UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

SECURITIES AND EXCHANGE COMMISSION, *Plaintiff,* v. COINBASE, INC. AND COINBASE GLOBAL, INC., *Defendants*.	23 Civ. 4738 (KPF)

BRIEF OF DEFI EDUCATION FUND AS *AMICUS CURIAE*
IN SUPPORT OF DEFENDANTS COINBASE, INC. AND COINBASE GLOBAL, INC.'S
MOTION FOR JUDGMENT ON THE PLEADINGS

CRAVATH, SWAINE & MOORE LLP
Worldwide Plaza
825 Eighth Avenue
New York, New York 10019
(212) 474-1000

Counsel for *Amicus Curiae* DeFi Education Fund

Dated: August 11, 2023

CORPORATE DISCLOSURE STATEMENT

Counsel for *amicus curiae* DeFi Education Fund certifies that *amicus curiae* have no parent corporation and no publicly held corporation owns 10% or more of any stock in *amicus curiae*.

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes & Rules

Other Authorities

INTEREST OF *AMICUS CURIAE*[1]

DeFi Education Fund ("DEF") is a nonpartisan research and advocacy group based in the United States. DEF's mission is to explain the benefits of decentralized finance ("DeFi"), help achieve regulatory clarity for DeFi technology, and contribute to the realization of the transformative potential of DeFi for everyone. DEF advocates for the interests of DeFi users, participants, and software developers working to create new DeFi products using blockchain technology that are decentralized and open to all users. Among other things, DEF educates the public about DeFi through op-eds, podcasts, and print media, meets with members of Congress to discuss DeFi issues, and submits public comments on proposed rulemakings that impact DeFi.

DEF has significant interest in this case, particularly in regard to allegations by the Securities and Exchange Commission ("SEC") concerning Coinbase's "Wallet" software application and "Staking Program" service. These allegations are relevant to the interests of software developers and information technology ("IT") service providers. A decision in favor of the SEC's overly expansive theories related to this software application and service would have a chilling effect on the developers and service providers that innovate in DeFi and, consequently, the users of this technology.

ARGUMENT

The SEC's allegations that Coinbase has acted as an unregistered broker through its Wallet application and has sold unregistered securities through its Staking Program require this Court to accept inferences that are not justified by the realities of how the technologies function. A review of the technological specifics of these two Coinbase applications demonstrates a fundamental mismatch between how the technologies work and how the SEC characterizes

[1] No party's counsel or other person except *amicus curiae* and its counsel authored this brief or contributed money to fund its preparation or submission.

them.[2] The SEC ignores these technological realities in an attempt to shoehorn these applications into the type of conduct the federal securities laws regulate.

While Coinbase is a highly recognizable and popular crypto asset exchange, it is also, most relevant to Wallet and the Staking Program, a software developer and IT services provider. A judgment that Coinbase acts as a broker through its Wallet application would require a strained and unsupported reading of existing law. Likewise, holding Coinbase liable for selling unregistered securities by simply acting as an IT services provider that administers individual users' participation in staking would upend decades of precedent related to fees-for-services arrangements.

I. COINBASE, AS THE SOFTWARE DEVELOPER OF WALLET, DOES NOT ACT AS A BROKER

The Securities Exchange Act of 1934 defines a "broker" as a person "engaged in the business of effecting transactions in securities for the account of others." 15 U.S.C. § 78c(a)(4)(A). Courts have consistently stated that the determination of whether a person acts as a broker requires an individualized "facts and circumstances" analysis of the relevant context and activities in question, with no single factor or element being dispositive. (*See* Defs.' Br. 25–26, ECF No. 36.) At their core, these factors indicate that a broker acts as an intermediary between customers and the securities markets. After examining the technical details of how

[2] On a Rule 12(c) motion, the Court can take judicial notice of certain matters "for the factual background of the case." *L-7 Designs, Inc. v. Old Navy, LLC*, 647 F.3d 419, 422 (2d Cir. 2011). Specifically, the Court may take judicial notice of "a fact that is not subject to reasonable dispute because it: (1) is generally known within the trial court's territorial jurisdiction; or (2) can be accurately and readily determined from sources whose accuracy cannot reasonably be questioned." Fed. R. Evid. 201(b); *see Effie Film, LLC v. Pomerance*, 909 F. Supp. 2d 273, 298 (S.D.N.Y. 2012). The descriptions that follow of how wallet applications and staking work (and Coinbase's versions of these technologies, in particular) are based on a widely held understanding of how blockchain technology functions, and are not reasonably subject to dispute. *See Friel v. Dapper Labs, Inc.*, No. 21 CIV. 5837 (VM), 2023 WL 2162747, at *2 n.2 (S.D.N.Y. Feb. 22, 2023) ("[T]he Court finds that statements regarding the scientific and technical operations of blockchain technology generally are 'not subject to reasonable dispute' and come from 'sources whose accuracy cannot reasonably be questioned.'").

Wallet works, it is clear that there is no basis for finding that Coinbase acts as an intermediary between users and the securities markets because the *user* of Wallet has full control over her interaction with the blockchain—not the developer.[3]

A. How a Wallet Application Works

Wallet is a "wallet application" developed by Coinbase that allows a user to interact with the blockchain using her associated "wallet." A "wallet" is a pair of two numbers—a private key and a public key[4] (Compl. ¶ 47, ECF No. 1)—that are necessary to interact with a blockchain. In general, a wallet application is a software program, most popularly in the form of a browser extension or mobile application.

A "private key" is nothing more than a randomly selected number in a range that is astronomically large. For example, to select a private key for use with Ethereum, which is the largest generalized computing blockchain, users select a random number between 1 and approximately 2^{256}, which is a 78-digit number roughly equal to the number of atoms in the visible universe.[5] By randomly choosing numbers in such a large range, it is effectively guaranteed that no two users will ever select the same private key.[6] Wallet applications assist a

[3] While not addressed in this brief, DEF also disputes the allegations regarding whether Coinbase acts as a broker through Wallet because the SEC does not allege facts to show that any of the tokens it identifies in the Complaint are "investment contracts." (*See* Defs.' Br. 25.)

[4] Technically, the public key is (usually) a pair of numbers, but for simplicity is referred to herein as a "number."

[5] Andreas M. Antonopoulos & Gavin Wood, *Mastering Ethereum: Building Smart Contracts and DApps* 63 (2018).

[6] Rather than using a long random number, which is hard to memorize and write down for storage, wallet applications frequently help the user select a mnemonic phrase, which is generally 12 or 24 words in a specific order. The mnemonic phrase is then passed through publicly available cryptographic algorithms to generate a private key (which is still just a number). The mnemonic phrase, and therefore the associated private key, is generated with the same amount of randomness as would occur with simply selecting a random number. Nothing about selecting a mnemonic phrase as opposed to a number changes the analysis.

user with randomly selecting a number in this range and saving the number on the user's hardware.

After the private key is selected, the "public key" can be derived. The wallet application will run publicly available cryptographic algorithms to do so. The public key is also just a number, and it is inextricably linked with the private key, such that there is only one public key for every private key. While the private key can be used to determine the public key, the public key can never be used to determine the private key; the relationship between the two keys goes "one way."

This is the entire process of establishing a wallet for use on a blockchain: selecting a random number (private key) and using it to derive another number (public key). A wallet application is software that helps users with this process. No third party is needed to establish a wallet because the process of selecting the private key and deriving the public key is done entirely locally, that is, on the device itself and without communication over the internet or the blockchain.

Wallet applications also support importing private keys the user previously selected. In this case, the wallet application will again store any supplied private key on the user's device and derive the associated public key. This seamless importing feature is possible because wallets are distinct from wallet applications—a number is just a number, and the process through which it was originally chosen is irrelevant. Thus, wallets are completely interoperable between wallet applications, regardless of how the private key was selected.

The public key is used to identify the user on the blockchain.[7] For example, for a user with wallet "123" (representing the public key) to transfer two ether (a cryptocurrency) to the wallet "456," she will need to prove that she possesses the private key associated with public key "123." Otherwise, anyone could simply assert that she is the user for that public key. To prove possession of the private key without revealing it, the user will append a "digital signature" to the transaction. All transactions on a blockchain require a digital signature. A digital signature is created by running a publicly available cryptographic signing algorithm that takes in the transaction data and the private key and returns data that represents the signature.[8] The wallet application helps the user create the signature. Because the private key is stored locally on the user's device, no one but the person who physically has access to that device—including the creator of the wallet application—can generate a valid signature and therefore transact on the person's behalf.[9] It is for this reason that wallet applications are described as "non-custodial" or "self-custodial." (*Id*. ¶ 64.)

Once the transaction is signed, the wallet application will send it to the blockchain network to be added to the ledger. A transaction will only be added to the ledger if it has a valid digital signature, which is verified by running a publicly available cryptographic verifying algorithm. The verifying algorithm takes in the transaction data, the signature, and the public key associated with the transaction and determines whether or not the transaction was in fact signed by the private key associated with that public key, without needing the private key itself.

[7] A derivation of the public key, called the "wallet address," is generally how wallets are publicly identified because they are shorter and more human-readable. For simplicity, this example describes a user transacting as represented by her public key directly.

[8] Andreas M. Antonopoulos, *Mastering Bitcoin: Programming the Open Blockchain* 138–44 (2017).

[9] *See* Coinbase Global, Inc., Annual Report (Form 10-K) at 9 (Feb. 21, 2023) ("*Coinbase 2022 Annual Report*"), https://tinyurl.com/4xxjf5pj; Defs.' Answer ¶ 11 n.6, ECF No. 22.

Thus, digital signatures allow for an objective method of verification without necessitating the disclosure of a private key.

In sum, a wallet application typically helps a user with: (1) selecting a sufficiently random number to represent the private key (or importing a previously selected private key) and deriving the public key; (2) storing that private key locally and securely on the user's device; (3) signing transactions using the locally stored private key; and (4) sending the signed transaction over the internet. All of these processes for establishing and using a wallet are based purely in objective methods coded in software, using publicly available cryptographic algorithms. Technically speaking, one could select a private key, derive the public key, sign transactions, and verify signatures using nothing more than a coin (for randomness) and a calculator; a wallet application simply makes the process much less cumbersome. Critically, at no point in this process does the *developer* of the wallet application have the ability to exercise any judgment or control over the user's wallet or crypto assets.

B. Coinbase Does Not Meet the Definition of a Broker as it Relates to Wallet

The SEC ignores the functionality of Coinbase's Wallet software, and wallet applications generally, in alleging that Coinbase, through Wallet (1) controls users' wallets (Compl. ¶ 307), (2) opens users' accounts (*id.*), and (3) routes users' orders (*id.* ¶ 64). These unsupported assertions are central to the SEC's allegation that Coinbase has performed "broker" activities through Wallet.[10] As explained below, each of these assertions is inconsistent with a complete understanding of how wallet applications work and therefore cannot support the SEC's allegation that Coinbase is a broker by virtue of developing Wallet and making it available for download.

[10] The SEC also claims Coinbase solicits "investors" in so-called "crypto asset securities" through Wallet. (Compl. ¶ 307.) The SEC's allegations in this regard are surely not sufficient to establish that Coinbase acted as a broker through Wallet.

1. Through Wallet, Coinbase does not control "accounts" or users' wallets, handle customer funds or crypto asset securities, or commingle and treat as fungible such assets, as the SEC alleges (Compl. ¶ 307). Coinbase has no control over Wallet users' wallets or assets because the private keys for users' wallets are stored directly on users' devices, not with Coinbase (or any third party). (*Id*. ¶ 64.) Wallet uses publicly available and objective cryptographic algorithms to sign transactions, not proprietary algorithms that it uniquely innovated or controls. These transactions are verified by the blockchain, not Coinbase. Crypto assets are not stored "in" a wallet, but rather, are recorded on a blockchain's ledger, with the only means of access dictated by who possesses the applicable private key. Coinbase cannot generate digital signatures for users' associated public keys, and therefore has no ability to control any users' wallets or assets.[11] Likewise, without control over Wallet users' wallets, it cannot commingle users' assets to pool them.

That Coinbase developed Wallet—the software application—is irrelevant to determining control over users' assets. To conclude otherwise would be tantamount to finding that companies that create a web browser (e.g., Chrome) have control over their users' online activities merely because the web browser provides an interface to surf the web.

2. Coinbase does not open customer "accounts" through Wallet, contrary to the SEC's allegation (Compl. ¶ 307). This is because there is no such thing as "opening" an "account" on a blockchain.[12] A blockchain has no notion of "open" versus "closed" "accounts," or which

[11] *Coinbase Web3 Wallet Terms of Service*, Coinbase, https://tinyurl.com/yc75dba3 (last updated May 25, 2023) ("You own and control digital assets held in your Web3 Wallet. . . . [Y]ou are at no time transferring your assets [to Coinbase] . . . ."); Defs.' Answer ¶ 33 n.37.

[12] There is no such thing as an "account" on a blockchain. While it is possible for a user of Coinbase.com to have an "account" on the Coinbase.com Platform, this is meaningless when it comes to discussing wallets—public keys and private keys—on a blockchain. The SEC uses the word "account" interchangeably and without definition in the Complaint (*see, e.g.*, Compl. ¶¶ 75, 307), and for that reason among others discussed here, its allegations regarding Wallet and broker activity fail.

private keys have been selected for use. A simple way to see why this is true is that it is perfectly valid to transfer crypto assets on a blockchain to a public key that no one has ever attempted to derive from a private key; the assets would simply be unobtainable until and unless someone randomly selects the private key associated with that public key. All wallets on a blockchain already exist, and users choose which one is theirs by selecting a random number (a private key). No one, including the developer of any wallet application, authorizes or manages this process; it depends entirely on the fact that, for all practical purposes, no two users will ever pick the same number. There is no checking or approval process, no "approved" versus "not approved" "accounts" or "list" being checked to make sure the user has registered. After a user selects a random number (a private key), she can immediately begin transacting on a blockchain using digital signatures. Therefore, there is nothing Coinbase or Wallet actively does to "open" an "account" because there is no "account" in the way the SEC alleges.

It cannot be the case that software that helps users select a random number and apply publicly available cryptography to derive another number constitutes "opening" an account. In fact, after a user selects a private key (with or without the help of a wallet application), she can freely take that private key and use it to transact in any wallet application. There is complete interoperability because the user—not any third party, and not any developer of a wallet application—maintains full control at all times. Coinbase simply does not have the requisite authority over Wallet users' wallets to "effect[] transactions in securities for the account of others." *SEC v. Kramer*, 778 F. Supp. 2d 1320, 1339 (M.D. Fla. 2011).

3. Finally, Coinbase does not route orders through decentralized exchanges using Wallet, as the SEC alleges (Compl. ¶ 64). A wallet application is simply software that facilitates communication to a blockchain network: it does *not* route orders "through . . . 'decentralized

exchanges'" (*id*). Indeed, for all transactions using Wallet, a user interacts with the blockchain, not through a decentralized exchange as the SEC alleges. Furthermore, Coinbase has no control over a user's assets or transactions. Only a user has control over her own assets, and the user is the sole decision-maker when it comes to transactions.[13] Wallet helps users discover pricing on decentralized exchanges, but this does not constitute the routing of orders on decentralized exchanges.

That Coinbase has, at times, received an "administrative fee" (*id*. ¶ 101) does not, on its own, turn Coinbase into a broker. Courts have made clear that the determination of whether a person acts as a broker is based on the totality of the circumstances. *See, e.g.*, *SEC v. RMR Asset Mgmt. Co.*, 479 F. Supp. 3d 923, 926 (S.D. Cal. 2020). The receipt of transaction-based compensation is only one of several factors courts have considered as part of their broker analysis, and courts have found it insufficient on its own to conclude a person is a broker. *See, e.g.*, *Kramer*, 778 F. Supp. 2d at 1338–41 (concluding defendant was not a broker because, despite receiving a transaction fee, it did not participate in negotiations, analyze financial status of the issuer, promote the investment or possess authority over the accounts of others).

* * *

A wallet application, such as Wallet, is software that helps users interact with blockchains. While the body of existing law and regulation governing "brokers" assumes and mandates a degree of centralized control, neither a wallet application nor its developer have control over users' wallets or assets. The SEC's attempt to regulate Wallet as a traditional

[13] *Coinbase Web3 Wallet Terms of Service*, Coinbase, https://tinyurl.com/yc75dba3 (last updated May 25, 2023).

broker and its allegations about how Wallet works are inherently at odds with the undisputed reality of how the technology functions.

II. COINBASE, AS A SERVICE PROVIDER IN THE STAKING PROGRAM, DOES NOT ENGAGE IN THE OFFER AND SALE OF SECURITIES

The SEC's allegation that staking service providers, including Coinbase through its Staking Program, engage in a securities offering also cannot withstand scrutiny when compared to the technological reality of how staking and staking services work. For a transaction or scheme to be an "investment contract" (and thus, a security), it must meet the four prongs of the *Howey*[14] test: (1) an investment of money (2) in a common enterprise (3) with a reasonable expectation of profits (4) from the efforts of others. There is no basis for finding that Coinbase engaged in an investment contract securities offering through the Staking Program, given that its role is limited to acting as an IT service provider.[15]

A. How Staking Works

Blockchains are distributed systems, where a decentralized network of participants called "validators" follow a protocol to reach agreement on the state of a ledger (a "consensus protocol"). Because distributed systems are designed to function without an administrator entrusted with determining the state of a ledger, consensus protocols instead align the economic interests of validators with reaching agreement (in accordance with a consensus protocol's rules). One such incentive mechanism is "proof of stake," where participants "stake" collateral and are rewarded in kind when they positively contribute to consensus and can have their stake devalued when they disrupt consensus. Thus, staking is an essential component to many blockchains'

[14] *SEC v. W.J. Howey Co.*, 328 U.S. 293, 298–99 (1946).

[15] While this brief focuses on certain *Howey* elements that upon review of the relevant technology are seen not to be satisfied, there are other deficiencies not addressed as to why the Staking Program is not an investment contract security under *Howey*. (*See* Defs.' Br. 27–30.)

consensus protocols, serving as a key ingredient in blockchain's core innovation: the ability to determine the state of a ledger no one controls.

When a "staker" seeks to participate in Ethereum's consensus protocol, she submits a single transaction to a "deposit" smart contract[16] that locks 32 of her ether and sets two values of her choice, a "validator public key" ("validator address") and "withdrawal public key" ("withdrawal address").[17] These values are immutably saved on the smart contract. The effect of this transaction is to allow one validator, the party who holds the private key associated with the specified validator address, to participate in the consensus protocol. Importantly, only the party who holds the private key associated with the specified withdrawal address is permitted to earn rewards and "unlock" the ether. Because the staker sets two different addresses that play different roles in the staking process—ownership and validation—a variety of staking arrangements are possible.

A staker who wants to stake on her own behalf, referred to as "solo staking," first locks the 32 ether and sets the validator address and withdrawal address to wallets that she controls. The solo staker is in full control of both the crypto assets and the validation process. To perform validation, the solo staker downloads any of a variety of publicly available open source software called a validator client[18] and runs it on a server (a computer)—either locally, such as on the

[16] A "smart contract" is publicly available code immutably stored on a blockchain that runs without the control of any party.

[17] *Keys in Proof-of-Stake Ethereum*, Ethereum Foundation, https://tinyurl.com/wswnpswn (last edited Apr. 12, 2023). The following description of how staking works is based on Ethereum, one of the five proof of stake blockchains the Staking Program supports. Ethereum is the largest proof of stake blockchain, and its staking mechanisms function similarly to the other four blockchains at issue. *See* Coinbase Global, Inc., Response Letter Re: Coinbase Global, Inc. Draft Registration Statement on Form S-1 (Dec. 21, 2020) ("*Dec. 21, 2020 Response Letter*"), https://tinyurl.com/43599ywc; Defs.' Answer ¶ 63 n.77. While there are some differences in how staking works on Ethereum compared to these other four blockchains, the SEC does not rely on those distinctions in its Complaint in support of its *Howey* allegations. (Compl. § V.)

[18] *See Dec. 21, 2020 Response Letter* ("[A] validator runs a technology infrastructure (i.e., a server operating standardized software) for performance of routine, non-discretionary operations . . . .").

staker's personal computer, or using a cloud-based solution, such as Amazon Web Services ("AWS"). Utilizing services like AWS is popular for solo stakers because managing *any* server is not a trivial process. The validator client needs access to the private key associated with the validator address, necessitating that it be stored locally with the staker or with the cloud provider.

While solo staking is popular, the process of running the validator client software can be outsourced to various validator providers. By hosting this software, validator providers make staking generally more convenient, which increases participation in staking and, in turn, helps secure the blockchain. To use a validator provider, the staker sets the validator address to one controlled by the validator provider rather than the staker herself. A staker can use a validator provider regardless of how she custodies her assets—whether through self-custody or through a custodian that supports staking—because the withdrawal address is separate from the validator address. When a staker sets the withdrawal address to a wallet she self-custodies and the validator address to a validator provider's wallet, that provider is a "non-custodial validator provider." When a staker sets the withdrawal address to a wallet another party custodies on her behalf and sets the validator address to that party's wallet, that provider is a "custodial validator provider." Coinbase, through the Staking Program, acts as a custodial validator provider. (*See* Defs.' Answer 65.)

Regardless of what type of validator provider is used, the validator provider performs its services by choosing from the same publicly available validator client options the solo staker can choose from and running the software on the staker's behalf (frequently itself using an AWS-type solution to run the validator client and store the relevant keys).[19] The core difference from

[19] *Dec. 21, 2020 Response Letter* ("To provide staking services, the Company downloads and executes standard validator software from an open source repository, like GitHub. . . . The manner in which the Company engages in staking is identical to thousands of other network participants who operate validator nodes . . . .").

solo staking is that the validator provider, not the staker, is uniquely in control of the wallet at the validator address. However, nothing inherent to this control over the wallet at the validator address gives the validator provider ownership of the staked crypto assets or earned rewards set to the withdrawal address, and there is no managerial component in providing such a service.

Staking rewards are given to validators as an incentive to participate in the consensus protocol and properly validate transactions.[20] Every 6.4 minutes, all eligible validators are randomly split into groups and assigned a block to validate. Within each group, one randomly selected validator will "propose" a block to the other validators who will "attest" to whether it is valid (e.g., that all transactions in the block contain valid signatures) by voting. When validators perform activities that help achieve consensus, the protocol sends rewards to their withdrawal addresses at a rate that depends on the number of validators.

There are two primary ways a validator can be penalized by the protocol when engaging in validation activities. *First*, a "minor penalty" can be issued if a validator does not vote when it is supposed to or makes a mistake in its vote. Behavior triggering minor penalties is often a result of factors outside the validator's control (such as losing internet connection). As its name suggests, these penalties are *de minimis*: if a validator fails to perform its duties and receives a minor penalty, it will have the chance to make up the loss 6.4 minutes later. *Second*, a "major penalty," also called "slashing," can be issued if a validator engages in actions that attack the network, such as proposing two blocks instead of one when selected as a proposer. Major penalties are not *de minimis* because instantly 1/32 of the stake is lost and significantly more can be lost if the offense was part of a coordinated attack. Unlike minor penalties, when a validator

[20] *Proof-of-Stake Rewards and Penalties*, Ethereum Foundation, https://tinyurl.com/yvfnvdhx (last edited July 18, 2023).

is slashed, the protocol also forces it to exit, meaning there is no ability for the validator to "make up" the loss. Slashing is extremely rare.[21] Running the validator client under normal conditions will never result in slashing, and validator clients will usually have guards to ensure that actions that would cause slashing cannot occur. Slashing is so rare that validator providers frequently cover the cost of a slashing event.

B. Coinbase Does Not Engage in a Securities Offering as it Relates to the Staking Program

The SEC ignores the technological reality of how staking and staking services work in alleging that Coinbase, through the Staking Program (1) performs a managerial service that dictates rewards and penalties (Compl. ¶¶ 313, 314, 316, 342–344, 355, 360, 364), (2) assumes control over users' stake as a result of validating (*id*. ¶¶ 311, 341), and (3) increases rewards through pooling (*id*. ¶¶ 314, 351, 355, 360). These assertions do not square with what a validator provider like Coinbase actually does, and thus, cannot support the SEC's allegation that Coinbase engages in a securities offering through the Staking Program.

1. The validator provider is not the primary determiner of a staker's ability to earn rewards or receive penalties, and therefore, the staker's rewards are not based on the "efforts of others" under *Howey* as the SEC alleges (Compl. ¶¶ 313, 314, 316, 342–344, 355, 360, 364). When a service provider's efforts are not the primary determiner of an investor's returns, its function does not satisfy the "efforts of others" prong under *Howey* because the provider's efforts are ministerial rather than managerial. *See SEC v. Life Partners, Inc.*, 87 F.3d 536, 539, 545–48 (D.C. Cir. 1996) (finding the "efforts of others" prong was not satisfied because the provider's role was "ministerial" where, the provider carried out important functions for

[21] As of February 2023, only 0.04% of Ethereum validators have experienced a slashing event, one-third of which were slashed in a single incident. Brayden Lindrea, *Only 0.04% of Ethereum validators have been slashed since 2020, says core dev*, Cointelegraph (Feb. 28, 2023), https://tinyurl.com/yw8632xy.

purchasers, including monitoring the insured's health and paying premiums to investors, but the primary determiner of the return on investment was the length of the insured's life, which was outside the provider's control). That is the case with respect to the Staking Program, as Coinbase's "effort" is not the primary determiner of the staker's rewards. Instead, the consensus protocol itself, which is software run on the blockchain and controlled by no one, determines what rewards are given to users.

When a staker solo stakes, the process looks very similar to using a validator provider.[22] Solo stakers frequently outsource hosting the validator client and storing the validator's wallet to an AWS-type service to ensure uptime. AWS's function is undoubtedly essential to whether the solo staker receives rewards or penalties: if AWS goes down, the validator will not run, and the staker will not receive her rewards and will receive minor penalties. Yet it would be inconceivable to conclude that AWS is engaging in a securities offering because it is handling an essential function in whether the staker receives her reward. Rather, AWS's function is squarely ministerial as an IT service provider.

Similarly, a validator provider like Coinbase, which merely runs the same validator client software as a solo staker and stores the validator wallet, often in the same cloud environment as a solo staker, also performs a ministerial function as an IT service provider. Besides performing the basic functions the validator provider is contracted to provide, its efforts are entirely irrelevant to the staker's rewards. While there is certainly a basic level of competence required to perform the service, there is no "best" validator provider because its efforts are constrained by the consensus protocol; exerting more efforts will not have any effect on rewards because the validator provider's efforts are channeled into a standardized protocol it does not control. For

[22] *See Dec. 21, 2020 Response Letter*.

example, on Ethereum, the validator provider has no control over the reward rate a validator earns for proposing or attesting blocks—this is set by the consensus protocol.[23] The validator provider has no ability to determine whether a validator is selected as a proposer or attestor (which earn different rewards)—this is done randomly. The validator provider cannot even control the process of when rewards are received, as this is initiated by the consensus protocol and dependent on the number of validators. Finally, the staker is not beholden to the validator provider. If the staker is not satisfied with the validator provider's services, she can switch to a variety of different validator providers or engage in solo staking because the validator client software is publicly available for anyone to use.

Similarly, the validator provider is *not* performing some essential service to prevent penalties. Both the solo staker and validator provider use the same publicly available validator clients. If there were a bug in one version of the software that caused a validator to not propose a block when it was supposed to, the solo staker and the validator provider would both be subject to the same minor penalty. And no additional efforts by the validator provider are required to *prevent* major penalties like slashing—in fact, additional efforts would be required to *cause* slashing.[24] This is because slashing requires active attempts to attack the network. Slashing cannot occur merely through the validator provider failing to perform its duties. Consequently,

[23] *Coinbase User Agreement*, Coinbase, https://tinyurl.com/ykdhucyt (last updated July 28, 2023) ("Rewards are determined by the protocols . . . ."); Defs.' Answer 65 n.120; *see also Coinbase 2022 Annual Report* at 12 ("[W]hen users stake their assets through Coinbase, the rewards they earn for helping to secure the network are directly tied to the rewards returned by on-chain network protocols and marketplaces . . . .").

[24] Even if the conduct that caused the slashing does not have malicious intent, it still requires active efforts to go against best practices. For example, one of the largest slashing events to date was the result of the provider "pursuing 'technical performance over double-signing robustness,' describing the outcome as 'not a good trade-off . . . [and not] worth the additional risk we inadvertently added.'" Cyrus McNally, *'Expensive lesson': 75 Eth2 validators slashed for introducing potential chain split bug*, Cointelegraph (Feb. 4, 2021), https://tinyurl.com/y8rxy8us.

slashing very rarely occurs, and unsurprisingly, Coinbase has never experienced a slashing event. (Defs.' Answer 161.)

Although Coinbase *could* cause harm to the staker by failing to perform its duties or actively subverting the consensus protocol, it does not follow that Coinbase exerts "effort" on behalf of the staker. Declining to exercise the ability to harm a party by failing to perform a duty or engaging in actively tortious conduct does not qualify as "efforts of others" under *Howey*. *Life Partners*, 87 F.3d at 545 ("The promoter's 'efforts' not to engage in criminal or tortious behavior, or not to breach its contract are not the sort of entrepreneurial exertions that the *Howey* Court had in mind when it referred to profits arising from 'the efforts of others.'").

2. Stakers do not transfer crypto assets or private keys to another party or otherwise give up control over their crypto assets when staking; therefore, there is no "investment of money" under *Howey* as the SEC alleges (Compl. ¶¶ 311, 341). There is no "specific consideration" provided by the staker to the validator because there is no effective change in ownership over crypto assets when staking, regardless of whether a party is using a validator provider. *See Int'l Bhd. of Teamsters v. Daniel*, 439 U.S. 551, 559 (1979).

When utilizing a non-custodial validator provider, the staked assets are solely owned by the staker, who has technical control over them on the blockchain. It is irrelevant that the staker temporarily "locks" her assets to stake them, because no one controls those assets while they are locked, and when they are unlocked they can only be returned to the staker. For custodial validator providers like Coinbase, ownership over staked assets is dictated by the terms of use between the user and the custodian. *In re Celsius Network LLC*, 647 B.R. 631, 652–54 (Bankr. S.D.N.Y. 2023). Because Coinbase's terms state that staking users retain all legal ownership

over their assets,[25] the act of staking has no inherent impact on ownership of assets. Furthermore, the fact that there is a minimal risk that a staker will experience losses, both because of how inherently rare penalties are and because Coinbase will generally cover the cost, means there is no "specific consideration" provided for an investment or risk of loss necessary to meet the "investment of money" prong of *Howey*. *See Gary Plastic Packaging Corp. v. Merrill Lynch, Pierce, Fenner & Smith, Inc.*, 756 F.2d 230, 239 (2d Cir. 1985).

3. Finally, the validator provider does not maximize the chance of stakers receiving more rewards by pooling users' assets; therefore, there is no "common enterprise" under *Howey* as the SEC alleges (Compl. ¶¶ 314, 351, 355, 360). For there to be a common enterprise, the effect of pooling must be to make it so the manager has the possibility of making "1+1" equal to "3." *See Revak v. SEC Realty Corp.*, 18 F.3d 81, 88 (2d Cir. 1994) (finding no common enterprise because individual unit owners did not benefit from the involvement of other unit owners). But under the Staking Program, Coinbase can only make "1+1" equal to "2." The pooling of Staking Program users' assets has no bearing on the expected returns for each of Coinbase's stakers.[26] This is because the reward payout will be proportional to the assets staked, and staking more assets will simply mean there are more stakers who need to be provided rewards. Coinbase's role as a validator provider looks nothing like a promoter-investor relationship associated with an investment contract, where the promoter promises to pool money from investors and use the invested capital to make managerial decisions that provide more returns for the common enterprise.

[25] Wells Submission on Behalf of Coinbase Global, Inc. and Coinbase, Inc. at 49 (Apr. 19, 2023) ("*Wells Submission*"); Defs.' Answer ¶ 59 n.74; *see also Coinbase 2022 Annual Report* at 12 ("Staking does not affect ownership of staked assets, and customers have the same custody relationship with us whether or not they stake.").

[26] *See Wells Submission* at 52; *Dec. 21, 2020 Response Letter*.

* * *

Validator providers, such as Coinbase through the Staking Program, exist to perform a ministerial IT service. The body of existing law governing what constitutes a securities offering assumes a manager who takes funds from investors with the promise to apply her know-how and effort to generate returns that would otherwise not be available to the investors. This conception is inherently at odds with Coinbase's role as an IT service provider that does none of these things.

CONCLUSION

For the foregoing reasons, along with those presented by Defendants, DEF urges the Court to grant Defendants' motion for judgment on the pleadings as it relates to the SEC's allegations that Coinbase acts as an unregistered broker through Wallet and engages in an unregistered securities offering through the Staking Program.

August 11, 2023

Respectfully submitted,

CRAVATH, SWAINE & MOORE LLP,

by

/s/ Benjamin Gruenstein

John D. Buretta
Benjamin Gruenstein
Daniel M. Barabander
Worldwide Plaza
825 Eighth Avenue
New York, NY 10019
(212) 474-1000
jburetta@cravath.com
bgruenstein@cravath.com
dbarabander@cravath.com

Counsel for *Amicus Curiae* DeFi Education Fund