Exhibit A

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA, Plaintiff, v. ANTON PERAIRE-BUENO, and JAMES PERAIRE-BUENO, Defendants.	Case No. 1:24-cr-00293-JGLC

[PROPOSED] BRIEF FOR *AMICUS CURIAE* DEFI EDUCATION FUND IN SUPPORT OF DEFENDANTS' MOTION FOR JUDGMENT OF ACQUITTAL OR, ALTERNATIVELY, TO DISMISS THE SUPERSEDING INDICTMENT

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page

CASES

STATUTES

INTEREST OF *AMICUS CURIAE*[1]

DeFi Education Fund ("DEF") is a U.S.-based nonpartisan research and advocacy nonprofit that advocates for sound policy for decentralized finance ("DeFi"). DEF's mission includes advocating for the interests of DeFi users, participants, and software developers working to innovate using blockchain technology that is decentralized and open to all users. Among other things, DEF educates lawmakers and the public about DeFi, meets with members of Congress to discuss DeFi technology, and submits public comments on proposed rulemakings that impact DeFi. DEF also regularly files *amicus* briefs in court cases that raise legal issues of broad importance for DeFi.

DEF has a strong interest in ensuring that growth in DeFi is not stifled by prosecutions based on unprecedented legal theories of which software developers have no fair notice. DeFi offers substantial benefits to the public, including disintermediated low-cost, peer-to-peer financial transactions, cross-border payments, transparency, open access to finance, and the ability to self-custody funds. However, prosecutions like this one, in which the Department of Justice takes a novel view of existing law, threaten to hinder continued innovation in DeFi and push future DeFi investment abroad.

[1] No counsel for any party authored this brief in whole or in part, and no person or entity other than *amicus* and its counsel made a monetary contribution intended to fund the preparation or submission of this brief.

INTRODUCTION

This case represents an attempt to use a criminal prosecution to impose novel and retroactive rules about how DeFi software developers, and those in the Ethereum ecosystem, must conduct themselves. The Government does not contend that the Defendants violated any law, regulation, or other pre-existing rule that was enacted to set the bounds of criminal liability for software developers who create and use novel Ethereum technology. Instead, the Government claims that their development and use of the software at issue violated the federal wire fraud statute. The problem for the Government is that wire fraud traditionally requires the use of a material misrepresentation to obtain property. In an attempt to get around that requirement, the Government argues that Defendants *implicitly* made false representations about the way they would behave by serving as "validators" in the Ethereum ecosystem. But that baseless assertion is nothing more than a transparent attempt to reinterpret the wire fraud statute to target conduct related to new technologies.

This unprecedented approach lacks any basis in the text of the general wire fraud statute on which the Government relies, any federal or state regulations, or any prior prosecution addressing similar conduct. If the Government is allowed to proceed on this type of theory, then it can use "wire fraud" prosecutions to circumvent the legislative and regulatory process. Instead of passing a new law or regulation, prosecutors can simply assert that software developers who use innovative technologies implicitly agreed to follow whatever rules the Government later decides are appropriate. That is anathema to the rule of law.

This type of regulation by prosecution runs afoul of the fundamental Due Process principle that conduct cannot be criminally punished without fair notice that the conduct was unlawful. Under that well-established principle, if the Government seeks to impose criminal liability based on new theories about innovative technologies, it must do so by setting out clear

rules through lawmaking, not by prosecuting conduct after the fact. Here, since there was no prior law or regulation that set forth the rules of conduct that the Government says the Defendants were somehow implicitly bound to follow, they plainly did not have fair notice that they would be criminally prosecuted for failing to follow those made-up rules.

The Government's theory of how Ethereum validators should behave has no basis in law or the technology itself. Ethereum is a decentralized, trustless blockchain with no terms of use. It was first conceived of in 2013, and did not go live until 2015. Rather than imposing centralized rules, the Ethereum protocol relies on economic incentives to guide behavior, with the assumption that users and developers will act rationally to maximize their own profits according to the economic incentives built into the protocol itself.

"Validators" are a key part of the Ethereum blockchain's consensus mechanism. Validators propose "blocks" of transaction data to be added to the Ethereum blockchain and attest to the validity of the proposed blocks, helping to secure the network and ensure consensus. Anyone can become a validator by "staking" Ether (the currency used in the Ethereum ecosystem), and a participant is not required to agree to any rules or terms of use prior to becoming a validator. Instead, validators' conduct is guided by economic incentives and disincentives—potential profits and costs—imposed by the Ethereum protocol depending on the validators' actions. As with other Ethereum participants, validators are not expected to act as trusted intermediaries, but as self-interested actors responding rationally to economic consequences.

While the consequences of this unprecedented prosecution are obviously significant for the Peraire-Buenos, this case also has broader implications: prosecutions like this one bring ambiguity and fear to software developers, chilling participation in DeFi and driving participants

abroad. Congress is currently working on legislation related to blockchain technology and decentralized systems, and relevant agencies are working on related regulations, all of which would bring certainty and clarity to this growing portion of the economy by setting out clear and predictable rules.[2] The DOJ should not get ahead of prospective lawmaking by bringing indictments based on ill-fitting interpretations of existing law, which will stifle growth by sowing confusion about the governing rules. The Court can and should avoid this result by enforcing the traditional limits of criminal prosecutions consistent with Due Process.

ARGUMENT

In this case, the Government seeks to use the federal wire fraud statute to prosecute two software developers, the Peraire-Buenos, based on a novel strategy they executed to enhance their profits from acting as validators for the Ethereum blockchain. The Government does not claim that this strategy violated any express rules for Ethereum validators or that the Peraire-Buenos made any express representations to the alleged victims of this scheme. Instead, the Government's primary theory is that by acting as validators on the blockchain, the Peraire-Buenos implicitly represented that they would follow an amorphous, unwritten code of conduct that would make them "legitimate" validators. According to the Government, the failure to abide by that implied code of conduct amounted to wire fraud—even if the Peraire-Buenos never purported to subscribe to such a code of conduct or had any way of discerning its contours. That

[2] *See, e.g.*, *Senate Ag Releases Long-Awaited Crypto Bill Draft*, Politico (Nov. 10, 2025) (reporting that Senate Agriculture Committee unveiled a bipartisan draft of crypto market structure legislation aimed at clarifying regulatory frameworks for digital assets), *available at* https://www.politico.com/live-updates/2025/11/10/congress/senate-ag-releases-long-awaited-crypto-market-structure-draft-00641759; Paul S. Atkins, *The SEC's Approach to Digital Assets: Inside "Project Crypto"* (Nov. 12, 2025) (speech at the Federal Reserve Bank of Philadelphia, describing the SEC's plans to pursue an innovation exemption to allow for digital asset activities that do not fit neatly within existing rules), *available at* https://www.sec.gov/newsroom/speeches-statements/atkins-111225-secs-approach-digital-assets-inside-project-crypto.

theory of wire fraud is unprecedented, and prosecuting the Peraire-Buenos based on this theory not only violates their Due Process rights but poses a threat to all blockchain developers.

I. Due Process Requires the Government to Impose New Rules on Novel Technologies through Lawmaking, Not Prosecutions.

A. Due process requires fair notice that conduct can lead to criminal penalties.

To "creat[e] a new offense," the "terms of a penal statute . . . must be sufficiently explicit to inform those who are subject to it what conduct on their part will render them liable to its penalties." *Connally v. Gen. Const. Co.*, 269 U.S. 385, 391 (1926). If potential defendants are left to "guess" as to whether their conduct is criminal, applying the law to them "violates the first essential of due process of law." *Id.* "The underlying principle is that no man shall be held criminally responsible for conduct which he could not reasonably understand to be proscribed." *Bouie v. City of Columbia*, 378 U.S. 347, 351 (1964) (quoting *United States v. Harriss*, 347 U.S. 612, 617 (1954)).

The requirement of clarity in criminal law also "guards against arbitrary or discriminatory law enforcement by insisting that a statute provide standards to govern the actions of police officers, prosecutors, juries, and judges." *Sessions v. Dimaya*, 584 U.S. 148, 156 (2018). Allowing convictions based on statutes that are not clearly applicable, by contrast, "threaten[s] to hand responsibility for defining crimes to relatively unaccountable police, prosecutors, and judges, eroding the people's ability to oversee the creation of the laws they are expected to abide." *United States v. Davis*, 588 U.S. 445, 451 (2019). In short, for a prosecution to satisfy Due Process, "[t]he dividing line between what is lawful and unlawful cannot be left to conjecture." *Connally*, 269 U.S. at 393.

Based on these principles, "due process bars courts from applying a novel construction of a criminal statute to conduct that neither the statute nor any prior judicial decision has fairly

disclosed to be within its scope." *United States v. Lanier*, 520 U.S. 259, 266 (1997). Even prosecution under a statute that is "on its face . . . admirably narrow and precise" thus violates Due Process where the scope of the statute as interpreted by the Government "has been unforeseeably and retroactively expanded." *Bouie*, 378 U.S. at 351–52; *see also Pierce v. United States*, 314 U.S. 306 (1941) (The "enlargement of a criminal Act by interpretation is at war with a fundamental concept of the common law that crimes must be defined with appropriate definiteness.").

The Second Circuit's decision in *United States v. Matthews*, 787 F.2d 38 (2d Cir. 1986), is also instructive. There, the defendant was prosecuted for violating securities laws by failing to disclose in a proxy statement that he was guilty of a crime with which he had not been charged. *Id*. at 46. Although the relevant regulations made it a crime to "omit[] to state [in a proxy] any material fact necessary in order to make the statements therein not false or misleading," none of the regulations specifically required disclosure of uncharged criminal conduct, and the "extent of the obligation to disclose such information [was] uncertain in light of existing cases." *Id*. at 43, 46–48. *Amici* further confirmed that the prosecution went "beyond any precedent in requiring disclosure of unadjudicated and uncharged conduct," and the general "reaction of knowledgeable authorities" to the lawsuit reflected that the lawsuit represented a new enforcement approach. *Id*. at 49. Thus, the Second Circuit held, "at least so long as uncharged criminal conduct is not required to be disclosed by any rule lawfully promulgated by the SEC, nondisclosure of such conduct cannot be the basis of a criminal prosecution." *Id*.

B. Imposing novel duties on DeFi through prosecutions like this, rather than by statute or regulation, fails to provide sufficient notice and represents an end-run around the limited rules Congress has created that could be relevant to such conduct.

The prosecution in this case runs afoul of these well-settled principles of Due Process, as the Government seeks to reinterpret the wire fraud statute rather than punish conduct that was

clearly criminal under existing law at the time the Peraire-Buenos acted. Although the Government apparently believes that the Defendants' conduct violated the norms of how Ethereum validators should behave, it cannot point to any law or regulation that enacts such a norm into law. Instead, it tries to use the wire fraud statute to get around that problem by claiming that anyone who acts as an Ethereum validator *implicitly certifies* that they will comply with the Government's favored norms. That is an astonishing contention, and it amounts to a clear effort to impose new, retroactive rules on Ethereum software developers under the guise of the wire fraud statute. Because the Government's nebulous rules of conduct for software developers have never been written into any law or regulation—and they certainly are not apparent on the face of the wire fraud statute or any precedent interpreting that statute—nobody has ever had fair notice that violating these supposed rules would subject them to criminal liability. *See Bouie*, 378 U.S. at 351 (permitting criminal liability only if defendant could "reasonably understand" his conduct was proscribed).

The wire fraud statute is not a "catch-all law[] designed to punish all acts of wrongdoing or dishonorable practices." *United States v. Connolly*, 24 F.4th 821, 833–34 (2d Cir. 2022). Rather, it prohibits material misrepresentations that are used to obtain property with an intent to defraud. *Id*. In an attempt to show a material misrepresentation here, the Government does not primarily claim that the Defendants expressly said or did anything that was false. Instead, it argues that by serving as validators in the Ethereum ecosystem, they somehow *impliedly* represented that they would follow an unwritten code of conduct, and that they acted "fraudulently" by failing to do so.

Without binding rules, the Government's validator theory amounts only to a claim that the Defendants somehow behaved badly. But such a subjective standard cannot provide the "sufficiently explicit" guidance required in the criminal context to satisfy Due Process. *Connally*,

269 U.S. at 391. Indeed, even after this prosecution, Ethereum software developers are left to "guess" at what the outer bounds of permissible conduct are. Nor does allowing the Government to expand criminal liability in this way satisfy basic separation-of-powers principles—if the Government seeks to enforce a new code of conduct for novel technologies like Ethereum, it must do so through ordinary lawmaking, not ad hoc prosecutions. See *Davis*, 588 U.S. at 451.

The federal wire fraud statute cannot be read to give notice to would-be Ethereum validators of the conduct required to act as a "legitimate" validator, much less that deviations from that standard could be felonies. Nor can the Government point to any source, outside this prosecution, otherwise providing the requisite notice.[3] As in *Matthews*, then, "at least so long as [acting as a "legitimate" validator] is not required . . . by any rule lawfully promulgated" by Congress or appropriate regulators, failure to meet that standard "cannot be the basis of a criminal prosecution." 787 F.2d at 49.

The Government's attempt to analogize this case to "anti-spoofing" cases overlooks the critical difference between decentralized finance platforms like Ethereum and more traditional regulated commodity exchanges. In a regulated exchange, some courts have held that placing a trade as part of a scheme to influence a commodity price, with the secret intent to cancel that trade, can be fraudulent because it conveys "false and misleading information regarding supply or demand." *United States v. Chanu*, 40 F.4th 528, 533 (7th Cir. 2022). The critical point in those cases, however, is that regulated exchanges have clear, binding anti-spoofing rules that traders agree to follow as a condition of trading on the exchange. *See, e.g.*, *United States v. Smith*, 150

[3] Indeed, as in *Matthews*, "knowledgeable authorities"—including the founder of Ethereum—have "questioned the wisdom" of the prosecution. *Compare Matthews*, 787 F.2d at 45 & n.4, with Vitalik Buretin (@VitalikBuretin), X (Nov. 4, 2025, at 5:13am) (noting that if the "code is law," then both the alleged victims and the defendants "are playing a fair game" and that he is "glad [the prosecution]'s being challenged").

F.4th 832, 840 (7th Cir. 2025) (relying on binding exchange rules "prohibit[ing] traders from manipulating or attempting to manipulate prices of exchange futures or options contracts," along with an express employer policy "prohibiting spoofing") (internal quotation marks omitted); *United States v. Bases*, 2022 WL 3586142, at *3 (N.D. Ill. Aug. 22, 2022) (binding exchange rules "required that any order placed on the exchange represented a genuine, bona fide intent to trade at the specified quantity and price"). In that context, when a person has agreed to be bound by rules that require trades to be placed in good faith, the act of placing a trade represents that the trader is not engaging in spoofing (i.e., does not intend to cancel the trade as part of a scheme to manipulate the commodity price).

By contrast, on a decentralized network like Ethereum, there are no such binding rules that software developers must agree to as a condition of engaging in transactions or serving as validators. Instead, the Ethereum blockchain has certain protocols that automatically allow transactions to take place under certain conditions, and that programmatically govern how validators may respond when a new block is proposed for validation. There are no binding rules that require validators to choose one course or another; and there certainly are no existing laws or guidance that gave the Defendants notice that what they did here would amount to wire fraud.[4]

To be sure, just because wire fraud is an old concept, that does not mean it could never be applied in a case involving a novel technology like Ethereum. There may be cases where the facts giving rise to a traditional wire fraud charge have some connection to blockchain technology—a bad actor can fraudulently convince a victim to hand over control of a digital wallet in exactly the

[4] To the extent the Government argues that protocol specifications about validator behavior and the slashing penalty applicable to certain validator conduct combine to provide some guidance about what behavior is acceptable or at least encouraged, these purported sources of norms are too vague and amorphous to serve the same functions as rules or regulations enforceable by criminal law.

same ways he could convince a victim to initiate a bank transfer or hand over a physical wallet filled with cash. Selling oceanfront property in Arizona is fraudulent whether the purchaser pays using a traditional bank or Ether, and prosecution under the wire fraud statute may well be appropriate in such cases. But what the wire fraud statute does not do—and what the Government is plainly trying to use it for in this case—is to impose a novel and unwritten code of conduct based on the Government's assertion of how people in new industries *should* behave, without any basis in any binding rule that existed before the conduct at issue took place. This reinterpretation of law without notice violates Due Process principles.

C. Wire fraud should not be used to circumvent the limits on the CFAA

If this type of prosecution were going to be brought at all under existing law, it would have to be brought under the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030. "Congress enacted the CFAA in 1984 to address 'computer crime.'" *United States v. Valle*, 807 F.3d 508, 525 (2d Cir. 2015). The CFAA prohibits, among other things, "intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby "obtain[ing] . . . information from any protected computer." 18 U.S.C. § 1030(a)(2). "[B]ecause 'protected computer' is defined as a computer affected by or involved in interstate commerce," it includes "effectively all computers with Internet access." *Valle*, 807 F.3d at 528 (quoting *United States v. Nosal*, 676 F.3d 854, 858 (9th Cir. 2012)).

Of course, the CFAA itself has significant limitations that would be difficult to satisfy here—which likely explains why the Government chose not to proceed under that statute despite its theory that the Peraire-Buenos wrongly obtained information by using their computer software to obtain an "unblinded" version of a potential block to be added to the blockchain. For example, to establish a violation under Section 1030(a)(2), the Government would be required to prove that the Peraire-Buenos had accessed information from a protected computer without authorization or

in a way that exceeded their "authorized access." The Supreme Court has held that proof of the latter turns not on the purposes for which information is accessed or the use to which the information is put, but on whether the defendant had authorization to access the information for *any* purpose. *Van Buren v. United States*, 593 U.S. 374, 396 (2021).

Notably, before the Supreme Court decided *Van Buren*, the Second Circuit reached the same conclusion, rejecting the Government's broader interpretation based on many of the same concerns raised by this case. The court held that the CFAA did not criminalize every violation of computer usage policy, but had to be read more narrowly due to the rule of lenity, which "ensures that criminal statutes will provide fair warning of what constitutes criminal conduct, minimizes the risk of selective or arbitrary enforcement, and strikes the appropriate balance between the legislature and the court in defining criminal liability." *Valle*, 807 F.3d at 523.[5]

The Government should not be permitted to achieve an end-run around these limitations by adopting an even more expansive interpretation of the federal wire fraud statute here. After all, if Congress concludes that the prohibitions of the CFAA are too narrow, it is free to amend that statute to encompass other types of misconduct—or to pass new laws to address the new problems it sees.

In fact, the reasoning relied on in *Van Buren* (and *Valle*) applies with even more force in this case. In both *Van Buren* and *Valle*, as in this case, the defendants used a computer system in a manner that was clearly enabled by the system itself. In both cases, the prosecution sought to

[5] Moreover, a first-time conviction for violation of the relevant provisions of the CFAA generally carries a maximum sentence of "imprisonment for not more than 5 years" when motivated by financial gain, 18 U.S.C. § 1030(c)(2)(C), a punishment far shorter than the sentence of up to 20 years generally authorized by the federal wire fraud statute. 18 U.S.C. § 1343. Even if the Peraire-Buenos could have been on notice of potential CFAA charges, then, charging them under the wire fraud statute significantly raised the potential penalty, itself a significant Due Process problem.

impose criminal penalties based on allegations that in doing so, the defendants violated external norms about how the defendants were *supposed* to use those systems. In *Van Buren*, those external norms were far more clearly defined than they are in the present case: the defendant in *Van Buren* had searched a law-enforcement database for personal purposes after receiving training expressly prohibiting such use, and he "knew the search breached department policy." *Van Buren*, 593 U.S. at 380. The same was true in *Valle*, as "the NYPD's policy, known to Valle, was that the[] databases could only be accessed in the course of an officer's official duties and that accessing them for personal use violated Department rules." *United States v. Valle*, 807 F.3d 508, 513 (2d Cir. 2015)). But the fact that the defendants had clear notice that their actions violated a relevant *policy* was still not enough to put them on notice that they had violated any *criminal law*. Here, of course, the Peraire-Buenos' conduct did not even violate any clearly established policy, and the lack of notice of a criminal violation is all the more clear.

II. The Government's Approach Risks Chilling Participation in Software Development in the Blockchain Space.

In addition to violating Due Process with respect to the Peraire-Buenos, this prosecution also threatens more broadly to chill participation in software development in the blockchain space. There is no centralized authority in the Ethereum ecosystem that prescribes a code of conduct or otherwise provides a set of rules by which software developers or technology innovators must abide. Instead, to pursue its case here, the Government was forced to rely on evidence supposedly establishing the intent of third-party software developers or the unspoken expectations of market participants in attempting to define the boundaries between permissible and impermissible conduct. Under that approach, though, no Ethereum developer—or blockchain developer more broadly—can feel confident that its conduct falls on the right side of that ill-defined line.

The resulting uncertainty and rational fear of prosecution could lead many existing developers to scale back their participation in the Ethereum or blockchain spaces, or withdraw altogether, and will deter others from taking the leap to innovate in these markets. Indeed, the regulation-by-enforcement approach has already driven some digital asset companies abroad, where the rules are clearer. *See, e.g.*, GAO, GAO-23-105346, *Blockchain in Finance: Legislative and Regulatory Actions Are Needed to Ensure Comprehensive Oversight of Crypto Assets* (June 2023), https://tinyurl.com/2neu5xhy; *A Review of the Fiscal Year 2024 Budget for the U.S. Securities and Exchange Commission: Hearing before the S. Subcomm. on Fin. Servs. & Gen. Gov't*, 118th Cong. at 1:38:00 (2023), https://tinyurl.com/3z6h3kxh; GAO, GAO-22-104625, *Blockchain: Emerging Technology Offers Benefits for Some Applications but Faces Challenges* (Mar. 23, 2022). Prosecutions like this one, if left unchecked, will only accelerate that trend, as developers will be left to speculate what conduct will come under prosecutorial scrutiny next.

CONCLUSION

For the foregoing reasons, the Court should find these prosecutions violate the constitutional right to Due Process.

Dated: December 19, 2025

Respectfully submitted,

/s/ Anthony J. Dick
Anthony J. Dick
JONES DAY
51 Louisiana Ave., NW
Washington, D.C. 20001
(202) 879-7679
ajdick@jonesday.com

CERTIFICATE OF SERVICE

I hereby certify that on December 19, 2025, I electronically filed the foregoing document with the Clerk of Court using the CM/ECF system which will send notification of such filing to all counsel of record in this matter who are on the CM/ECF system.

/s/ Anthony J. Dick
Anthony J. Dick

CERTIFICATE OF WORD-COUNT

I hereby certify that the foregoing document contains 4,121 words calculated consistent with Federal Rule of Appellate Procedure 32(f).

/s/ Anthony J. Dick
Anthony J. Dick