BLOCKCHAIN ASSOCIATION

April 29, 2024

VIA EMAIL (IaaScomments@bis.doc.gov)

Elizabeth Cannon
Executive Director for Information and Communications Technology and Services
Office of Information and Communications Technology and Services
Bureau of Industry and Security
Department of Commerce
14th Street and Constitution Avenue NW
Washington, DC 20230

Re: Department of Commerce Proposed Rulemaking RIN 0694-AJ35; Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities

Dear Executive Director Cannon:

Blockchain Association respectfully submits this letter in response to a request for comments by the Department of Commerce's Bureau of Industry and Security ("BIS") on its proposed rule "Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities," 89 Fed. Reg. 5698 (Jan. 29, 2024) (the "Proposed Rule"). BIS issued the Proposed Rule to implement Executive Order ("E.O.") 13984 ("Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities") and E.O. 14110 ("Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence").

Blockchain Association thanks BIS for the opportunity to comment on the Proposed Rule. Malicious cyber-enabled activities pose a genuine threat to U.S. national security and economic prosperity, and BIS deserves recognition for its efforts to propose regulations to enable the United States to better address these risks.

Blockchain Association (hereinafter the "Association") is the leading nonprofit membership organization dedicated to promoting a pro-innovation policy environment for the digital asset economy. The Association endeavors to achieve regulatory clarity and to educate policymakers, regulators, courts, and the public about how blockchain technology can create a more secure, competitive, and consumer-friendly digital marketplace. The Association represents nearly 100 member companies reflecting the wide range of the blockchain industry, including software developers, exchanges, custodians, investors, and others supporting the public blockchain ecosystem.

The Association shares BIS's goal of securing the United States against cyber-enabled threats to national security, including protecting critical infrastructure and preventing intellectual property theft. However, the Association believes that BIS can best achieve the objectives of the Proposed Rule, which seeks to address the risk of foreign actors using U.S. cloud services to harm critical infrastructure or national security, by ensuring that the Proposed Rule does not inadvertently sweep in those, like the Association's membership, that may use Infrastructure as a Service ("IaaS") but are not themselves providers or resellers of IaaS. Specifically, BIS should explicitly confirm our understanding that participants in decentralized blockchain systems, including but not limited to developers, validators, miners, Remote Procedure Call ("RPC") nodes, relayers, and node operators, are neither persons offering or otherwise providing, nor constitute, "Infrastructure as a Service products," ("IaaS products") as the term is defined in the Proposed Rule, nor "resellers" or "foreign resellers" of such products under the Proposed Rule.

We believe that BIS's exclusion of such participants from the Proposed Rule appropriately recognizes that they, and the blockchain infrastructure, are fundamentally different from conventional IaaS providers and infrastructure constituting IaaS products. Indeed, the Proposed Rule and its authorizing Executive Orders implicitly recognize this by remaining silent on blockchain and digital assets. BIS should confirm this explicitly in the Final Rule.

Although the Proposed Rule defines "Infrastructure as a Service product" broadly, this definition does not include blockchain participants referenced above that contribute to a blockchain ecosystem.

Like other consumers of conventional IaaS products, key blockchain participants will typically not manage or control the underlying hardware that IaaS providers make available and will only use this infrastructure to complete specific tasks that support blockchain systems, such as validating transactions or optimizing efficiency. Given these important differences, as well as other arguments set forth below, and the attendant harm that could result if the IaaS provider and reseller concepts covered such blockchain participants, the Association encourages Commerce to confirm that the Proposed Rule does not apply to blockchain participants.

The Proposed Rule also contains no discussion of blockchain systems or digital assets, the technical feasibility of blockchain participants implementing the Proposed Rule's Customer Identification Program (CIP) requirements, or the potential financial and other impacts that the

Proposed Rule would have on blockchain systems.[1] Moreover, as we detail in this letter, blockchain systems have historically not been a vector for launching the kinds of malicious cyber-enabled activities described by BIS. If the Proposed Rule did apply to blockchain systems, the Administrative Procedure Act ("APA") would require BIS to address and provide the public a meaningful opportunity to comment on all those issues (among others). BIS's failure to do so further demonstrates that the Proposed Rule does not apply to blockchain systems and their participants.

I. The Proposed Rule Does Not Apply to Blockchain Participants Who Use IaaS Products.

Given the foregoing differences between IaaS providers and resellers of IaaS products on the one hand, and blockchain participants on the other hand, BIS should make clear in its Final Rule that the definitions of "U.S. IaaS provider," "U.S. reseller," and "foreign reseller" do not cover blockchain participants.

The Proposed Rule would require that (1) U.S. IaaS providers and their foreign resellers establish written CIPs to collect, verify, and maintain identifying information about their foreign customers; (2) U.S. IaaS providers notify Commerce outside of an annual CIP reporting cycle in various situations, including when the provider undergoes a significant change in business operations or corporate structure; and (3) newly established U.S. IaaS providers submit a CIP certification prior to furnishing any foreign customer with an IaaS account. Our understanding is that none of the foregoing requirements apply to developers, validators, miners, RPC nodes, relayers, and other blockchain participants as they are not "IaaS providers," "resellers," or "foreign resellers."

The prototypical "U.S. IaaS provider," such as Google Cloud or Microsoft Azure, offers cloud computing services to customers that are fundamentally different from the specific and individual functions performed by the blockchain participants who contribute to the execution of digital asset transactions on decentralized blockchain systems. By failing to mention blockchain systems or digital assets and not considering the feasibility, costs, or other impacts, we interpret the

[1] E.O. 13984 and E.O. 14110 as well as Commerce's Proposed Rule were issued to address a national emergency declared in E.O. 13694 and pursuant to the International Economic Emergency Powers Act ("IEEPA"), which grants the President certain powers "to deal with any unusual and extraordinary threat," including the power to "regulate" the "importation or exportation of, or dealing in" "any property in which any foreign country or a national thereof has any interest by any person, or with respect to any property, subject to the jurisdiction of the United States." 50 U.S.C. § 1701 *et seq*. IEEPA requires *inter alia* that the President notify Congress of (1) the circumstances which necessitate such exercise of authority; (2) why the President believes those circumstances constitute an unusual and extraordinary threat, which has its source in whole or substantial part outside the United States, to the national security, foreign policy, or economy of the United States; and (3) why the President believes such actions are necessary to deal with those circumstances. 50 U.S.C. § 1703. We note that the President has not explained to Congress why regulating blockchain participants that use IaaS services or requiring such blockchain participants to establish CIPs, notify Commerce, or submit CIP certifications is necessary to deal with the national emergency declared by the President in Executive Order 13694.

Proposed Rule to recognize the distinction between decentralized blockchain systems and other IaaS providers.

In relevant part, the Proposed Rule defines an IaaS product as "any product or service offered to a consumer . . . that provides processing, storage, networks, or other fundamental computing resources, and with which the consumer is able to deploy and run software that *is not predefined*, including operating systems and applications" (emphasis added). Although blockchain participants can purchase computing resources from IaaS providers, they do not offer IaaS products because they perform specific and individual functions. For example, some blockchain participants validate transactions or secure blockchain networks by executing consensus and cryptographic algorithms on software that is predefined by blockchain protocols. Similarly, while some blockchain participants may purchase computing resources from third-party IaaS providers to run software that increases the speed and scalability of blockchain networks, they neither purchase IaaS from blockchain participants nor provide it to other blockchain users.

The Proposed Rule would also impose CIP requirements on U.S. "resellers" of U.S. "IaaS accounts."[2] U.S. resellers would be responsible for establishing the identity of their potential customers, including all prospective beneficial owners of these accounts, and determining whether they are U.S. persons, and would also be responsible for verifying the identity of their foreign customers under this Proposed Rule.[3] Participants in a blockchain system are not "resellers," as defined in the Proposed Rule. The Proposed Rule defines a "reseller" as someone who maintains a "reseller account."[4] A "reseller account" is defined as an "IaaS account" established to provide IaaS products to a person who will then offer those products subsequently, in whole or in part, to a third party.[5] An "IaaS account" means a formal business relationship established to provide IaaS products to a person in which details of such transactions are recorded.[6]

These concepts and definitions are not applicable to and cannot appropriately describe the relationship between blockchain participants. First, participants who support the proper functioning of a blockchain and the ecosystem built on top of it are not offering any type of "IaaS product." Second, the interactions between blockchain participants do not generally involve a "formal business relationship." Third, and importantly, blockchain participants do not typically resell services provided by other blockchain participants. Rather, they each complete specific tasks based on shared blockchain protocols. In effect, there is no "reseller account." Accordingly, blockchain participants are not "resellers" as defined in the Proposed Rule.

[2] 89 Fed. Reg. at 5703.
[3] *Id*.
[4] *Id.* at 5702.
[5] Exec. Order 13,984 (Jan. 19, 2021); 89 Fed. Reg. at 5701.
[6] *Id*.

II. Excluding Blockchain Participants from the Proposed Rule Would Be Consistent with BIS's General Approach of Enabling Other Agencies to Maintain Their Primacy in Regulating the Financial Sector and Financial Sector Technology.

Decentralized blockchain systems rely on individual and unrelated participants performing specific functions to facilitate the validation of transactions, some of which are financial in nature. Forcing compliance with the Proposed Rule upon blockchain participants would subvert the consensus-based protocols that underpin decentralized blockchain systems.

BIS has not historically regulated the export of finance technology ("FinTech") or blockchain-related infrastructure. Rather, it has traditionally deferred to other federal agencies and allowed specialized financial regulators to take the lead in regulating technologies that support FinTech and digital asset-related products and services. This deference is particularly evident in BIS's decision to exempt different financial sector products from its information security controls. This longstanding approach has allowed for the rapid introduction and proliferation of financial sector products that use otherwise controlled technologies, such as those that enable information security.

BIS's Commerce Control List ("CCL") identifies items subject to Department of Commerce jurisdiction. The CCL classifies certain information security items as Category 5, Part 2 items and regulates their design, development, export, and use by applying certain national security and encryption item licensing policies.[7] Using specific export control classification numbers and their associated licensing policies, BIS has regulated different types of cryptographic and other information security technology; however, in regulation and practice, BIS has exempted the same technology when it is incorporated in banking sector products to ensure the privacy and integrity of financial sector participants and transactions.[8]

BIS's restraint in regulating the application of information security technologies used in the financial sector has helped ensure that financial institutions have had the required flexibility to quickly develop and implement appropriate levels of information security across financial systems and transaction types. The same restraint is warranted in any proposed BIS regulation that could impact blockchain-based systems. BIS should not impose regulations that could undermine the decentralized, consensus-based protocols that blockchain participants currently use to validate transactions.

[7] 15 C.F.R. § 774.1 Supplement No. 1.
[8] *Id*.

III. Regulating Blockchain Participants Would Not Advance the Proposed Rule's Objectives.

As the Proposed Rule explains, IaaS products "offer customers the ability to run software and store data on servers offered for rent or lease without having to assume the direct maintenance and operating costs of those servers."[9] The Proposed Rule targets these products because foreign malicious cyber actors have in the past and continue to leverage U.S. IaaS products to engage in a range of malicious cyber-enabled activities.[10] Based on our review of the ANPRM and other relevant executive orders, proposed rules, and U.S. Government agency publications, there is a long list of malicious cyber-enabled activities that leverage IaaS:

- data theft, including, among other types of data, intellectual property, health data, government information, and financial user information;
- espionage (including corporate espionage);
- targeting of U.S. critical infrastructure;
- cyber-attacks, such as denial of service attacks;
- exploitation of U.S. networks and systems to facilitate data breaches, potentially modifying critical files or data streams, or otherwise impacting the availability of data across U.S. networks; and
- training large AI models that can assist or automate malicious cyber activity.[11]

In the Proposed Rule, BIS also explains that malicious actors "[a]fter carrying out such illicit activity, [. . .] can quickly move to replacement infrastructure offered by U.S. IaaS providers of U.S. IaaS products" and that this "temporary registration and ease of replacement for such services makes it more difficult for the government to track malicious actors."[12] The Proposed Rule attempts to address these threats by implementing CIP requirements for U.S. IaaS providers and their U.S. and foreign resellers.

While the Association shares and supports BIS's efforts to prevent the use of IaaS products for these purposes, we believe that imposing the proposed CIP requirements on blockchain participants will not advance these efforts for a few reasons.

First, available reporting indicates that blockchain infrastructure is generally not deployed to launch cyberattacks of the types noted above. We understand the U.S. government shares this understanding as none of the publications describing the malicious activities being targeted reference the use of blockchain systems to launch or otherwise enable such malicious activities.

---

[9] 89 Fed. Reg. at 5698
[10] *Id*.
[11] *See* 89 Fed. Reg. 5698; 86 Fed. Reg. 53018 (Sept. 24, 2021); 86 Fed. Reg. 6837 (Jan. 25, 2021); 84 Fed. Reg. 22689 (May 17, 2019); 82 Fed. Reg. 1 (Dec. 28, 2016); 80 Fed. Reg. 18077 (Apr. 1, 2015); and CISA Alert AA20-258A (Oct. 24, 2020).
[12] *Id*.

Second, the decentralized, consensus-based nature of blockchains makes them more resilient to attack and manipulation than traditional IaaS platforms. For example, with respect to blockchains utilizing a proof of work mechanism for network validation, malicious actors would need to compromise a majority of nodes to control a blockchain network. Such a move, through a 51% attack or a selfish mining attack, is complex, computationally expensive, and subject to quick detection.[13]

In short, the constant validation that globally dispersed blockchain participants perform makes a blockchain system an unlikely vehicle for launching or supporting the malicious cyber-enabled activities this Proposed Rule aims to address; thus, applying the Proposed Rule to blockchain participants would not necessarily advance the Proposed Rule's objective.

IV. A CIP Regime of the Type Contemplated by the Proposed Rule Is Inappropriate for Blockchain's Decentralized Technology and Products.

A. CIPs Contemplated by the Proposed Rule Rely on an Intermediated System.

The Proposed Rule requires that U.S. IaaS providers and their foreign resellers maintain CIPs, perform effective customer verification, and maintain identifying information about their foreign customers.[14] To facilitate this requirement, the Proposed Rule would mandate that all U.S. IaaS providers implement their own CIPs, require CIPs of their foreign resellers, and report to the Department of Commerce on these CIPs.[15] Such CIPs should be risk-based and tailored to match the service provider's unique service offerings and customer bases.[16] The Proposed Rule would require, at a minimum, the collection of the following data: a customer's name, address, the means and source of payment for each customer's account, email addresses and telephone numbers, and internet protocol (IP) addresses used for access or administration of the account, and the CIPs would need to account for the collection of identifying information about the actual account owner and all beneficial owners of the account.[17]

As contemplated, establishing, administering, and enforcing the requirements of the CIP requires a centralized actor (in this case, U.S. IaaS providers and U.S. resellers of U.S. IaaS products). Such centralized actors would collect, store, and maintain identifying information about its customers and report required information to the Department of Commerce. Such persons would not only facilitate transactions but also have visibility into the use of their services by their customers.

---

[13] *See* 51% Attack: Definition, *Who Is at Risk, Example, and Cost*, Investopedia (June 7, 2023), https://www.investopedia.com/terms/1/51-attack.asp; Griffin Mcshane, *What Is a 51% Attack?*, CoinDesk (May 11, 2023), https://www.coindesk.com/learn/what-is-a-51-attack/; Sam Cooling, *Selfish Mining Attack (Bitcoin)*, Techopedia (Oct. 3, 2023), https://www.techopedia.com/definition/selfish-mining-attack-bitcoin.

[14] *See* 89 Fed. Reg. 5698; 86 Fed. Reg. 53018 (Sept. 24, 2021); 86 Fed. Reg. 6837 (Jan. 25, 2021); 84 Fed. Reg. 22689 (May 17, 2019); 82 Fed. Reg. 1 (Dec. 28, 2016); 80 Fed. Reg. 18077 (Apr. 1, 2015); and CISA Alert AA20-258A (Oct. 24, 2020).

[15] *Id*.

[16] *Id*.

[17] *Id*.

B. Blockchain Systems Are Disintermediated by Nature.

Public blockchains are permissionless, decentralized, and immutable ledgers that enable a globally distributed, unaffiliated network of participants to share data and reach consensus on the validity of that data on a disintermediated basis. Decentralized systems are disintermediated by nature: no organization, association, or group of persons is necessary to administer such systems or provide tools that users may use to interact and transact. Autonomous, self-executing smart contracts and the connection of users to such autonomous software or other users in a peer-to-peer fashion differentiate decentralized activity from centralized activity.

Put differently: blockchain systems operate without centralized control and are, instead, constructed using open-source software. Decisions regarding protocol changes are typically made by a community of participants or, depending on the protocol, may not be able to be made at all. Through different governance methods, the participants can propose and implement changes of blockchains ecosystems directly. A single individual, however, cannot unilaterally alter decentralized blockchains.

C. An Account-based Model Is Inconsistent with the Nature of Blockchain Systems.

The Proposed Rule would require IaaS providers and resellers to collect CIP information regarding customers who hold accounts and draws the concept and definition of account from E.O. 13984, which defines IaaS accounts as a "formal business relationship established to provide IaaS products to a person in which details of such transactions are recorded."[18] Most blockchain participants do not enter into the kinds of bilateral, formal relationships described in the definition. For example, among other blockchain participants, RPC nodes, block builders, validators, and node operators each function independently of one another and generally do not form account relationships with particular users of blockchain systems.

As part of the blockchain model, blockchain participants do not have access to user-identifying information and generally do not interact with users at all. The absence of a centralized party that has the ability to alter the parameters of a blockchain system unilaterally is a key feature of blockchain systems. Consequently, establishing a centralized entity to implement changes necessary to attempt to capture user information in these systems would be inconsistent with the nature of blockchain systems.

The ability to keep user identities private is one of the fundamental concerns of many digital asset holders and other blockchain participants. Blockchains are transparent, chronological records of transactions maintained by blockchain participants. Due to the public and immutable nature of the vast majority of information regarding transactions on a blockchain, any attempt to link these already public transactions to personal identities would create a serious and permanent privacy issue for those users. If a user's personal identifying information is ever

[18] Exec. Order 13,894, Sec. 5(d).

connected to these public transactions, their entire transaction history—both past and future—and potentially other sensitive information would be exposed. This is akin to publishing an individual's entire credit card transaction history online. Therefore, to protect user privacy, it is crucial that blockchain participants are not required to collect and maintain users' personal identifying information.

Forcing public blockchains to maintain personal, sensitive information about users would fundamentally change their structure and introduce many risks inherent to the traditional finance system that disintermediated systems are designed to eliminate. Imposing the Proposed Rule's CIP requirements on miners, validators, and other blockchain participants would force them to act as intermediaries, introducing the same cybersecurity risks and vulnerabilities that currently plague traditional financial institutions and technology companies.

Furthermore, blockchain participants range from sophisticated entities to thousands of individuals, including those who may be under 18. BIS did not intend its Proposed Rule to impose CIP requirements on individuals. Requiring individual blockchain participants to collect and store personal identifying information poses significant potential risks to basic expectations of privacy as well as, in some cases, a user's personal safety and well-being. For example, by collecting customer identifying information in a single location, the customer information could become a more attractive target for hackers seeking to discover who is responsible for current and historical transactions.

Participants in decentralized blockchain systems are not situated to collect, verify, and store the information required by the CIP contemplated in the Proposed Rule. Beyond the inherent incongruence between participants in decentralized blockchain systems and traditional IaaS providers, who deal with customers at arm's length, forcing blockchain participants to maintain a CIP could actually increase risks to privacy and safety of digital asset users.

V. The Lack of Any APA-required Analysis of the Proposed Rule's Impact on the Digital Asset Industry Endorses the Association's View That It Does Not Apply to Blockchain Systems.

The fact that BIS has not explicitly considered and addressed the potential consequences of its Proposed Rule on the digital asset industry—as would be required under the APA if the Proposed Rule were intended to apply to blockchain participants—signals the rule's inapplicability to blockchain participants. BIS should confirm this explicitly in the Final Rule.

Under the APA, an agency rulemaking is "unlawful" if it exceeds the agency's constitutional or statutory authority or is "arbitrary, capricious, [or] an abuse of discretion."[19] A rulemaking is "arbitrary and capricious" if, among other things, the agency "entirely fail[s] to consider an important aspect of the problem."[20] Agencies must further "assess both the costs and the

[19] 5 U.S.C. § 706(2)(A)–(C).
[20] *Motor Vehicle Mfrs. Ass'n of U.S., Inc. v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 43 (1983).

benefits of [an] intended regulation," "propose or adopt a regulation only upon a reasoned determination that the benefits of the intended regulation justify its costs," and make decisions based on "the best reasonably obtainable scientific, technical, economic, and other information concerning the need for, and consequences of, the intended regulation."[21] The burden is higher for "significant regulatory action," which is defined in part as "any regulatory action that is likely to result in a rule that may . . . [h]ave an annual effect on the economy of $100 million or more or adversely affect in a material way the economy, a sector of the economy, productivity, competition, jobs, the environment, public health or safety, or State, local, or tribal governments or communities," as well as rules that may "[r]aise novel legal or policy issues."[22] The APA also requires agencies to "give interested persons an opportunity to participate in the rule making through submission of written data, views, or arguments."[23]

The regulatory requirements introduced by the Proposed Rule, if construed by BIS to encompass relevant blockchain participants, would subject them to substantial costs as well as significant, unprecedented, and, given the nature of the blockchain system, near-impossible compliance requirements. Those consequences are "important aspects of the problem" that the APA would require BIS to address—after providing the public an opportunity to comment—in order to apply the Proposed Rule to such blockchain participants.[24]

The Proposed Rule does not discuss decentralized finance, digital assets, or blockchain, and its impact assessment is silent on the potential impact of the proposed regulations on blockchain systems. Further, BIS has neither considered nor solicited public comment on the technical feasibility issues, significant costs, and operational burdens that implementation of the CIP would impose on blockchain participants. In fact, as a result of the CIP's burdens, many blockchain participants would likely be forced to cease their activity altogether. More fundamentally, BIS has not grappled with the fact that requiring such persons to adopt CIPs would not achieve the stated goals of the Proposed Rule, as discussed in detail above, because blockchain infrastructure has historically not been used to deploy or enable the kinds of malicious cyber activities that are targeted by the Proposed Rule and its authorizing Executive Orders.

BIS's failure to conduct any APA-required analysis related to the digital asset industry confirms that the rule does not apply to the blockchain ecosystem and its participants.

* * *

[21] Exec. Order No. 12,866, 3 C.F.R. 638 (1993).
[22] *Id.*
[23] *Id.* at § 553(c).
[24] *State Farm*, 463 U.S. at 43.

For the foregoing reasons, the Blockchain Association requests that BIS make clear in any final rule regulating IaaS products, providers, and resellers that the regulations do not apply to blockchain participants. The Blockchain Association thanks BIS for the opportunity to comment on this important rulemaking.

Respectfully submitted,

Sarah Milby
Head of Policy
Blockchain Association

cc: Stephanie Brooker
Chris Timura
Adam Smith
Matt Gregory
Nick Harper
Gibson Dunn & Crutcher LLP