ICLE International Center for Law & Economics

Comments of the International Center for Law & Economics, 'Ensuring Responsible Development of Digital Assets'

Docket No. TREAS-DO-2022-0018

Submitted: November 3, 2022

Authored by:

Mikołaj Barczentewicz (Senior Scholar, International Center for Law & Economics)

Comments of the International Center for Law & Economics, Docket No. TREAS-DO-2022-0018

November 2022

Mikołaj Barczentewicz[*]

I. Introduction

We thank the U.S. Treasury Department for the opportunity to participate in this Request for Comment on "Ensuring Responsible Development of Digital Assets."[1] Our response most directly addresses part "B" of the Request for Comments, focusing particularly on the following questions:

- "What additional steps should the United States government take to more effectively deter, detect, and disrupt the misuse of digital assets and digital asset service providers by criminals?" (B1)
- "Are there specific areas related to AML/CFT and sanctions obligations with respect to digital assets that require additional clarity?" (B2)
- "What additional steps should the U.S. government consider to address the illicit finance risks related to mixers and other anonymity-enhancing technologies?" (B7)
- "What steps should the U.S. government take to effectively mitigate the illicit finance risks related to DeFi?" (B8)

Agencies whose primary function is law enforcement are chiefly concerned with the effectiveness of that mission and may not have the resources to properly consider the costs of actions that appear to promise effectiveness. We thus welcome the whole-of-government approach to the responsible development of digital assets adopted in Executive Order 14067, which invites a rigorous assessment of costs and benefits across various policy objectives.[2] The principal policy objectives set out in the Executive Order cover both law-enforcement and national-security concerns, while supporting technological advances and promoting access to safe and affordable financial services. Given the Order's broad scope, some ways of pursuing its diverse policy objectives may be in tension. Our aim in this response is to shed light on two important areas of such tension.

[*] Mikołaj Barczentewicz is a senior scholar with the International Center for Law & Economics (ICLE). He is also a senior lecturer in law and the research director of the Law and Technology Hub at the University of Surrey.

[1] *Ensuring Responsible Development of Digital Assets; Request for Comment*, TREAS-DO-2022-0018-0001, 87 FR 57556, U.S. DEP'T OF THE TREASURY (Sep. 20, 2022), https://www.federalregister.gov/d/2022-20279.

[2] *Executive Order on Ensuring Responsible Development of Digital Assets*, WHITE HOUSE (Mar. 9, 2022), https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets (hereinafter, "Executive Order").

First, policymakers must determine which entities in the crypto ecosystem are the most appropriate targets for law-enforcement and national-security efforts. We suggest that the costs of targeting crypto's infrastructural or "base" layer may to a disproportionate extent impede the attainment of other policy objectives.

Second, it is important to determine the appropriate policy response to privacy-enhancing crypto technologies. As Treasury seeks to forward the goals of consumer and investor protection, promotion of access to finance, support of technological advances, and reinforcement of U.S. leadership, all point in favor of facilitating responsible use of privacy-enhancing technologies, including so-called "privacy coins."

II. Targeting the 'Base Layer'

Crypto's "base layer" is in some important ways analogous to the basic infrastructure of the Internet and of traditional finance. We understand the base layer to include:

- The "infrastructural" participants of blockchain networks—*e.g.*, miners, validators, and node operators;[3] and
- Service providers that directly serve the former—*e.g.*, private relay operators like Flashbots and specialized node-hosting services[4] like Infura, Alchemy, or even Google.[5]

One approach to prevent and counteract undesirable activity "on top" of crypto's infrastructure layer would be to lay legal duties on base-layer participants to mitigate such activity, particularly where they may, in even some remote sense, have facilitated it. This approach will often be inappropriate, however, either because it is bound to be ineffective or because it will impose disproportionate costs relative to its benefits.

Infrastructural participants of blockchain networks are not often in the best position to apply rules like anti-money-laundering ("AML") and combating-the-financing-of-terrorism ("CFT") obligations because they do not have direct relationships with end users. They therefore do not possess the information needed and, even if they do act, cannot offer redress to the affected users. Moreover, in open networks like Ethereum and Bitcoin, imposing legal duties on U.S.-based actors (*e.g.*, miners

[3] Mikolaj Barczentewicz, *Base Layer Regulation*, REGULATION OF CRYPTO-FINANCE, https://cryptofinreg.org/projects/base-layer-regulation. Some operators (*e.g.*, Infura) act both as infrastructural network participants in their own right (*e.g.*, as node operators) and also offer services to infrastructural participants.

[4] *Id.*

[5] Amit Zavery & James Tromans, *Introducing Blockchain Node Engine: Fully Managed Node-Hosting for Web3 Development*, GOOGLE CLOUD (Oct. 27, 2022), https://cloud.google.com/blog/products/infrastructure-modernization/introducing-blockchain-node-engine.

or validators) is very likely to be ineffective, as many network participants will be located in other jurisdictions. Finally, some base-layer participants may simply find it impossible to comply with some legal duties, which could prompt them to leave U.S. jurisdiction.

Recent enforcement actions arising from the strict-liability duty not to facilitate transactions with entities sanctioned by the U.S. Treasury Department help to illustrate the concerns that attend imposing such duties on base-layer participants. In August 2022, a number of Ethereum addresses deployed by Tornado Cash were added to the Specially Designated Nationals and Blocked Persons List ("SDN").[6] Following this designation—out of an abundance of caution and adopting an expansive interpretation of the law—some base-layer participants of Ethereum (validators, block builders, proposers, and relay operators) began to filter out transactions that interacted with SDN-listed Ethereum addresses, so that they would not contribute to including those transactions on the blockchain. While it appears that a fairly large segment of the base layer joined in this effort, it has been—and will very likely remain—ineffective at stopping transactions with sanctioned entities from being included on the blockchain.

One reason the filtering effort has been ineffective is that it was focused on blockchain addresses, which is what base-layer participants have access to. But sanctioned entities can create new addresses and use other methods to obfuscate their identities in transactions. The scope of filtering could theoretically be broadened, also using on-chain analysis, but this would likely be overinclusive.[7] It would therefore threaten to harm other users; potentially leave filtering base-layer operators less competitive than non-filtering ones; and likely hasten the development of changes to Ethereum to bypass such filtering.

There are, to be sure, examples of situations where it would be difficult to use a new address to circumvent filtering. Some designated blockchain addresses (*e.g.*, the addresses of autonomous smart contracts deployed by Tornado Cash) are not controlled by anyone and thus cannot "move" to new addresses on their own. But even where a smart contract is autonomous, its original deployers—or, in the case of open-source code, anyone—could copy the code and deploy a new smart contract that would perform the same functions as the original. The need to redeploy smart contracts to new addresses often would create significant friction and costs for all who relied on the original smart

[6] *U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash*, U.S. DEP'T OF THE TREASURY (Aug. 8, 2022), https://home.treasury.gov/news/press-releases/jy0916.

[7] @ElBarto_Crypto, Twitter (Aug. 13, 2022, 8:21 AM), https://twitter.com/ElBarto_Crypto/status/1558428428763815942 ("[W]hile only 0.03% of addresses received ETH from tornado cash, almost half the entire ETH network is only two hops from a tornado cash receiver.").

contract, but as we will note in a moment, there are also cases where redeployment may not be necessary.

Even if the scope of filtering is broadened, one reason that filtering efforts may remain ineffective is that even a relatively small number of validators—including those located outside the United States—can ensure that any transaction be included on the blockchain, albeit with some delay. The extent of that delay will be proportionate to how many non-filtering validators there are among the universe of all validators. Importantly, the Ethereum addresses included on the Tornado Cash SDN list largely do not represent the kinds of smart contracts that require rapid communication.[8]

With more time-sensitive transactions—*e.g.*, smart contracts used to liquidate on-chain collateral—delays could significantly affect utility. In cases where such delays could harm users, there would be a strong incentive to swiftly redeploy contracts to new addresses. Moreover, were the addresses of such time-sensitive smart contracts ever included on the SDN list, it would likely prompt changes to the Ethereum protocol to render base-layer filtering impossible. Indeed, development work in this direction was already underway prior to the Tornado Cash designation and may have accelerated in its aftermath. The proposed changes would involve the introduction of privacy-enhancing solutions to Ethereum, which we will discuss in the next section.

Here, we wish to focus on what these technical changes could mean for U.S. sanctions law if a determination is made that it is, indeed, illegal (on a strict-liability basis, *i.e.*, irrespective of intent) for a U.S.-based Ethereum validator to propose (or perhaps even "attest to") a block containing transactions with sanctioned entities.[9] If changes to the Ethereum protocol render the contents of transactions hidden from validators, then those validators could never be certain that they are in compliance with the prohibitions. This would effectively force validators (and other base-layer operators) to leave the United States. Ethereum would likely continue to function and remain accessible to U.S.-based users, but the technological and economic position that the United States currently holds in the base layer of the ecosystem would be diminished significantly.

To this point, our comments have concerned targeting the base layer for undesirable activity that happens "on top" of it—*i.e.*, for facilitating the actions of others. It is, however, also possible for base-layer participants to engage in illicit activity in their own right. In such cases, it would certainly be appropriate that they be a target of law enforcement. For example, node operators could use their

[8] All but one designated Ethereum addresses deployed by Tornado Cash represent smart contracts, but the SDN list also includes Ethereum addresses that do not represent smart contracts, which are associated with other sanctioned entities.

[9] For an argument that it is not illegal, *see* Rodrigo Seira, Amy Aixi Zhang, & Dan Robinson, *Base Layer Neutrality: Sanctions and Censorship Implications for Blockchain Infrastructure*, PARADIGM (Sep. 8, 2022), https://www.paradigm.xyz/2022/09/base-layer-neutrality.

privileged access to private information about pending securities or commodities transactions in ways that would constitute market manipulation under the Securities Exchange Act or the Commodity Exchange Act.[10] Validators could also engage in potentially illegal market manipulation through some forms of "MEV extraction."[11]

An alternative to targeting the base layer is to target the application layer—*i.e.*, services built on top of the base layer, with the primary function of interacting with end users.[12] Of particular interest in this space are services that intermediate between crypto assets and the rest of the financial system—*i.e.*, "on-ramps" and "off-ramps."[13] Due to their user-facing role, such services tend to already possess—and can more easily acquire—information needed for effective compliance with legal obligations related to user activity, such as AML/CFT and sanctions obligations. Because these services have direct relationships with users, they also can ask for additional information and provide redress opportunities in certain cases—*e.g.*, where a user is mistakenly flagged as high risk by automated tools. Moreover, crypto on- and off-ramps have been regulated as money transmitters or under analogous regulatory regimes in certain other jurisdictions.[14]

Targeting the base layer of permissionless blockchain networks may have symbolic value, but it is unlikely to achieve genuine law-enforcement or national-security goals. Imposing rules with which it would be impossible for base-layer operators to comply will simply push those operators to other jurisdictions. More effective targeting of the base layer is possible in permissioned blockchain networks, but requiring blockchain networks to be permissioned would run counter to the goal of reinforcing U.S. financial and economic leadership. It would amount to giving up on the promise of permissionless blockchains like Ethereum and Bitcoin. Finally, targeting the base layer is unnecessary, as the application layer presents a more appropriate target for legal obligations.

[10] Mikolaj Barczentewicz & Anton Wahrstätter, *How Transparent Is Ethereum and What Could This Mean for Regulation?*, REGULATION OF CRYPTO-FINANCE, https://cryptofinreg.org/projects/public-data-supervision.

[11] Mikolaj Barczentewicz & Alexander F. Sarch, *Shedding Light in the Dark Forest: A Theory of Liability for Cryptocurrency "MEV" Sandwich Attacks*, available at SSRN (Oct. 5, 2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4187752.

[12] Autonomous smart contracts that do not rely on off-chain cooperation and also are not controlled are not part of the application layer, as we understand it here. From the perspective of asserting legal control, they are functionally part of the base layer (*e.g.*, to "remove" such a smart contract from the blockchain, it would require the cooperation of an overwhelming majority of validators). Also, strictly speaking, end users may also interact with some base-layer participants, *e.g.*, by submitting transactions directly to a node's remote-procedure-calls (RPC) interface.

[13] *See also* Miles Jennings, *Regulate Web3 Apps, Not Protocols*, A16Z (Sep. 29, 2022), https://a16zcrypto.com/web3-regulation-apps-not-protocols.

[14] *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*, FINANCIAL CRIMES ENFORCEMENT NETWORK (May 9, 2019), https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-certain-business-models.

Recommendation addressing 'specific areas related to AML/CFT and sanctions obligations with respect to digital assets that require additional clarity' (RFC question B2)

As we note above, base-layer efforts to filter transactions with sanctioned entities are currently ineffective and are likely to become impossible, given in-progress technological developments. We also noted that the application layer is the more appropriate target for sanctions law. The primary effect of the prevailing uncertainty surrounding the potential legal exposure of base-layer participants of public blockchains like Ethereum and Bitcoin has been to threaten U.S. technological and economic leadership in digital assets.

The U.S. Treasury Department's Office of Foreign Assets Control ("OFAC") could address this uncertainty by offering a public statement—perhaps in its sanctions FAQs—that it does not regard any of the following as the prohibited facilitation of a transaction with a designated entity, either on public blockchains in general or, at least, on Ethereum and Bitcoin:

1. To include such a transaction in a block, by mining or validating ("proposing");
2. To accept such a transaction and the block in which it was included as valid for the purposes of adding new blocks referencing the first block; or
3. To receive and retransmit such a transaction for inclusion by potential miners or validators (*e.g.*, by a node, a block builder, or a relay).

We stress that this issue is independent from any evaluation of either the propriety or legality of sanctioning any particular entity, or of the inclusion of addresses of autonomous smart contracts on the SDN list.[15]

III. Privacy-Enhancing Technologies

Ethereum and Bitcoin—the most widely used public blockchains—were not designed with user privacy in mind. Pseudonymity of blockchain addresses is easily broken, for example, whenever a user discloses their identity to make a purchase. The effect of breaking pseudonymity is that the other party will likely be able to discover the entirety of that user's past activity on the blockchain. It is akin to a user giving someone access to their entire history of bank or credit-card transactions. The

[15] There has been some controversy regarding the legality of sanctioning the autonomous smart contracts deployed by Tornado Cash. *See* Paul Grewal, *Sanctions Should Target Bad Actors. Not Technology.*, COINBASE (Sep. 8, 2022), https://www.coinbase.com/blog/sanctions-should-target-bad-actors-not-technology; Jerry Brito & Peter Van Valkenburgh, *Coin Center Is Suing OFAC Over Its Tornado Cash Sanction*, COINCENTER (Oct. 12, 2022), https://www.coincenter.org/coin-center-is-suing-ofac-over-its-tornado-cash-sanction; Steve Engel & Brian Kulp, *OFAC Cannot Shut Down Open-Source Software*, DECHERT LLP (Oct. 18, 2022), https://ipfs.io/ipfs/QmTC9q5yidSWoM2HZwyTwB3VbQLVbG5cpDSBTaLP8voYNX.

risk of so massive a breach of financial privacy—potentially exposing users to targeting by thieves and fraudsters—is inimical to the goal of "access to safe and affordable financial services" that President Biden set out in Executive Order 14067.[16]

The lack of privacy on blockchains like Ethereum and Bitcoin has proven convenient for law enforcement, who have leveraged it to prosecute crimes.[17] But it would be mistaken to regard the current level of transparency as a benchmark either for "responsible" public blockchains or for services built atop them. Safe and accessible public blockchains of the near future—including planned changes to Ethereum—will not offer the same transparency on which today's criminals and law enforcement alike rely.

It is useful to examine the now-sanctioned Tornado Cash within this context. Tornado Cash was arguably the most effective "on-chain" tool to protect user privacy.[18] For some use cases, users can enjoy similar privacy-protecting effects by routing their transactions through regulated exchanges like Coinbase, FTX, or Binance, but this comes at the expense of having to trust one of those third parties. The tradeoffs involved in going "off-chain" to achieve "on-chain" privacy include additional risk, friction, and delays, which could at least partially negate the point of using a public permissionless blockchain. If public blockchains are an innovation worth preserving and supporting, as the Executive Order implies, then a solution should be found that does not erase their primary salutary features.

Fortunately, there are technological solutions to preserve user privacy that simultaneously enable effective mitigation of illicit activity. One such solution is selective disclosure.[19] Even where the pseudonymous identifiers of senders and recipients—or the contents of a blockchain message (transaction)—are hidden, users may nonetheless be able to selectively disclose in a non-falsifiable way that,

[16] Executive Order, *supra* note 3, at Sec. 1; On cryptocurrencies' promise for financial inclusion, including in situations especially needing privacy (*e.g.*, domestic violence, authoritarian regimes), *see, e.g.*, Alex Gladstein, *Finding Financial Freedom in Afghanistan*, BITCOIN MAGAZINE (Aug. 26, 2021), https://bitcoinmagazine.com/culture/bitcoin-financial-freedom-in-afghanistan; Charlene Fadirepo, *Why Bitcoin Is a Tool for Social Justice*, COINDESK (Feb. 17, 2022), https://www.coindesk.com/layer2/2022/02/16/why-bitcoin-is-a-tool-for-social-justice; *How Cryptocurrency Meets Residents' Economic Needs in Sub-Saharan Africa*, CHAINANALYSIS (Sep. 29, 2022), https://blog.chainalysis.com/reports/sub-saharan-africa-cryptocurrency-geography-report-2022-preview.

[17] *See, e.g.*, Andy Greenberg, *Inside the Bitcoin Bust That Took Down the Web's Biggest Child Abuse Site*, WIRED (Apr. 7, 2022), https://www.wired.com/story/tracers-in-the-dark-welcome-to-video-crypto-anonymity-myth.

[18] For an explanation of Tornado Cash's functionality, *see* Alex Wade, Michael Lewellen, & Peter Van Valkenburgh, *How Does Tornado Cash Work?*, COINCENTER (Aug. 25, 2022) https://www.coincenter.org/education/advanced-topics/how-does-tornado-cash-work.

[19] *See also* Peter Van Valkenburgh, *Open Matters: Why Permissionless Blockchains Are Essential to the Future of the Internet*, COINCENTER (December 2016) https://www.coincenter.org/open-matters-why-permissionless-blockchains-are-essential-to-the-future-of-the-internet.

for example, they control the account from which a certain transaction was made. This would allow on- and off-ramp services between crypto-assets and the rest of the economy to serve as gatekeepers that perform appropriate AML/CFT or sanctions screening of customers who wish to exchange their "private coins" for fiat currency or other goods. To be sure, service providers and law enforcement would likely have access to less information under this sort of blockchain analysis than they do today, especially regarding the transactions of parties other than the customer in question (although service providers may have access to disclosed transactions from many customers). As we noted above, however, the current level of transparency poses a regrettable risk to user privacy and safety and thus cannot serve as a normative benchmark.

Tornado Cash, Zcash, and Monero all offer forms of selective disclosure.[20] While the transaction volume in these protocols is small relative to Ethereum or Bitcoin, it would be worthwhile to devote resources toward developing rules and guidance—especially for money transmitters and financial institutions—on how to facilitate transactions with those protocols responsibly. A pragmatic reason for this investment is that public blockchains and the services built on them are moving in the direction of increased privacy. Thus, the issue of privacy cannot be adequately addressed by blunt instruments like sanctioning an entire protocol, as happened with Tornado Cash. Even today, the hypothetical prohibition of Ethereum or Bitcoin would cause immense economic damage. Soon, such action could jeopardize the stability of the global economy.

As public blockchains grow, they will become more attractive both for lawful uses and for illicit uses. While illicit use may remain small as a percentage of total transactions, the volume of illicit transactions will likely rise in absolute numbers.[21] The anticipated improvements in crypto privacy will cause significant tension for the prevailing law-enforcement and national-security approaches to digital assets. In this context, Treasury's Digital Asset Action Plan may not be entirely adequate.[22]

It is, to start, puzzling why the Digital Asset Action Plan adopted the label "*anonymity*-enhancing technologies," rather the commonly used "*privacy*-enhancing technologies."[23] This focus on

[20] Zooko Wilcox & Paige Peterson, *The Encrypted Memo Field*, ELECTRIC COIN CO. (Dec. 5, 2016), https://electriccoin.co/blog/encrypted-memo-field; *View Key*, MONEROPEDIA, https://www.getmonero.org/resources/moneropedia/viewkey.html; Wade, Lewellen, & Van Valkenburgh, *supra* note 18.

[21] *Crypto Crime Trends for 2022: Illicit Transaction Activity Reaches All-Time High in Value, All-Time Low in Share of All Cryptocurrency Activity*, CHAINANALYSIS (Jan. 6, 2022), https://blog.chainalysis.com/reports/2022-crypto-crime-report-introduction.

[22] *Action Plan to Address Illicit Financing Risks of Digital Assets*, U.S. DEP'T OF THE TREASURY (Sep. 20, 2022), https://home.treasury.gov/system/files/136/Digital-Asset-Action-Plan.pdf.

[23] A query for "anonymity-enhancing technologies" in the Google Scholar database returns about 40 results, while a query for "privacy-enhancing technologies" returns more than 30,000 results. *See*

"anonymity" rather than "privacy" directs attention away from the tension among important policy objectives set out in Executive Order 14067. The importance of privacy and the aim to strengthen it (while also countering illicit activities) is mentioned 10 times in the Executive Order. Anonymity is not mentioned.

The Action Plan itself also refers to the goal of strengthening privacy several times. It is notable, however, that Priority Action 5 ("Holding Accountable Cybercriminals and Other Illicit Actors") does not. It is in this section that the Action Plan singles out "mixing services" as an area of "primary concern." Treasury's recent enforcement actions—notably the branding of Tornado Cash as a "notorious (…) mixer"[24]—suggest that the term "mixing services" is meant to refer to some of the popular privacy-enhancing technologies upon which both law-abiding Americans and foreign nationals alike have been relying.

In other words, rather than balancing the goals of strengthening privacy and mitigating illicit finance, as set out in the Executive Order, Priority Action 5 suggests a near-exclusive exclusive focus on the latter.[25] Furthermore, it is hard to avoid the impression that, in a further departure from the Executive Order, the Action Plan treats strengthening privacy as chiefly a research concern (and thus assigns it primarily to the National Science Foundation) and not an issue to be given considerable weight in law-enforcement or national-security missions.

Recommendation: 'additional steps the U.S. government should consider to address the illicit finance risks related to mixers and other anonymity-enhancing technologies' (RFC question B7)

Given the value of both preserving and strengthening financial privacy, as well as the pragmatic concern that the largest public blockchains are moving in the direction of greater privacy, we suggest that a more constructive law-enforcement approach is needed with respect to the already-deployed privacy-enhancing technologies. This approach could include reversing the designation of Tornado Cash, combined with offering guidance for money transmitters and financial institutions on how to approach transactions with tools like Tornado Cash in a responsible manner. These guidelines could rely, among other mechanisms, on selective-disclosure functionalities built into privacy-enhancing tools.

https://scholar.google.com/scholar?q=%22anonymity-enhancing+technologies%22 (accessed Oct. 28, 2022); https://scholar.google.com/scholar?q=%22privacy-enhancing+technologies%22 (accessed Oct. 28, 2022).

[24] U.S. Department of the Treasury, *supra* note 6.

[25] U.S. Department of the Treasury, *supra* note 22.