards, ensuring that all required steps, tests, and approvals are completed before a model is deployed.
- **Tracking Data Provenance:** Blockchain can be used to record the sources and lineage of training data, helping to ensure that only approved and ethically sourced data is used in model development.
- **Monitoring Model Performance:** Blockchain can be utilized to track and record a model's performance over time, including any deviations from expected behavior or potential biases that emerge.
- **Managing Model Updates:** Any changes or updates to the AI model can be recorded on the blockchain, providing a clear history of how the model has evolved and who authorized these changes.
- **Ethical AI Practices:** Blockchain can help enforce the implementation of ethical AI tests and procedures by making them an integral part of the development process that must be completed and recorded.
- **Latent Feature Monitoring:** Advanced blockchain-based governance systems can track the behavior of latent features within AI models, helping to detect unexpected changes or potentially problematic patterns.
- **Facilitating Regulatory Compliance:** By providing a comprehensive and tamper-proof record of an AI model's development and operation, blockchain can help organizations demonstrate compliance with emerging AI regulations and standards.

***Question 8*: What types of input data are financial institutions using for development of AI models and tools, particularly models and tools relying on emerging AI technologies? Please describe the data governance structure financial institutions expect to apply in confirming the quality and integrity of data. Are financial institutions using "non-traditional" forms of data? If so, what forms of "non-traditional" data are being used? Are financial institutions using alternative forms of data? If so, what forms of alternative data are being used?**

As discussed in Question 2, some projects combining DLT and AI are best categorized as "blockchain for AI," whereby blockchain serves to improve the internal processes for AI-based technologies. One challenge with AI models is that it is not always possible to tell what data were used to train a model,

even with access to model weights, since training models represent an amalgamation of training data. This introduces several challenges that do not exist in traditional software, including IP issues, lack of compensation for owners of data, the use of low-quality data, and the introduction of biases in models. As discussed in previous responses, blockchain technology has the potential to aid in verifying the authenticity and integrity of data used to train AI models (i.e., "Blockchain for AI").[19]

- **Integrity of Data Models/Model Training:** Blockchain can be used to develop solutions that help users and developers ensure that the data and models have not been modified without their knowledge.[20]
    - For example, an API-based service could allow data-owners and AI developers to record time-stamped hashes of datasets and models to ensure their integrity and log the entire process of model development and the datasets used to track the entire lifecycle, in a way that could be made available to third party auditors or regulators. The system could even be directly integrated into ML development tools. This could help improve the integrity and trustworthiness of models by making their development process more transparent and secure.
    - It may also be possible to log relevant proofs of the "unlearning" of particular data from models on-chain to demonstrate to the satisfaction of regulators that a certain provider's data have been removed from a given model.
    - Logging hashes for data and model outputs on-chain can also help to combat deepfakes.
        - For example, applications may be able to ensure the authenticity of the data used by checking digital signatures associated with the source of the data on-chain, or a decentralized version of "Snopes.com" could be designed and implemented on-chain to flag deepfakes.
- **Data and Model Rights Management:** A non-fungible token (NFT) can demonstrate one's ownership of any given digital content or data.[21]
    - Depending on the use case, the content in question could be a model input, such as a prompt to a Generative AI tool, data used to train a model, parameters of a model, or the output of a model.
    - The NFT would allow the user or developer to assert their ownership and further transfer ownership of the corresponding digital asset to another.
    - It may also be possible to develop blockchain-based access control mechanisms for data and models.

[19] Rajarshi Gupta and Vijay Dialani, *Blockchain for AI*, Coinbase Blog (Mar. 8, 2024), https://www.coinbase.com/blog/blockchain-for-ai.
[20] *Id*.
[21] *Id*.

- For example, a smart contract could allow or limit access based on a given list of user addresses.
- Alternatively, a mechanism integrated with a decentralized identity solution (possibly using cryptographic techniques such as zero-knowledge proofs) could allow access based on certain demonstrated attributes (e.g., age or geographic location) while preserving the privacy of the user.

- **Incentives and Payments for Data, Models, and Compute Resources:** By enabling a payment mechanism for participation in AI model training, blockchains can incentivize the sharing of high-quality data, among other things.[22]
  - Blockchain can facilitate low-fee micropayments for the use of a generative AI model using a stablecoin.
  - A smart contract could allow revenue sharing across multiple co-owners of a model in a decentralized fashion.
  - Blockchain-based co-ownership models may allow small to medium size model developers to join forces and compete against larger firms in the space.
  - Crypto rewards could also be used to incentivize data providers, data annotators, model developers or human feedback providers anywhere in the world to join a new decentralized project to develop a new generative AI model or solution, with appropriate mechanisms to track contributions so that incentives can be fairly allocated.
  - Blockchain could also be used to create a decentralized data/model/compute marketplace that makes it easy for compute providers, training data providers, model developers and users to search for and be matched to each other, to offer incentives, make payments, and enter into contracts and agreements.
  - A blockchain-based decentralized review system implemented using smart contracts could incorporate both automated and human-based reviewers in a system that incentivizes high throughput and thorough, high quality review of data and models.
- **Distributed Computing Resources:** Blockchain enables the creation of decentralized networks where computational power can be shared across many nodes. This allows AI tasks to be distributed and processed by multiple machines in parallel, rather than relying on centralized servers or data centers. By leveraging the collective computing power of a distributed network, blockchain can provide the massive computational resources needed for AI workloads.
  - This is also known as "decentralized physical infrastructure," or "DePIN." DePINs combine physical infrastructure with blockchain technology to create decentralized networks for various applications. Specifically, DePINs use peer-to-peer (P2P) networks where individuals contribute physical infrastructure resources like data storage, wireless connectivity, sensors, or energy grids. They enable autonomous, real-time interactions

[22] *Id*.

within physical infrastructures using technologies like smart contracts and the Internet of Things (IoT).[23]

    - Participants are incentivized through token rewards for providing services or resources to the network. Although DePINs have the potential to transform infrastructure management, most projects are still in their nascent stages, and there remain regulatory hurdles and scalability limitations. Additionally, integration of blockchain with physical systems requires robust security measures and user-friendly interfaces.

- **Incentives Through Tokenization:** Blockchain networks often use cryptocurrency tokens to incentivize participants to contribute their computing power. Users who offer their computational resources for AI tasks can earn tokens as rewards, creating an economic model that encourages more nodes to join the network and contribute resources.

    - Relatedly, crypto can be used to incentivize and compensate users for sharing their data for model training purposes.

    - For example, FLock.io allows users to train a model such that it is "split" between multiple servers, so that no party has access to all of the training data.[24] This allows a user to participate in training the model directly—as opposed to having his or her data taken from another source—without revealing any of it to third parties. Not only does this schema promote user privacy, but it also encourages user autonomy and honesty: users are incentivized to participate in the training process through crypto rewards and penalized for any efforts to sabotage the training process.

- **Efficient Resource Allocation:** Smart contracts on blockchain networks can be used to automatically allocate computing resources to AI tasks based on predefined rules and conditions. This allows for more efficient utilization of available computing power across the network.

- **Enhanced Scalability:** The peer-to-peer architecture of blockchain networks enables greater scalability compared to centralized systems. As more nodes join the network, the overall computing capacity grows, allowing AI applications to scale more easily.

- **Improved Data Management:** Blockchain can provide a secure and transparent way to manage the vast amounts of data required for AI training and inference. This can help streamline data access and sharing while maintaining privacy and security.

- **Cost Reduction:** By leveraging distributed computing resources, blockchain-based AI solutions can potentially reduce the costs associated with building and maintaining large centralized computing infrastructures.

- **Global Accessibility:** Decentralized AI computing networks built on blockchain technology can provide more equitable access to AI resources globally, allowing participants from various locations to contribute and benefit from the network.

---

[23] Arunkumar Krishnakumar, *Decentralized Physical Infrastructure Network (DePIN) Explained*, Cointelegraph (Feb. 20, 2024), https://cointelegraph.com/explained/decentralized-physical-infrastructure-network-depin-explained.
[24] Introduction to FLock.io, Flock.io, https://docs.flock.io/ (last visited July 29, 2024).

c. Fair Lending, Data Privacy, Fraud, Illicit Finance, and Insurance

***Question 9*: How are financial institutions evaluating and addressing any increase in risks and harms to impacted entities in using emerging AI technologies? What are the specific risks to consumers and other stakeholder groups, including low- to moderate-income consumers and/or underserved individuals and communities (e.g., communities of color, women, rural, tribal, or disadvantaged communities)? How are financial institutions protecting against issues such as dark patterns – user interface designs that can potentially manipulate impacted entities in decision-making – and predatory targeting emerging in the design of AI? Please describe specific risks and provide examples with supporting data.**

The following constitute major threats to both traditional financial institutions and digital asset firms: social engineering, malware attacks/hacks, and identity impersonation. These threats are even greater among communities with less access to financial or social capital and that are more vulnerable to predatory actors.

- Fraudsters have long depended upon social engineering tactics to gain the trust of potential victims and glean information that will grant the illicit actors access to private accounts at financial institutions. AI can make social engineering scams more effective through more versatile deepfakes, for instance. AI could also help scammers to more easily generate fake—albeit unique—websites, photos, and online personas, which would make pig butchering schemes harder to detect. Even if there is not yet much public reporting of pig butchering scammers using AI, these enhanced capabilities are likely to raise fraud risks for users of all types of financial institutions, including crypto exchanges.

- Bad actors have also relied on malware to hack into systems and access money. AI can help effectuate malware attacks by generating new code at rates that cybersecurity systems cannot respond to quickly enough. In crypto, bad actors have hacked exchanges by taking advantage of vulnerabilities in the protocols. Here, AI may also be better at detecting such vulnerabilities.

- One of the oldest methods for bypassing the security measures of financial institutions is identity impersonation. The proliferation of AI can take these scams to entirely new levels, with the ability to imitate voices and even moving images. In both crypto and traditional finance, bad actors have been able to bypass KYC measures for institutions using AI.

- Nevertheless, digital identity (or digital ID) solutions, which can be secured by the same cryptographic techniques that secure blockchains, could help mitigate the risks of identity impersonation. The potential value of digital ID solutions is evident in FinCEN's recent tech sprints on digital identity in which multiple participants demonstrated how emerging cryptographic techniques such as zero knowledge proofs and multi-party computation can bolster privacy and data security in various public and private sector services.[25] It is notable that several

[25] FDIC FinCEN Digital Identity Tech Sprint - Key Takeaways and Solution Summaries, FinCEN News (Sep. 29, 2022), https://www.fincen.gov/news/news-releases/fdic-fincen-digital-identity-tech-sprint-key-takeaways-and-solution-summaries.

proposals recommended the use of emerging digital identity standards, including the Worldwide Web Consortium (W3C) Verifiable Credentials and ISO compliant mobile driver's licenses. Integrating such standards into financial services could mitigate the risks of identity threats derived from both AI-based and conventional fraud typologies.

While threats perpetuated by social engineering, malware attacks/hacks, and identity impersonation are common to both traditional financial institutions and digital asset firms, alike, the latter may be better positioned to address the challenges.

- As discussed, blockchains enable the preservation of large swaths of irreversible and immutable data. Accordingly, analytics tools can be applied to blockchains to better detect past and future illicit activity.
- Moreover, the blockchain industry is already working on digital identity solutions to ensure that only licit actors are able to transact on blockchain networks.
- Finally, the decentralized architecture of blockchains offers some infrastructural resiliency by preventing central points of failure even if attacks on base-layer infrastructure do occur.

***Question 10*: How are financial institutions addressing any increase in fair lending and other consumer related risks, including identifying and addressing possible discrimination, related to the use of AI, particularly emerging AI technologies? What governance approaches throughout the development, validation, implementation, and deployment phases do financial institutions expect to establish to ensure compliance with fair lending and other consumer-related laws for AI models and tools prior to deployment and application? In what ways could existing fair lending requirements be strengthened or expanded to include fair access to other financial services outside of lending, such as access to bank accounts, given the rapid development of emerging AI technologies? How are consumer protection requirements outside of fair lending, such as prohibitions on unfair, deceptive and abusive acts and practices, considered during the development and use of AI? How are related risks expected to be mitigated by financial institutions using AI?**

As discussed in our responses to Questions 7 and 8, blockchain technology is capable of and holds continued potential to make the process of AI model training more transparent by tracking data inputs. This, in turn, will decrease the chances of faulty model outputs, such as those demonstrating unsubstantiated and discriminatory preferences.

- For example, firms like FICO have developed proof of concept blockchain-based solutions to train and audit AI models, which could eventually ensure that credit scoring and other tools used to determine lending which depend on AI do not contain discrimination bias.[26]
- Los Angeles-based EQTY Lab also created a new method, employing cryptography and blockchain, to track the origins and characteristics of large language models, and provide

[26] Scott Zoldi, *How to Use Blockchain to Build Responsible AI: An Award-Winning Approach*, FICO Blog (Oct. 17, 2023), https://www.fico.com/blogs/how-use-blockchain-build-responsible-ai-award-winning-approach-0.

transparency on their inner workings, so companies and regulators can easily inspect them.[27] The method aims to automatically examine the AI model as it is being created, rather than focus on its output.

***Question 11*: How are financial institutions addressing any increase in data privacy risk related to the use of AI models, particularly emerging AI technologies? Please provide examples of how financial institutions have assessed data privacy risk in their use of AI. In what ways could existing data privacy protections (such as those in the Gramm-LeachBliley Act (Pub. L. No. 106-102)) be strengthened for impacted entities, given the rapid development of emerging AI technologies, and what examples can you provide of the impact of AI usage on data privacy protections? How have technology companies or third-party providers of AI assessed the categories of data used in AI models and tools within the context of data privacy protections?**

As alluded to in our responses to Questions 4, 7, and 9, blockchain technology can significantly help mitigate risks related to data privacy in training AI models through several key mechanisms:[28]

- **Decentralized Data Storage:** The distributed nature of blockchains allows for storing sensitive data across multiple nodes rather than in a centralized database. This decentralization reduces the risk of large-scale data breaches and unauthorized access.
- **Enhanced Data Security:** Blockchain's cryptographic algorithms and immutable ledger provide robust security features, making it extremely difficult for malicious actors to tamper with or steal data used in AI model training.
- **Privacy-Preserving Techniques:** Blockchain can facilitate privacy-enhancing technologies like federated learning, which allows AI models to be trained on distributed datasets without centralizing raw data. This approach significantly reduces the risk of data exposure.
    - Fully Homomorphic Encryption ("FHE") is one such privacy-preserving technique that can be used to train an AI model in a privacy-preserving manner. For example, the company Privasea utilizes FHE to train AI models for processing encrypted data, ensuring input privacy.[29] This innovation facilitates a ChatGPT-like model that operates on encrypted prompts so that the service provider never sees users' unencrypted content. The system processes these encrypted inputs and generates encrypted outputs, which only the user can decrypt and understand. This method protects user data from exposure and is

[27] Reed Albergotti, *As More Governments Look at AI Rules, Accenture Tests Software to Help Companies comply*, SEMAFOR (Feb. 9, 2022), https://www.semafor.com/article/02/09/2024/accenture-tests-software-to-help-companies-comply-with-ai-rules.
[28] Stanton Heister and Kristi Yuthas, *How Blockchain and AI Enable Personal Data Privacy and Support Cybersecurity*;T. M. Fernández-Caramés, & P. Fraga-Lamas (Eds.), "Advances in the Convergence of Blockchain and Artificial Intelligence," IntechOpen (2021), https://www.intechopen.com/chapters/75936; Ahmed M. Shamsan Saleh, *Blockchain for Secure and Decentralized Artificial Intelligence in Cybersecurity: A Comprehensive Review*, Blockchain: Research and Applications (Feb. 29, 2024) https://doi.org/10.1016/j.bcra.2024.100193; *How AI Can Benefit from Blockchain-Based Infrastructure*, LCX (Feb. 27, 2024), https://www.lcx.com/how-ai-can-benefit-from-blockchain-based-data-infrastructure/.
[29] Privasea AI Whitepaper, https://drive.google.com/file/d/1jbxWMgEziupt119gvM1n0Mu8sDdM7VWF/view.

particularly crucial for sensitive sectors like finance, where it is particularly important to safeguard against data leaks.

- **Transparent and Auditable Data Trails:** Blockchain's immutability holds the potential to ensure that all data transactions and model training processes can be transparently recorded and audited. This feature enhances accountability and helps in maintaining regulatory compliance.

- **Secure Data Sharing and Marketplaces:** Blockchain-based data marketplaces allow individuals and organizations to securely share or sell their data for AI training while retaining ownership and control. Smart contracts can automate data access permissions and ensure proper data usage and management.

- **Identity Management and Authentication:** Blockchain can provide secure and verifiable identity authentication, mitigating identity-related risks in AI model training and data access.

***Question 12*: How are financial institutions, technology companies, or third-party service providers addressing and mitigating potential fraud risks caused by AI technologies? What challenges do organizations face in countering these fraud risks? Given AI's ability to mimic biometrics (such as a photos/video of a customer or the customer's voice) what methods do financial institutions plan to use to protect against this type of fraud (e.g., multifactor authentication)?**

Traditional financial institutions can benefit from much of the computer science tools and approaches used in the digital asset space. As discussed in Part A, blockchain analytics tools are adept at detecting and mitigating potential and past fraud activity. The same cryptographic methods that secure blockchains can also help protect the traditional financial system against AI risks through the adoption of cryptographically-signed digital credentials for account access. Using digital identity solutions (as mentioned in our response to Question 9) can bolster KYC controls against AI-driven identity verification threats, even in an environment where deepfakes and synthetic identities are becoming more sophisticated.[30]

***Question 13*: How do financial institutions, technology companies, or third-party service providers expect to use AI to address and mitigate illicit finance risks? What challenges do organizations face in adopting AI to counter illicit finance risks? How do financial institutions use AI to comply with applicable AML/CFT requirements? What risks may such uses create?**

AI can be useful at most stages of the customer and transaction lifecycle with respect to AML/CFT and sanctions compliance, including (i) conducting due customer diligence and document verification, (ii) detecting unusual transaction patterns (rather than traditional rule-based systems), (iii) responding to and

[30] Linda Jeng, et al., *Chains of Trust: Combatting Synthetic Data Risks of AI* (June 4, 2024), https://ssrn.com/abstract=4854347; The Investment Case Series #1: Blockchain, the Key Technology to Combating AI-driven Identity Risks, 21shares Insights (May 25, 2023), https://www.21shares.com/en-eu/research/blockchain-and-ai; Charlyn Ho, *AI And Blockchain Can Mitigate Fraud Risk Caused By Deepfakes*, Forbes (July 9, 2024), https://www.forbes.com/sites/digital-assets/2024/07/06/ai-and-blockchain-synergies-mitigate-risk-of-deepfakes-in-kyc/.

evaluating AML and sanctions alerts that arise from screening vast numbers of payments, and ensuring consistency and good audit trails with compliance-related decision-making.

AI is particularly useful in supporting the transactions monitoring needed for AML/CFT compliance, especially in generating alerts and drafting internal narratives about suspicious transactions. Such machine learning that improves the monitoring process can gain greater insights from operational data and help automate compliance tasks that typically rely on manual processes and observations. It can improve compliance teams' evaluation of conventional transactions as well as blockchain activity. With blockchain analysis, software developers can use AI to build better models to cluster cryptocurrency wallet addresses and improve identity attribution of entities transacting on blockchains.

Despite the potential for AI to efficiently detect illicit activity, there remains the challenge of ensuring that models meet regulatory requirements, including those related to consumer protection. To address this challenge financial institutions must adopt robust data governance frameworks, invest in model interpretability techniques, maintain strong cybersecurity measures, and ensure ongoing human oversight and involvement in AI-driven AML/CFT processes. Additionally, they should stay informed about evolving regulatory requirements and guidance related to AI use in financial services.

Some of the specific potential risks associated with the use of AI models for transactions monitoring include the following:

- AI models rely heavily on the quality and representativeness of input data. Inaccurate or biased data can lead to false positives or false negatives, potentially undermining the effectiveness of AML/CFT efforts.
- AI systems, especially complex ones, often operate as "black boxes," making it difficult to understand how they arrive at decisions. This lack of transparency can be problematic for compliance analysts and regulators who need to validate the rationale behind system outputs.
- AI systems are vulnerable to manipulation by malicious actors who may attempt to deceive the system's decision-making process. This could compromise the integrity of AML/CFT compliance processes.
- While AI can enhance efficiency, there is a risk of overreliance on automated systems. Human oversight remains crucial, especially for complex cases and high-risk scenarios.
- AI models may complicate compliance with existing data privacy laws, particularly as they become more adept at identifying owners of previously anonymized data.
- Many financial institutions rely on third-party AI providers, which can complicate risk management as AI complexity increases. When firms rely on third party providers, firms must ensure that these providers also have strong risk management strategies in place, particularly since such reliance increases the risk that confidential or sensitive data falls into the wrong hands.

C. Further Actions

***Question 18*: What actions are necessary to promote responsible innovation and competition with respect to the use of AI in financial services? What actions do you recommend Treasury take, and what actions do you recommend others take? What, if any, further actions are needed to protect impacted entities, including consumers, from potential risks and harms? Please provide specific feedback on legislative, regulatory, or supervisory enhancements related to the use of AI that would promote a financial system that delivers inclusive and equitable access to financial services that meet the needs of consumers and businesses, while maintaining stability and integrity, protecting critical financial sector infrastructure, and combating illicit finance and national security threats. What enhancements, if any, do you recommend be made to existing governance structures, oversight requirements, or risk management practices as they relate to the use of AI, and in particular, emerging AI technologies?**

Regulators must craft any new regulation of this emerging and promising technology with precision and nuance, and avoid using a broad brush. Overregulation is the greatest risk to innovation while a technology is within its nascent development. In order to unlock the benefits of AI (e.g., enhancing financial services, promoting financial inclusivity, and countering illicit activities), responsible regulation necessitates well-informed, evidence-driven policy choices achieved through collaborative participation.

***Question 19*: To what extent do differences in jurisdictional approaches inside and outside the United States pose concerns for the management of AI-related risks on an enterprise-wide basis? To what extent do such differences have an impact on the development of products, competition, or other commercial matters? To what extent do such differences have an impact on consumer protection or availability of services?**

U.S. regulators should assess and learn from other jurisdictions' attempts to regulate AI, particularly to the extent that such jurisdictions neglect to adopt thoughtful, risk-based approaches to regulation. The EU has sought to take the lead in AI regulation by adopting the AI Act, which is set to be the world's first comprehensive law regulating artificial intelligence.[31] The EU aims for the AI Act to have a global impact similar to GDPR, potentially serving to influence AI regulation in other jurisdictions.[32] This ambition has been demonstrated via the EU's input into—and influence over—broader developments in international bodies' work in this field, such as the Council of Europe and the OECD. The AI Act will ban AI practices deemed to pose unacceptable risks, such as social scoring systems and manipulative AI, and impose strict requirements on high-risk AI systems in areas like critical infrastructure, education, and law enforcement. The U.S. should cautiously evaluate the EU's approach and ascertain if it may be prematurely restrictive while AI development is still relatively nascent.

The EU's requirements around AI are not only likely to impact U.S. financial institutions operating in Europe, but they may influence the processes firms employ in the U.S., where there is less regulatory certainty. It is important for U.S. policymakers to observe the regulations developing globally, especially

[31] *EU AI Act: First Regulation on Artificial Intelligence, European Parliament* (June 8, 2023), https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence (last updated June 18, 2023).
[32] *EU Formally Adopts World's First AI Law*, Sidley Blog Post (Mar. 21, 2024), https://datamatters.sidley.com/2024/03/21/eu-formally-adopts-worlds-first-ai-law/.

in the EU, and to promote a risk-based approach to regulating AI in financial services that takes into consideration global regulatory developments. However, U.S. policymakers should be cautious of adopting overly expansive rules that may stifle innovation and make AI system development accessible to only the biggest players in the space. U.S. policymakers should also prioritize research and development of decentralized AI in order to promote greater resilience and innovation of the AI sector.

***

Respectfully submitted,

Sheila Warren
Chief Executive Officer
Crypto Council for Innovation

Ji Hun Kim
Chief Legal & Policy Officer
Crypto Council for Innovation

Yaya J. Fanusie
Director of Policy for AML & Cyber Risk
Crypto Council for Innovation