BLOCKCHAIN ASSOCIATION

Comments on the Financial Action Task Force's "Draft Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers"

April 2021

The Blockchain Association
1701 Rhode Island Avenue N.W.
Washington, D.C. 20036

April 20, 2021

Secretariat
Financial Action Task Force

Re: Draft Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers

To whom it may concern:

The Blockchain Association submits these comments in response to the Financial Action Task Force's (the "FATF") "Draft Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers"[1] (the "Draft Updated Guidance"). The Blockchain Association (the "Association") is a not-for-profit organization dedicated to improving the public policy environment for public blockchain networks to allow them to develop and prosper in the United States. The Association endeavors to educate policymakers, courts, law enforcement, and the public about distributed ledgers and the need for regulatory clarity to allow for a more secure, competitive, and innovative digital marketplace. The Association is comprised of industry leaders who are committed to responsibly developing and supporting public blockchain networks fueled by cryptocurrencies. Its diverse membership reflects the diversity of this dynamic market and includes projects that contribute to distributed networks, cryptocurrency exchanges, and early stage investors that support the entire ecosystem. Given this diverse membership, the Blockchain Association is well positioned to provide the FATF with insight into the practical implications of the recommendations put forth in the Draft Updated Guidance.

The Association fully supports the FATF's continued focus on the robust regulation of custodial intermediaries in the virtual asset ("VA") ecosystem, as this is the single most effective AML/CFT measure currently available to national regulators. At present, participants in the market must leverage the services of custodial virtual asset service providers ("VASPs") in order to

[1] Financial Action Task Force (FATF), "Draft Updated Guidance for a Risk-Based Approach to Virtual Assets and VASPs" (March 2021), *available at* https://www.fatf-gafi.org/media/fatf/documents/recommendations/March%202021%20-%20VA%20Guidance%20update%20-%20Sixth%20draft%20-%20Public%20consultation.pdf.

exchange their VAs for fiat currency.[2] These custodial institutions play a role that is substantially similar to intermediaries in the traditional financial ecosystem. Thus, the application of the existing FATF Standards to these VASPs is an effective approach to their regulation. As custodial intermediaries, these VASPs are well-positioned to play a gatekeeping role.

The existing AML/CFT regime is predicated in large part on keeping bad actors from using or infiltrating the financial system to launder their ill-gotten gains. Focusing on custodial intermediaries in the VA ecosystem is consistent with this approach. However, this traditional paradigm is not suited to combat ML/FT risks in the disintermediated financial ecosystem, i.e. an ecosystem predicated on the absence of custodial intermediaries. Effectively addressing ML/FT risk in the disintermediated system will require a new AML/CFT paradigm that is not focused on the roles and responsibilities of gatekeepers but rather employs technological solutions that support law enforcement efforts to police the decentralized financial system. Such solutions can leverage the very cryptographic technologies that have enabled the creation of distributed ledgers and their many innovative and far-reaching applications. The solutions will require cutting edge work, but we believe that they are technically feasible and will vindicate the core AML/CFT objectives that the FATF safeguards. This way forward will require a partnership between FATF and national authorities, on the one hand, and leaders in the digital assets industry, on the other, to devise standards and solutions that satisfy legal, technical, and commercial needs. The Association commits itself to support this effort fully.

This effort will be no small task, and the technologies that will enable effective AML/CFT in the disintermediated ecosystem still require technical development and input from regulators and experts. To provide the space and time to do this work, the Association respectfully requests that the FATF delay issuance of final guidance with respect to the disintermediated ecosystem for one year. This would allow governments, multilateral bodies, private firms, and other stakeholders to develop the tools and framework that offer the most promising potential solutions to the challenges at hand: to assist law enforcement and regulators in combating money laundering and countering terrorist financing and to prevent the misuse of the disintermediated ecosystem by bad actors. The Association and its members stand ready to devote their energy and expertise to assist FATF and other relevant bodies in this critical endeavor.

* * *

With the publication of Satoshi Nakamoto's white paper, "Bitcoin: A Peer-to-Peer Electronic Cash System,"[3] decentralized systems materialized into a tangible reality. In his paper, Nakamoto proposed "a purely peer-to-peer version of electronic cash that would allow online payments to be sent directly from one party to another without going through a financial

---

[2] Chainalysis, "The 2020 State of Crypto Crime" (January 2020) 12, *available at* https://go.chainalysis.com/rs/503-FAP-074/images/2020-Crypto-Crime-Report.pdf.

[3] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" (October 2008), *available at* https://bitcoin.org/bitcoin.pdf.

institution."[4] In other words, Nakamoto, using a permissionless and distributed system, devised a way to conduct decentralized payments. With the inception of Bitcoin, a new digital era began, and with it, a host of benefits to the global economy and society. More recently, the advent of "decentralized finance" protocols has similarly allowed individuals to perform a variety of financial transactions electronically on a peer-to-peer and non-custodial basis, i.e. without the participation of an intermediary. Perhaps most notably, decentralized finance represents one of the most promising solutions to the longstanding challenge of increasing financial inclusion, a challenge that has long hindered universally shared goals such as eradicating poverty and supporting the development of emerging economies. Of course, decentralized finance also offers security advantages, both through advanced encryption and by placing less reliance on centralized gatekeepers that may be the subject of hacking and exploitation from increasingly sophisticated illicit actors. Among the numerous other advantages of decentralized finance are lower costs, increased transparency, mitigation of systemic risks including reliance on systemically important financial market utilities, increased certainty, increased market competition, and protection of privacy.

These benefits have driven the meteoric adoption of decentralized financial services over the last year. On April 15, 2020, $728 million worth of digital assets were "locked" in decentralized finance protocols.[5] One year later, that figure rose to $55.8 billion, a 7,664% increase.[6] The potential for rapid mass adoption of decentralized financial services has rightly prompted interest in these systems from regulatory bodies around the world, including the FATF.

Regulation of decentralized financial systems presents challenges because anyone with an internet connection can deploy, use, experiment with, and participate in the maintenance of decentralized protocols. The Draft Updated Guidance represents an attempt to address this challenge by dramatically expanding the perimeter of regulations designed for custodial financial intermediaries to include any individual or entity that benefits from the provision of a financial service, "regardless of whether the profits are direct gains or indirect."[7] This regulatory approach, aimed at ensuring "…very few VA arrangements will form and operate without a VASP involved at some stage…,"[8] would not prevent the use of decentralized financial services by illicit actors. For example, while newly created centralized protocols could restrict access to known and identified public addresses, the code that powers decentralized finance protocols is open source, which means that it can be copied, edited to exclude such restrictions, and redeployed on a permissionless network in around 30 minutes by an individual with moderate coding skills and an internet connection. As a result, the open source nature of decentralized financial protocols

[4] Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 1.

[5] DeFi Pulse, "Total Value Locked (USD) in DeFi" (accessed April 15, 2021), *available at* https://defipulse.com/. "Total value locked" represents the dollar amount of assets secured by (i.e. staked in) decentralized finance protocols.

[6] Ibid.

[7] FATF, "Draft Updated Guidance," 30.

[8] Id., 26.

renders reliance on gatekeepers to control access to decentralized financial services unfeasible because there will always be permissionless alternatives available.

In the end, the Association fears that the Draft Updated Guidance's approach may prove counterproductive. The Draft Updated Guidance would not prevent illicit use of decentralized financial protocols or P2P transactions, and it effectively implements a *de facto* ban on licit actors' development of and participation in them. In addition, law enforcement's existing "window" into the decentralized ecosystem, provided by the interaction between custodial financial intermediaries and the P2P ecosystem, would begin to shut. For example, the Draft Updated Guidance discourages the interaction of the regulated custodial and P2P ecosystems, stating that VASPs "…should consider whether any VAs or products they plan to launch, or transact with, will enable P2P transactions… Similarly, VASPs and other obliged entities should consider the extent to which their customers may engage in, or are involved, in P2P activity."[9] Because illicit actors generally must leverage the services of a custodial VASP to derive benefits from ill-gotten gains, bifurcating the P2P ecosystem from the compliant VASP ecosystem may appear to be an effective approach to mitigating ML/TF risks in the P2P ecosystem today.

Relying on illicit actors' need to use custodial services over the medium to long term may be risky, however, if illicit actors are ever able to directly benefit from cryptocurrencies without exiting into the custodial fiat ecosystem. Should illicit actors be able to do so after the compliant VASP and P2P ecosystems have been bifurcated, law enforcement would have total visibility into transactions through the compliant custodial VASP ecosystem while having almost no visibility into the P2P ecosystem. This bifurcation would create two parallel financial systems: one centralized, permissioned, and totally surveilled, and the other totally decentralized, permissionless, and, at best, pseudonymous. The fact that many cryptocurrency seizures executed by law enforcement in the United States were enabled by attribution established when illicit funds entered the custodial VASP ecosystem evidences the potential consequences of restricting the interaction between the custodial and P2P ecosystems. Such a bifurcated world would inhibit law enforcement from monitoring and disrupting illicit activity within decentralized financial networks and, critically, prevent society from realizing the benefits of disintermediated systems.

Additionally, the Draft Updated Guidance would be impossible for many newly designated "VASPs" to implement. AML/CFT obligations designed for custodial financial intermediaries cannot be fulfilled by many of the entities and individuals the Draft Updated Guidance would designate as VASPs. The very nature of decentralized governance ensures no single actor or entity can exercise sufficient control over a protocol to function in the way that a custodial financial intermediary does in the traditional financial ecosystem. Moreover, because regulations designed for custodial intermediaries assume the intermediary has custody over the assets, newly captured non-custodial VASPs would be unable to comply with requirements like asset freezes because users of decentralized financial protocols retain total independent control of

[9] FATF, "Draft Updated Guidance," 15.

their assets. Entities potentially captured by the Draft Updated Guidance that would be unable to implement or comply with existing AML/CFT controls across decentralized financial protocols include: (i) governance token holders, (ii) software developers, (iii) noncustodial entities, and (iv) autonomous computer programs. We discuss each of these entities below.

1. Governance token holders

The FATF Glossary's definition of a VASP is restricted to "any natural or legal person who… as a business conducts…" the listed activities "…for or on behalf of another natural or legal person."[10] We do not believe that this definition captures governance token holders of decentralized systems because they do not conduct any of the listed activities "for or on behalf of another natural or legal person." As several passages within the Draft Updated Guidance that extrapolate on the Glossary's definition may be read to designate these token holders as VASPs—at some points regardless of the extent to which the person influences the protocol—we respectfully request that the FATF clarify its intent. For example, the Draft Updated Guidance states that "where customers can access a financial service, it stands to reason that some party has provided that financial service."[11] Moreover, the Draft Updated Guidance states that the "…FATF does not seek to regulate the technology that underlies VAs or VASP activities, but rather the natural or legal persons behind such technology or software applications that facilitate financial activity…."[12] It also states that "each natural or legal person constituting the governance body could also be a VASP depending on the extent of the influence it may have."[13] All of these statements could be interpreted to include governance token holders, notwithstanding the prerequisite that a VASP conducts the listed activities for or on behalf of another natural or legal person.

Designating any governance token holder of a decentralized software program as a VASP would obligate them to implement associated AML/CFT controls for the program. In practice, this obligation would be impossible for governance token holders of a decentralized and non-custodial system to implement. First, decentralized governance prevents any individual actor from changing the parameters of the program. As such, compliance with a VASP designation would not lead to the implementation of KYC and/or other AML/CFT programs across decentralized software programs that provision financial services (which would also necessarily be centralized). Instead, law abiding governance token holders, appreciating they could not unilaterally implement or comply with the obligations required of VASPs, would have to divest in order to comply with the law.

As a consequence, governance of decentralized financial protocols would either be left to illicit actors unwilling to comply with the law, or governance would be totally eliminated. Neither

[10] FATF, "Draft Updated Guidance," 21.

[11] Id., 29.

[12] Id., 26.

[13] Id., 27.

outcome is ideal. As law-abiding individuals could still use decentralized financial protocols, they would either be exposed to protocols governed totally by illicit actors or completely autonomous protocols. An "ungovernable" protocol would undermine other policy priorities such as consumer protection. For example, security vulnerabilities are routinely discovered in decentralized financial protocols, and governance token holders can vote to implement patches to remove them. Indeed, some protocols reward individuals who discover vulnerabilities in their code, akin to a "bug bounty." Thus, the lack of active governance, or governance dominated by illicit actors, would expose users to higher risk of fraud, theft, and manipulation.

2. Software developers

We applaud FATF's exclusion of software developers from the definition of VASPs in the Draft Updated Guidance "...when solely developing or selling the application or platform."[14] However, several passages clearly implicate software developers, including those not using "...the new application or platform to engage as a business..."[15] in the listed activities for or on behalf of another person. For example, the Draft Updated Guidance states that regulators should ascertain, among other things, "who generated and drove the creation and launch of a product or service"[16] in determining which entities should be designated as VASPs. It further states that

> **launching a service that will provide VASP services**, for instance, does not relieve a provider of VASP obligations, **even if those functions will proceed automatically** in the future, especially **but not exclusively** if the provider will continue to collect fees or realize profits, regardless of whether the profits are direct gains or indirect. The use of an automated process such as a smart contract to carry out VASP functions does not relieve the controlling party of responsibility for VASP obligations. For purposes of determining VASP status, **launching a self-propelling infrastructure to offer VASP services is the same as offering them**, and similarly commissioning others to build the elements of an infrastructure, is the same as building them.[17]

The Draft Updated Guidance seems to imply that a software developer that publishes completely autonomous and open-source code that could be used to provide a financial service could be considered a VASP, even when that developer has no ongoing control over the program and does not profit directly or indirectly from the use of the program. This policy would seek to regulate individuals and entities *solely* publishing certain computer programs that can be used to engage in financial transactions. Indeed, how could developers of autonomous, open-source code implement AML/CFT controls across a protocol that is no longer under their control and can be copied and used by anyone with an internet connection? They could not.

---

[14] FATF, "Draft Updated Guidance," 26.

[15] Ibid.

[16] Id., 30.

[17] Ibid (emphasis added).

While the Draft Updated Guidance seems to imply that member states should regulate *ex-ante* natural or legal persons who launch a decentralized financial protocol, implementing such a policy may prove difficult in jurisdictions such as the United States, which has strong free speech protections. Moreover, *ex-ante* regulation of natural or legal persons who launch software protocols would be difficult to enforce in practice, as launching self-propelling infrastructure to offer VASP services is nearly costless for anyone with an internet connection. Moreover, if the FATF seeks to include entities in the VASP definition that do not collect fees or derive profits directly or indirectly from the provision of a disintermediated financial service ("but not exclusively"), it should clarify this intent. In most contexts, the generation of profits is generally understood to be the central function of entities acting "as a business," which is a prerequisite to be a VASP under the FATF Glossary's definition, irrespective of which limb may apply to a person's specific activities.[18]

3. Non-custodial entities

The Draft Updated Guidance abandons the existing Guidance's recognition that regulations designed for custodial financial intermediaries should only apply to custodial financial intermediaries. For example, the existing text of the Guidance (removed from the Draft Updated Guidance) states that

> countries should consider whether the [potential VASP] activities involve a **natural or legal person** that conducts **as a business** the five functional activities described **for or on behalf of** another natural or legal person, both of which are **essential elements** to the definition and **the latter of which implies a certain level of 'custody' or 'control' of the virtual asset, or 'ability to actively facilitate the financial activity' on the part of the natural or legal person that conducts the business for a customer**.[19]

The existing Guidance (removed from the Draft Updated Guidance) further states that, when discussing the "safekeeping and/or administration" prong of the VASP definition,

> countries should account for services or business models that combine the function of safeguarding the value of a customer's VAs with the **power to manage or transmit the VAs independently from the owner**...

and that these

> services include persons that have **exclusive or independent control of the private key** associated with VAs belonging to another person or **exclusive and**

[18] FATF, "Draft Updated Guidance," 22.

[19] Id., 30 (emphasis added).

independent control of smart contracts to which they are not a party that involve VAs belonging to another person.[20]

Expanding the application of financial surveillance requirements beyond custodial financial intermediaries is not a difference in degree but a difference in kind, and it contradicts existing guidance issued by member countries, like the United States, and relied upon by industry participants.[21] Indeed, non-custodial decentralized financial protocols cannot establish existing AML/CFT controls because they would have to centralize in order to permission access to the system, and non-custodial entities cannot comply with requirements that assume the regulated entity has custody of another natural or legal person's assets, such as asset freezes. Moreover, non-custodial businesses like hardware wallet providers merely provide a "tool" with which individuals secure the keys to their own assets; these wallets, like a home safe manufacturer, simply allow individuals to safely retain total independent control of their assets. Additionally, it should be underscored that even the perfect implementation of these requirements would not address illicit actors' access to and use of permissionless decentralized financial protocols.

4. Autonomous computer programs

Although the Draft Updated Guidance states that a software program "…is not a VASP under the FATF standards,"[22] it also states that "where the platform [i.e. the software program] facilitates the exchange, transfer, safekeeping or other financial activity involving VAs (as described in limbs (i)-(v) of the VASP definition), then the platform [i.e., the software program] is necessarily a VASP conducting exchange and/or transfer activity as a business on behalf of its

---

[20] FATF, "Draft Updated Guidance," 32 (emphasis added).

[21] *See, e.g.,* Financial Crimes Enforcement Network (FinCEN), "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies" (May 2019) available at https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.

"The regulatory interpretation of the BSA obligations of persons that act as **intermediaries between the owner of the value and the value itself** is not technology dependent. The regulatory treatment of such intermediaries depends on four criteria: (a) who owns the value; (b) where the value is stored; (c) whether the owner interacts directly with the payment system where the CVC runs; and, (d) whether the person **acting as intermediary** has **total independent control** over the value" (p. 15 (emphasis added)).

"If the multiple-signature wallet provider restricts its role to creating un-hosted wallets that require adding a second authorization key to the wallet owner's private key in order to validate and complete transactions, the provider is not a money transmitter because it does not accept and transmit value" (p. 17).

"Under FinCEN regulations, a person is exempt from money transmitter status if the person only provides the delivery, communication, or network access services used by a money transmitter to support money transmission services.72 72. 31 CFR § 1010.100(ff)(5)(ii)(A). Consistent with this exemption, if a CVC trading platform only provides a forum where buyers and sellers of CVC post their bids and offers (with or without automatic matching of counterparties), and the parties themselves settle any matched transactions through an outside venue (either through individual wallets or other wallets not hosted by the trading platform), the trading platform does not qualify as a money transmitter under FinCEN regulations" (p. 24).

[22] FATF, "Draft Updated Guidance," 23.

customers."[23] Computer programs that facilitate the exchange, transfer, safekeeping, or other financial activities involving VAs are not natural or legal persons and can be completely autonomous, free to use, and unchangeable. It is unclear how such a computer program "…is necessarily a VASP conducting exchange and/or transfer activity as a business on behalf of its customers."[24] As defined by the FATF, "a smart contract is a computer program or a protocol that is designed to automatically execute specific actions such as VA transfer between participants without the direct involvement of a third party when certain conditions are met."[25] Where no entities are involved in the provision of a financial service other than the "participants" and the "smart contract," it is unclear which actor the FATF intends to capture in the definition of a VASP and how that actor would implement VASP obligations.

* * *

The Draft Updated Guidance would also impose novel requirements on regulated VASPs to ascertain and record information about *individual* (non-FI) counterparties with which they have no relationship and who are transacting on their own behalf. While the Draft Updated Guidance notes that Recommendation 16 intends to manage wire transfers, defined "…as any transaction carried out on behalf of an originator *through a FI* by electronic means with a view to making an amount of funds available to a beneficiary person *at a beneficiary FI*…,"[26] it then proposes to apply Recommendation 16 to "…VA transfer[s] between a VASP and an unhosted wallet,"[27] i.e. individuals transacting on their own behalf without using a FI. In other words, the Draft Updated Guidance proposes to require VASPs to proactively collect and record information about their customers' *counterparties*—individuals with whom those financial institutions may have no relationship whatsoever. Making matters worse, VASPs would be required to record this information for all transactions, not just those above Recommendation 16's USD/EUR 1,000 *de minimis* threshold.[28] Moreover, the FATF specifically states that, in the context of transactions between VASPs and self-hosted wallets, countries should require VASPs to scrutinize those transactions for suspicious activity and sanctions compliance. In addition, FATF indicates that countries should also consider "requiring VASPs to treat such VA transfers as higher risk transactions that require enhanced scrutiny and limitations." The requirement to proactively collect information about individuals with which a FI has no relationship whatsoever represents a radical expansion of custodial financial intermediaries' AML/CFT obligations that "would

[23] FATF, "Draft Updated Guidance," 29.

[24] Ibid.

[25] Id., 17.

[26] Id., 51-52.

[27] Id., 52.

[28] Id., 56.

transform a regulatory regime designed to prevent financial institutions from using privacy as a shield for complicity in their customers' illicit activity into a tool of general surveillance."[29]

It is also unclear how VASPs would implement the requirement. There are no existing precedents or mechanisms for VASPs to obtain the information the Draft Updated Guidance would require about customers' counterparties. A threshold problem with the Draft Updated Guidance's customer counterparty identification requirement is that associating cryptocurrency wallets' public addresses with individual users may be both impractical and of limited utility at the scale the FATF envisions. As the Securities and Exchange Commission (SEC) has explained, an individual or entity "may not be able to demonstrate that no other party has a copy of the private key and could transfer the [associated] digital asset[s]…."[30] In other words, the fact that one individual (or hypothetically "identified" counterparty) has access to a private key associated with a certain cryptocurrency address does not mean that the individual exercises *exclusive* control over the associated digital assets. Just as a FI would be unable to reasonably determine that a person in possession of a physical wallet has ongoing exclusive control and ownership of the cash stored in it, it is impossible to determine at scale whether a cryptocurrency private key is under the exclusive control and ownership of the person using that key.

Compounding that problem, the Draft Updated Guidance fails to clearly define the types of transactions subject to additional requirements. The Draft Updated Guidance only addresses "VA transfer[s] to/from unhosted wallets,"[31] but that type of transaction accounts for a small and decreasing amount of total activity on public blockchains. Much of the innovation taking place in the ecosystem involves software protocols that allow users to engage in a broad range of economic activities without the need to rely on custodial intermediaries. For example, transactions can occur between a hosted wallet and a "smart contract," a self-executing software protocol that has no information to record and transmit. The Draft Updated Guidance does not reflect the technical possibility that the recipient of a cryptocurrency transaction could be a software program rather than an individual or business.

* * *

To develop an effective regulatory system that addresses ML/FT risks in the decentralized finance ecosystem while also preserving the enormous benefits that it offers, regulators and industry stakeholders must develop a new approach that matches the space that is being regulated. If regulators and stakeholders are to truly and effectively mitigate the ML/TF risks

---

[29] Jaikumar Ramaswamy, "Comment on FR Doc #2020-28437" (January 4, 2021), *available at*: https://www.regulations.gov/comment/FINCEN-2020-0020-6556.

[30] U.S. Securities and Exchange Commission, "Joint Staff Statement on Broker-Dealer Custody of Digital Asset Securities" (July 8, 2019), *available at* https://www.sec.gov/news/public-statement/joint-staff-statement-broker-dealer-custody-digital-asset-securities.

[31] FATF, "Draft Updated Guidance," 60.

associated with this novel ecosystem, they cannot depend on regulating “gatekeepers” in a system designed to function without them.

Instead of trying to regulate an intermediary that does not exist or forcing new projects to function like pre-existing, easily regulatable forms, a more effective approach is to concentrate efforts on the development and consensus-based adoption of new regulatory mechanisms that can be incorporated into decentralized finance protocols. Because of the nascence of the ecosystem, a regulatory mechanism of this kind has not yet been developed. Several projects with this aim in mind are currently in development, but they need to be refined, supported, and incentivized, which takes time. To that end, the Blockchain Association respectfully requests the FATF delay consideration of the Draft Updated Guidance until 2022 so that a solution can be developed in collaboration with regulatory bodies and tested in blockchain and cryptocurrency ecosystems. The seeds of a successful regulatory framework that effectively mitigates the ML/TF risks associated with decentralized finance are present. It is now up to industry stakeholders and regulators to provide these potential solutions with the nourishment and incentive they need to fully grow and develop.

Critically, for any solution to be useful, they would have to be adopted by decentralized financial protocols. In this manner, the most critical question is how to incentivize as many decentralized financial protocols as possible to adopt solutions that are developed. As explained throughout this document, decentralized governance limits the viability of coercing the adoption of any potential solution, and the open source code that powers them can always be redeployed excluding restrictions. It should be noted that any potential solution will not be a panacea. Supporting law enforcement efforts to police and respond to illicit activity in the decentralized financial ecosystem must also form a core element of any effective framework. Law enforcement has already implemented tools that leverage transparent blockchains to disrupt illicit activity in the decentralized financial ecosystem. Further equipping and resourcing law enforcement to broadly adopt these tools, and to develop new ones, will be critical.

As part of its efforts to facilitate a constructive dialog with regulators, the Association has created an in-house working group to coordinate with domestic and international regulators aimed at (1) exploring these potential solutions, (2) identifying the most promising, and (3) incentivizing the rapid development and implementation of them. The Association believes that no existing AML/CFT regime can effectively mitigate potential ML/FT risks in decentralized finance. Developing a new way is our only viable option and the Association stands ready to marshal the collective contributions of its membership to partner with FATF in meeting this challenge.

Sincerely,

Kristin Smith
Executive Director