November 1, 2022

Mr. Scott Rembrandt
Deputy Assistant Secretary
Office of Terrorist Financing and Financial Crimes
U.S. Department of the Treasury
1500 Pennsylvania Avenue, NW
Washington, D.C. 20220

Re: FR Doc. 2022-20279, "Ensuring Responsible Development of Digital Assets; Request for Comment"

Dear Deputy Assistant Secretary Rembrandt:

We welcome the opportunity to provide the U.S. Department of the Treasury with our feedback to the Request for Comment titled Ensuring Responsible Development of Digital Assets in line with Executive Order 14067 of March 9, 2022. We want to express our appreciation for your efforts in seeking to better understand the impact of digital assets on the U.S. economy, and we appreciate the Administration's approach to improving the regulation of this emerging industry with a whole-of-government approach that starts with collecting relevant details, often from industry participants such as ourselves, which we are more than happy to provide.

The Hedera Council ("Council") is a coalition of twenty-seven (27) independent and unaffiliated organizations who collectively operate and govern a Distributed Ledger Technology ("DLT") network based on the hashgraph consensus algorithm (the "Hedera Network"). As with other DLT networks, the Hedera Network provides a network-native digital asset for application developers and users to utilize when making the micropayments required whenever they consume a Hedera Network service, i.e., whenever their application makes an API call to the network. In the case of the Hedera Network, that digital asset is called an "hbar." This is a fundamental requirement of any public implementation of digital asset technology because anyone can use such APIs to build Web3 applications with high throughput, fair ordering, and low-latency consensus finality in seconds without relying on centralized infrastructure, but only if there is a cryptographically secure method of fairly compensating all of the decentralized infrastructure providers responsible for making these services available to the public. In the case of the Hedera Network, our coalition of independent network node operators provides

these services in an environmentally and financially sustainable manner, as documented in a recent study from University College London.[1] This is partially due to the fact that the Hedera Network uses a proof-of-stake security model, which is an increasingly popular and environmentally sustainable method of securing a distributed public ledger.

While we commend the comprehensive nature of the Request for Comment, we have chosen to focus our response on questions where we could provide details on competitive aspects of a distributed ledger technology that we are especially familiar with. The comment below specifically addresses Questions 2 and 3 of the AML/CFT Regulation and Supervision section in the Request for Comment:

> "Are there specific areas related to AML/CFT and sanctions obligations with respect to digital assets that require additional clarity? What existing regulatory obligations in your view are not or no longer fit for purpose as it relates to digital assets? If you believe some are not fit for purpose, what alternative obligations should be imposed to effectively address illicit finance risks related to digital assets and vulnerabilities?"

Thank you for your consideration and please reach out to us with any questions.

* * *

The disintermediation of both financial and non-financial transactions is one of the primary innovations inherent in digital asset infrastructure. Participants in a DLT network are able to completely self-custody their digital assets by retaining the privately-generated set of keys required to transact from an associated network account. Transactions on the network are also able to be effectuated completely peer-to-peer without requiring an intermediary to accept and transmit digital assets to the recipient on behalf of the sender. The primary role of the network's underlying infrastructure is simply to (a) ensure the validity of the transaction and (b) create a consensus record of the current state and history of the network.

Participants in DLT networks benefit from disintermediation in many ways. The lack of an intermediary can reduce the cost of a transaction by removing a required party that would otherwise need to be compensated for their services. Disintermediated transactions can reach settlement faster without requiring a third party to accept, custody, and transmit the asset to the recipient. Participants also benefit from the enhanced data reliability and availability of audit trails inherently generated in a decentralized consensus process and are not required to trust the data provenance of a centralized entity. At the same time, the disintermediation of transactions presents novel challenges to regulators seeking to enforce public policy initiatives and prevent illicit activity in the financial system.

Financial regulators traditionally achieve their policy objectives by enforcing requirements upon intermediaries in a financial ecosystem. The disintermediated nature of DLT networks may therefore require clarification or novel application of regulatory requirements. For example, U.S.

[1] http://blockchain.cs.ucl.ac.uk/blockchain-energy-consumption/

sanctions laws prohibit the facilitation of transactions with or between sanctioned entities; however, such requirements have traditionally contemplated either the parties to the transactions or their intermediaries. Enforcement of sanctions within a DLT network requires additional precision and clarity to effectively achieve desired policy outcomes without undermining the benefits and purpose of the technology. To achieve the required precision, regulations and liabilities should be imposed on the network participants that are best positioned to enable effective controls.

In August of 2022, the Office of Foreign Assets Control ("OFAC") sanctioned the virtual currency mixer Tornado Cash due to its use by a previously sanctioned entity. Importantly, Tornado Cash is fundamentally a collection of open-source software libraries with a diverse set of contributors made available for general, disintermediated use. Specifically, its software protocols are smart contracts allowing participants to deposit then withdraw the same digital assets, for various privacy-related purposes, without ever surrendering custody or control. Due to its nature as a usage- and user-neutral technology, no individual bad actor was ultimately named in the issuance of the sanction that had the capability to control the usage of the software. This enforcement action created substantial uncertainty for developers and DLT network participants to both understand the scope of sanctions enforcement and to control for such outcomes and liabilities.

In contrast, there are elements within a DLT network ecosystem that do have actors and do have interactions with users that may be controlled for, such as website providers and application operators that earn revenue through attracting users and providing access to DLT protocols and their related functionality. The stronger the relationship between an operator and a user, the more effective regulatory controls can be. For example, the process of geo-filtering user traffic to prevent usage from jurisdictions comprehensively embargoed by OFAC can be enhanced beyond simple IP filtering with additional user metadata when the user interacts with an operator through a website or other means.

This principle applies across other financial regulation regimes as well. The Bank Secrecy Act ("BSA") requires financial intermediaries and other types of money service businesses to register with the Financial Crimes Enforcement Network ("FinCEN") and are responsible for regulatory requirements such as customer due diligence and currency transaction and suspicious activity reporting. As applied to disintermediated activities on DLT networks, there are often no custodial intermediaries that meet the profile of a traditional money service business that is able to perform such user controls. Network node operators (also known as "validators") are performing passive, non-discretionary validation and recordkeeping functions and do not stand between two participants in the network.

To apply the principle of "same activity, same risk, same regulation," there are many parallels to draw with existing communications and financial activities that are informative in the DLT context. For example, a mobile phone service provider does not become a money transmitter simply because it enables customers to use mobile applications that facilitate funds transfers. Rather, any money transmitter obligations would run to the provider of the mobile application

enabling funds transfers, and the phone service provider would merely be the provider of communication or network access services. The BSA already codifies this concept in the "Network Access Exclusion" to the definition of a regulated "money transmitter," which excludes persons that merely provide the delivery, communication, or network access services used by a money transmitter, but did not opine directly on its applicability to network node operators in its most recent comprehensive guidance to the DLT industry.[2] Further, the lack of similar exclusion from OFAC controls may require node operators to implement untenable control mechanisms regardless of the money transmitter exclusion, and should also be explicitly exempted.

Finally, the public recordkeeping function of the network nodes is a tremendous opportunity over the traditional financial systems to identify, quantify, analyze, and therefore enforce penalties against illicit financial actors. This inherent transparency and traceability of the movement of funds allows investigators and compliance professionals to more efficiently map out actions, methods, and tools utilized by bad actors in a particular scenario or identify patterns across related activities. It allows for tracing the source of funds through multiple transfers, an opportunity to develop deeper network intelligence than may otherwise be visible in legacy financial systems without intense manual investigatory techniques.[3] There are already many examples of law enforcement successfully relying on the traceability of DLT network activities, such as the infamous Silk Road investigation.[4]

For the reasons mentioned above, we highlight the need for the U.S. Department of the Treasury to (a) clarify the scope of regulated intermediaries within a DLT network ecosystem, specifically with respect to node operation and software development, by explicitly providing guidance that (i) the Network Access Exclusion applies to DLT network node operators and (ii) extending an OFAC exemption to the same activity, (b) enforce and enhance cross-border compliance with existing regulations for DLT service providers that do perform traditional intermediation in financial transactions such as custodians and centralized exchanges by engaging with other jurisdictions through the FAFT to increase consistency in global compliance standards, and (c) embrace the technological capabilities and characteristics of DLT technologies that afford greater visibility and automation to law enforcement efforts by affording innovators the certainty necessary to invest time and capital to build novel and powerful tools through more prescriptive guidance and open collaboration with the private sector rather than dissuade such investments through continued regulation by enforcement.

Hedera is happy to provide assistance to the Treasury on these initiatives as well. Thank you for your consideration.

* * *

---

[2] https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf

[3] https://www.coincenter.org/education/policy-and-regulation/how-can-law-enforcement-leverage-the-blockchain-in-investigations/

[4] https://www.coincenter.org/silk-road-corruption-case-shows-how-law-enforcement-uses-bitcoin/

Sincerely,

Brett McDowell, Chair
Hedera Hashgraph, LLC