LeXpunK

LeXpunK Comment on Proposed Treasury Regulations

LeXpunK is a community of lawyers and software developers dedicated to providing open-source legal resources and support for the decentralized finance ("DeFi") industry, providing a voice for groups that wish to associate through Decentralized Autonomous Organizations ("DAOs"), and advocating for these communities. Many of our constituents program smart contracts, user interfaces, networks, RPCs, and other core mechanics of digital assets and digital asset transfers. LeXpunK acknowledges the Treasury Department's overall efforts to bring clarity to taxation of digital assets in the U.S., but respectfully requests that the Gross Proceeds and Basis Reporting by Brokers and Determination of Amount Realized and Basis for Digital Asset Transactions proposed regulations (REG 122793-19, the "Proposed Regulations") be withdrawn insofar as they apply to digital asset middlemen pending (1) further study by the IRS into how blockchain technology works and (2) the issuance of clarifying guidance on the taxation of DeFi transactions.

This comment directly responds to question 20 in the request for comment in the Proposed Regulations, namely, whether the definition of "sale" should include wrapping and unwrapping of digital assets. It should not. LeXpunK believes that an inquiry into this specific matter will shed light on other issues present in the Proposed Regulations. The issues described herein therefore also touch on (1) duplicative reporting of transactions[1]; (2) the impact of these reporting requirements on non-US brokers and users;[2] (3) the potential information security issues raised by the reporting requirements in the Proposed Regulations. Finally, LeXpunK respectfully requests that the Treasury Department re-evaluate its use of terms in the Proposed Regulation, as some terms it uses do not match the technical definitions of those same terms or are undefined.

Because this comment is focused on technical aspects of DeFi, a glossary of terms is included at the conclusion of the comment for reference. This comment focuses on one specific transaction, the wrapping of ETH into wETH, for illustrative purposes. The lack of clarity of the Proposed Regulations with respect to the wrapping contract is indicative of the larger problems posed by the Proposed Regulations for tax administration.

As a threshold matter, LeXpunK does not oppose, in principle, the entire idea of third-party reporting for digital asset transactions. However, third-party reporting should be restricted to actual brokers of digital asset transactions. The preparation of tax returns for U.S. Persons who own, trade, or otherwise dispose of digital assets is incredibly onerous, and third-party reporting could decrease the confusion regarding the reporting of taxes in the U.S. However, the Proposed Regulations will likely increase, rather than decrease, taxpayer confusion in reporting digital

[1] See Request 27 of the Proposed Regulations.
[2] See Requests 28-34 of the Proposed Regulations.

asset disposition in the U.S. This is because the Proposed Regulations cast too wide a net for the third parties who must report transactions, which will cause significant over-reporting of transactions, increasing taxpayer confusion. Furthermore, the Proposed Regulations will impose reporting requirements on autonomous software and networks which do not have operators that can furnish the data required. Finally, the Proposed Regulations leave open substantive matters, including failing to provide critical guidance as to what transactions constitute a "disposition" of a digital asset, which will prevent third-party reporters from being able to accurately report basis information relating to digital asset transactions.

LeXpunK recommends that the Treasury Department first address the open substantive questions regarding the taxation of digital assets, and revisit the reporting requirements once these substantive questions have been addressed.

Example Transaction

For the purposes of this comment, LeXpunK will focus on a very common transaction in DeFi – the exchange of the Ether token (ETH) for the wrapped Ether token (wETH). This process is known as "wrapping,", and the reverse is known as "unwrapping." The ETH token is a gas token for the Ethereum network. This means that the ETH token must be used by all users of the Ethereum network to process transactions, and it is the property by which validators, blockbuilders and node operators are compensated for processing transactions on the Ethereum network. Notably, ETH cannot be used in an ERC-20 token contract, also known as a "smart contract". wETH solves this problem. wETH is an ERC-20 token. The process of wrapping ETH (i.e., converting it to wETH) is therefore a necessary predicate step to using ETH in any smart contract on the Ethereum network. Similarly, the process of unwrapping wETH (i.e. converting it to ETH) is critical to being able to utilize wrapped ETH for its designed function as a gas token.

In addition to the symbolic value of analyzing the wETH contract, LeXpunK focuses on this transaction because it is very common. wETH is held by almost one million users of the Ethereum network, and it has been transferred nearly 200 million times in 14 million separate transactions. Over 3 million ETH, or $5 billion worth of ETH is held in the wETH smart contract. Furthermore, the similarity of the wrapping contract to many other smart contracts makes it illustrative of the deficiencies in the current guidance for dispositions of digital assets and the concomitant problems with the reporting requirements of the Proposed Regulations.

ETH is the native token of the Ethereum blockchain. It is one of the most widely held and used tokens in the world. ETH can be wrapped, i.e. converted to wETH, in several fashions, all of which utilize the wrapping smart contract. The wrapping contract consists of approximately 100 lines of code. It is immutable, it has no administrative privileges and it has no operators. There are no fees to use the wrapping contract, besides the gas fees required to use the Ethereum network.

Although the value of ETH and wETH should always be equivalent, the function of the two tokens is very different. ETH and wETH can be exchanged freely, permissionlessly, and with no exchange fees, but they also can have separate markets.This means that while exchanges, centralized or decentralized, may treat ETH and wETH as interchangeable, it is possible for different markets to establish different prices for each asset.

Specifically, ETH is used as the gas token for the Ethereum network, meaning that it is used as payment for verifying transactions. Gas, on a blockchain network, is the compensation a user pays to node operators in exchange for the computing power expended by nodes and validators to validate and store transaction information on the blockchain ledger. ETH can be used by smart contracts for basic functions. For example, a smart contract can transfer ETH or it can hold ETH.

However, as described above, ETH is not an ERC-20 token. ERC-20 is an EIP standard[3] and it provides the basic standards for software to operate on the Ethereum network. An ERC-20 token is a token which can perform functions that meet these standards. The ETH token cannot perform those functions, where wETH can. Therefore, wETH fulfills an important function on the Ethereum network, it represents ETH, but can be used in smart contracts.

Mechanics of a Smart Contract Transaction

To illustrate the variety of software providers who would be deemed to be "facilitating" DeFi transactions and would therefore be required under the Proposed Regulations to store user PII and issue 1099-DAs, this comment will describe the mechanics of a wrapping transaction.

When a user uses the wETH smart contract to wrap ETH, the smart contract is initiated through a transfer of ETH to the wETH smart contract address. This process involves the user using a wallet (i.e. a piece of software that facilitates sending transactions to the Ethereum network) or by manually building the transaction. To send ETH using the Ethereum network, a transaction must be validated on the blockchain and the recorded balances of ETH in the Ethereum network must be updated.

The process is initiated by a user, manually or with a wallet software, preparing the transaction. The wETH smart contract address and contract interface details are requested from the blockchain, most commonly using a remote procedure call or "RPC", which is an interface for software to read and write transactions to the Ethereum network. The user then defines the parameters of the transaction, which is how much ETH to wrap, and sets a gas price. The amount of gas used on Ethereum is determined by how much computation the transaction takes and is always paid in ETH. The gas price is used to pay validators for finalizing the transaction on the

[3] EIP refers to the Ethereum Improvement Protocol – it is the consensus mechanism of applying upgrades to the Ethereum network.

blockchain, and is determined on the number of, and competitive price set by, existing pending transactions.

Once the transaction is prepared, the user signs the transaction with the private key of their wallet, which cryptographically proves that the owner of the wallet is initiating this transaction. The transaction is then sent to a node that is currently synced with all other nodes on the Ethereum blockchain. This process is most commonly completed by a user's wallet software and again uses the RPC interface to submit the transaction to the blockchain network. After checking that the transaction is valid and signed, the node sends the transaction to a list of pending transactions called the mempool. The mempool consists of all pending transactions waiting to be selected and validated on the blockchain.

Note that while the Ethereum network has rules for network consensus, mempool management is not standardized. This means that different node operators may have different prioritization or validation rules, and some allow for transactions to remain private from the public mempool. The amount of gas included with a transaction determines its priority in the mempool, and, if the gas is not high enough, a transaction may be removed from the mempool without being completed.

For the transaction to be included in a block, it must be propagated. Because Ethereum is a proof of stake, or “PoS”, network, propagation occurs through validators. Valid transactions in the mempool are known as “pending” transactions. A blockbuilder will track pending transactions and bundle them into blocks. A blockbuilder first prepares the header of the block, which is the block’s unique identifying information, and then fills the block with pending transactions.

Once the blockbuilder completes the block, the block can be executed by a validator. Execution refers to the state transition of the Ethereum network. In order for the state transition to occur, a sufficient number of validators must agree that transactions in the block are valid. It is during this state transition that the wrapping contract is called. Before the ETH can be wrapped, though, a validator must confirm that the user has enough ETH to both satisfy the gas costs of the transaction and provide the stated amount of ETH in the transaction to be wrapped.

Assuming that the transaction is valid, it is part of a block that is approved by the validators. This results in a portion of the user’s ETH being provided to the blockbuilders, nodes, and validators for the service of transitioning the network state, and some of the user’s ETH being transferred to the wrapping smart contract. The amount of ETH sent by the user is then transferred and stored in the wrapping smart contract and the contract issues the exact equivalent amount of ERC-20 wETH tokens for the user (using the same process outlined above).

In its simplest form this transaction can be completed by a user building their own transaction and submitting it directly to a node. This is very time-consuming, though. At minimum, most users use a software wallet solution, to automate the transaction-building process on the user end,

and an RPC which is software that manages the process of sending the transaction to a node. The user can generally choose which wallet, RPC, and node they use for a given transaction. However, the transaction cannot be completed without the services of the blockbuilder and validator, whose selection the user does not control.

There are other ways a user may interact with the wrapping smart contract. A user may transact with another smart contract that calls the wrapping smart contract as part of that contract's code, as described above. A user may also transact with the wrapping smart contract through a front end, which may facilitate a transaction to wrap ETH as part of a function such as trading or bridging tokens.

A front end is a website that has an interface that allows the user to interact with a smart contract, through their wallet, without programming the transaction. Most users use front ends for almost all transactions, and some front ends perform multiple transactions on a user's behalf with singular instructions.

The Problem Posed by Wrapping

The initial problem posed by wrapping is substantive. Is ETH "materially different" from wETH? If not, the wrapping contract is not a disposition of a digital asset. If so, wrapping (or unwrapping) of ETH constitutes a disposition of the asset. The Treasury Department should issue regulations that clarify that transactions like wrapping do not constitute disposition before issuing the Proposed Regulations. From a technical perspective, ETH and wETH are materially different. ETH can be used to perform network functions in Ethereum. wETH is an abstraction of ETH that can perform none of those functions. wETH, on the other hand, is a composable ERC-20 token that can be used in smart contracts, and ETH cannot be used in such fashion, except in the limited circumstances outlined above.

From an economic perspective, there is no difference between ETH and wETH. 1 ETH should always equal 1 wETH, unless there are extreme market inefficiencies, as the two can be freely exchanged as long as the Ethereum network is functioning. Existing IRS guidance highlights the functionality of ETH as gas (see CCM 202124008) as differentiating ETH from BTC. Under this guidance, it would therefore follow that ETH is materially different from wETH because the latter cannot be used as gas. However, it should be noted that CCM 202124008 is materially incorrect in its assessment of the use of BTC. BTC is used to pay transaction fees on its network, making it comparable to ETH.

Other IRS guidance (CCM 202316008) highlights the importance of an "ascension to wealth" in determining whether a disposition has occurred. There should be no ascension to wealth when exchanging ETH for wETH, but the two tokens embody differing entitlements. It is important to note that tokens do not embody entitlements at all, so this guidance is confusing by its terms.

This IRS guidance relies on *Cottage Savings Ass'n v. Commissioner*, 499 U.S. 554 (1991), to make the determination as to when an asset exchange constitutes a disposition. However, *Cottage Savings* is entirely focused on legal rights (it deals with an exchange of promissory notes).

This case does not actually provide useful instruction for determining when an exchange of one token for another is a disposition. Tokens do not encompass legal rights; they are software. Much like it does not make sense to ask whether a .docx file encompasses different legal rights from a .pdf of the same text, it makes little sense to ask whether ETH encompasses different legal rights from wETH. A .pdf file cannot be used in the same fashion as a .docx file, but that does not mean that they encompass separate, or any, legal rights. Unlike promissory notes, which explicitly describe the legal rights of the holder of the note, tokens on a network only have meaning within the context of that network and do not represent an enforceable right in the legal sense.

It is important to note that without resolving the basic issue of when two tokens are sufficiently different that such tokens are "materially" different, it will be impossible for brokers to determine basis information with respect to gross proceed reporting. Therefore, the Treasury Department should consider issuing regulations under section 1001 which specifically address when two tokens are materially different prior to requiring brokers to essentially guess (and to arrive at different conclusions) regarding a user's basis in a token.

Compensation

The following parties to the wrapping transaction may receive compensation throughout the wrapping process:

- The wallet provider
- The RPC
- The blockbuilder
- The validator
- The front end

Notably, the smart contract which performs the actual wrapping or unwrapping of ETH does not receive a fee.

The Definition of Digital Asset Middleman is Unclear in the Proposed Regulations

Section 80603(a) of the Infrastructure Act clarifies that the definition of broker under section 6045 includes any person who, for consideration, is responsible for regularly providing any service effectuating transfers of digital assets on behalf of another person. With respect to the wrapping contract, there will be, in general, at least five different brokers under this definition. All five would be included as a "digital asset middleman" under proposed § 1.6045-1(a)(21) if they are in "a position to know the identity of the party" using the wrapping contract. Subsection (ii)(A) of this rule states that if a person can change the amount of the fee which they charge, they are presumed to be in a position to know the identity of the user.

It is unclear whether the wrapping contract itself is a digital asset trading platform under the rules because, although it facilitates the exchange of one digital asset (ETH) for another (wETH), it does not do so for a fee. However, assuming that the exchange of wETH to ETH, or vice versa is a disposition, multiple software providers may be responsible for reporting that transaction under the Proposed Regulations. Each of these providers may have differing information as to the asset's cost basis.

The Proposed Regulations do not shed light in any meaningful sense on how to determine a digital asset's cost basis. LeXpunK agrees with Treasury that the existing regulations under Section 1012 of the Code "do not expressly address the calculation of basis for digital assets", but also contends that the Proposed Regulations are equally unhelpful. Additional rules for determining the cost basis of digital assets acquired with cash are marginally helpful. However, the reality of digital asset transactions is that the overwhelming majority of these transactions do not involve cash. Rather, they involve the exchange of one digital asset for a different one.

Proposed Regulations 1.1012-1(h) and 1.1012-1(j) answer questions relating to the determination of the cost basis of a digital asset acquired in exchange for a different digital asset. But neither Proposed Regulation attempts or purports to answer the predicate question of when such exchange has occurred. The Proposed Regulations leave taxpayers, and critically, reporting brokers, in the same position they are in now, having to reason with reference to decades old case law about when there is a sufficient exchange of "legal rights" with respect to two different tokens to determine when a taxable disposition has occurred.

The same issue is present in Proposed Regulation 1.1001-7. This regulation adopts the materially different standard for determining when an exchange of digital assets is a disposition, but provides no guidance as to what factors a taxpayer should use in determining whether differences between two tokens are material. Digital asset brokers will similarly be unable to determine when a reportable transaction has occurred.

Therefore, under the proposed rules it is likely that many taxpayers will receive conflicting information reporting on the same transaction. This will make tax reporting and compliance more difficult on the taxpayer and on the IRS.

The Exception for Validators in the Proposed Regulations is Inadequate for its Intended Purpose

The Proposed Regulations also fail to effectively exclude validators from the reporting requirements, although the intent appears to be that such service providers are excluded. The exception to facilitative services in Proposed Regulation 1.6045-1(a)(21)(iii)(A) only applies to validators engaged "solely" in the business of validating transactions. It is unclear what "solely" means in this context, as many validators also receive income from priority payments. A priority payment is a fee paid by a user to attempt to have their transaction processed more quickly. This is paid in addition to the base gas fee, which is determined by network congestion. In other words, validators are not engaged "solely" in the business of "validating transactions", because they are also engaged in the business of transaction *ordering/*prioritization.

Treasury should remove "solely" from this definition, because it is not clear whether a validator receiving both base fees and priority payments is engaged solely in the business of validating transactions.

The Proposed Regulation's Position-to-Know Standard is Arbitrary

The "position to know" standards contained in the definition of digital asset middleman misstate the relationship between access to user information and fees. For example, an RPC node may charge a fee for providing blockchain information to a decentralized application, but have no relationship whatsoever with the end user of the application. Such an operator would be in a "position to know" according to the definition of a digital asset middleman because they can set the fee for providing information regarding the blockchain state, but, as a practical matter, it is not possible for such software providers to interact directly with individual users or request personal identification from said users.

The Proposed Regulations would require software providers with tenuous relationships to users to request PII from users. It is well known that a knowledge of a person's name, social security number and address is more than sufficient for such a person's identity to be stolen.[4] The digital asset middlemen reporting requirements require any person who is able to alter a fee for any service relating to a blockchain to collect the user's PII. Given that the reporting requirements in the Proposed Regulations will require multiple different people to report the same transaction, the Treasury Department is increasing the risk of identity theft without any benefit in tax compliance.

The Proposed Regulations' Indicia for Foreign Transactions are Unrelated to Blockchain Transactions

[4] See IRS Publication 5027 https://www.irs.gov/pub/irs-pdf/p5027.pdf

Finally, many middlemen who are organized outside of the United States may simply wish to exclude US persons from their user base, as the costs to comply with the reporting requirements will exceed the marginal benefit of the fee for those services. The Proposed Regulations do not provide nearly enough specificity as to how a service which is conducted entirely outside of the United States can sufficiently prevent U.S. persons from accessing their service to avoid the reporting requirements.

The U.S. indicia listed in proposed § 1.6045–1(g)(4)(iv)(B)(1) through (5) are insufficient for determining whether a non-US digital asset broker who operates non-custodial blockchain software is interacting with a US person. Of these five factors, four are categorically inapplicable to blockchain service providers: customer permanent address, location of a user's bank account, customer account location, and customer place of birth. A digital asset middleman that charges fees for use of a smart contract cannot require a user of the smart contract to provide this information.

Even the first factor, the IP address of the user's communication device is only known to operators of front ends, and is not information that is accessible by persons who may have other modalities of involvement with blockchain systems. The Treasury Department should consider providing direct guidance as to how digital asset middlemen who do not operate front ends and only operate blockchain software can ascertain the location of their users to determine if such users are US persons. The Treasury Department should also confirm in its guidance that a front end digital asset middleman can rely on software which prevents IP addresses from within the United States from accessing their front end to determine that their services are not available to US persons.

Undefined or Improperly Defined Terms in the Proposed Regulations

It is important for the regulations regarding digital asset broker reporting requirements to avoid creating new definitions of terms which vary from the existing ordinary or technical uses of those terms. Even basic terms used repeatedly in the Proposed Regulations and preamble are undefined or defined outside of their normal usage. There are several critical examples of this, which may cause major issues.

a. Ambiguity of "Wallets"

The Proposed Regulations and preamble repeatedly refer to "wallets" as equivalent to a "user account". A wallet is a piece of software used for setting up transactions. Wallets are not, primarily, key management software, although most can perform key management on top of their other functions. Wallet software is primarily used to create and broadcast transaction requests for ultimate processing by validators of a blockchain network. Furthermore, a user can store their private key in any manner. Under the definitions in the Proposed Regulations, a physical safe

which contains a private key written on a piece of paper is a "wallet," but software that holds no private keys and is only responsible for transaction packaging/broadcasting is also a "wallet". This makes the term "wallet" ambiguous and not an appropriate concept for drawing regulatory boundaries.

Under the Proposed Regulations, a person providing wallet software to a user is a reporting broker unless "the sole function [of the wallet] is to permit persons to control private keys which are used for accessing digital assets on a distributed ledger". Prop. Treas. Reg. § 1.6045–1(a)(23). However, the Proposed Regulations also state that "[s]oftware that provides users with direct access to trading platforms from the wallet platform is not an example of software with the sole function of providing users with the ability to control private keys to send and receive digital assets." *Id.*

The Proposed Regulations do not define "platform" so it is impossible to understand what differentiates a "wallet" from a "wallet platform". Fundamentally, the purpose of wallet software is to allow users to interact with other blockchain addresses, including smart contracts that, presumably, are "trading platforms" (the Proposed Regulations also give no guidance as to what constitutes a trading platform).

Depending on the exact definition of "wallet," users may be free to access blockchains without using a wallet. There is no reason to treat users who use wallet software differently from those who do not for reporting purposes. "Accounts," in contrast, are either: (a) pairings of a private key held by a user with one or more public keys (aka "addresses") as recognized on a particular blockchain network (these are so-called "externally owned accounts" or "EOAs"); or (b) smart contracts on a particular blockchain–with some but not all smart contracts being under the control or influence of one or more users, each from their own respective externally owned accounts.

Perplexingly, the Proposed Regulations define both a "hosted wallet" and "unhosted wallet," but do not define a "wallet." This error is further evident in the definition of "held in a wallet or account" found in Prop. Treas. Reg. § 1.6045–1(a)(23). This definition states:

> For purposes of this section, a digital asset is considered held in a wallet or account if the wallet, whether hosted or unhosted, or account stores the private keys necessary to transfer control of the digital asset. A digital asset associated with a digital asset address that is generated by a wallet, and a digital asset associated with a sub-ledger account of a wallet, are similarly considered held in a wallet. References to variations of held in a wallet or account, such as held at a broker, held with a broker, held by the user of a wallet, held on behalf of another, acquired in a wallet or account, or transferred into a wallet or account, each have a similar meaning.

This definition conflates a wallet and an account. An account (as in an EOA) is accessed by a private key. It cannot store a private key. Therefore, an account is fundamentally different from a wallet. The impact of this definition of wallet is that any software provider that provides software which both: a) manages private keys, and b) programs transactions for a user on a blockchain, is a reporting broker.

However, such a rule does not take into account that such a software provider is not in the position to know any of the information which would be required to issue a 1099-DA. Such software providers are not in a position to know the identity or location of the users of such software. Furthermore, they are not in a position to know the nature of transactions for which their software is used, i.e. whether users are, in fact, disposing of digital assets, for federal income tax purposes, using their software.

The only indicia of ownership of an account is control of the private key related to such account. The Proposed Regulations attempt to skirt this simple fact by treating wallets as something which they are not.

b. Ambiguity of "Smart Contracts"

The term smart contract is also misused in the Proposed Regulations. A smart contract is simply any executable software stored on a blockchain and executed by validators on behalf of users within the blockchain's virtual machine environment. As outlined herein, smart contracts can be used with or without counter-parties, and with or without fees. Despite the name "smart contracts," they need not constitute, represent, or form a part of the performance of a legal agreement. Likewise, as is demonstrated by the issues posed by the wrapping contract, the use of a smart contract is not determinative of the tax treatment of any given transaction.

c. Ambiguity of "Sale" and "Purchase" and "Disposition"

Critically, the Proposed Regulations fail to state or understand that it is not possible for a digital asset to be "purchased" or "sold," ***as such terms are used in the Internal Revenue Code***, on the blockchain. This is because dollars (or any currency) do not exist on the blockchain. Although stablecoins do exist on the blockchain and reference dollars, they are not dollars. Therefore, the only transaction which can occur on the blockchain, from the perspective of the Internal Revenue Code, is an exchange of property. Therefore, all references to "payments" occurring on a blockchain must be re-evaluated because what is actually being described is an exchange of intangible property, which is not defined as a "payment" anywhere else in the Internal Revenue Code.

From this perspective the failure of the Proposed Regulations, as set forth herein, to address when the exchange of property on a blockchain constitutes a disposition and when it does not is a critical failure to provide much needed regulatory guidance on the taxation of digital assets.

d. Ambiguity of "Platform"

It is unclear what is intended with the term "platform" which is used frequently in the Proposed Regulations. As used in the preamble, the use of the term "platform" varies between implying that the term refers to systems *operated by* a person, and a person who receives benefits from systems. "Wallets" are also described as "platforms" in the preamble, however, the preamble also suggests that "platforms" may be unincorporated associations that are businesses. The preamble also confusingly seems to refer to"platforms" as distinct from "smart contracts" and "protocols".

Similarly, the Proposed Regulations themselves refer to "websites" as being analogous to "platforms". *See* Proposed Reg. 1.6045-1(b)(ix). Examples 17, 18 and 19 of Proposed Regulation 1.6045-1 refer to a business that operates "a website that regularly provides online services to customers in order to match would-be sellers of digital assets with would-be buyers." It is unclear what differentiates a "website" from a "platform" in this context. Likewise, Example 22 of this same Proposed Regulation refers to "a business that operates a website that licenses unhosted wallets". Nowhere in this example is the significance of the existence of a "website" (or a "license") explained.

Thus, in general, the term "platform" is highly ambiguous within both the Preamble and the Proposed Regulations.In spite of the frequent use of the term, no definition of "platform" is offered. It is unclear what the commonality is between all of the different things described as "platforms" in the Proposed Regulations.

Personally Identified Information Concerns

Many of these service providers involved in blockchain transactions that will be treated as reporting brokers are not customer facing. Some are simply automated software that exists solely on the blockchain network. One feature of DeFi that separates it from traditional finance is that transactions in DeFi are composable, meaning that the transactions themselves are embodied in tokens which can be used in other transactions. Composability also refers to smart contracts which can be called as parts of other smart contracts in ways that are not visible to a user. Currently, a DeFi transaction may include many market participants who do not face the user.

Blockchain networks are public; anyone can access the information therein. Transaction information is pseudonymous - each transaction is permanently recorded on a public ledger and associated with a wallet address, but not linked to personal identities. Given the public and permanent nature of most digital asset transaction information on a blockchain, any effort to connect wallet addresses to personal identities could result in severe, lasting privacy concerns for those users. This is akin to having one's entire credit card transaction history published on the internet, exposing each user's entire transaction history to the public. This would pose significant

threats to DeFi users. Therefore, maintaining the privacy of user identities is a core concern for many digital asset holders.

Most persons and software meeting the criteria of a broker or a middleman in the Proposed Regulations would prefer to not collect user PII, and would certainly prefer to not link user PII with network addresses. This is not motivated by a desire for secrecy, necessarily, but to protect users. As the preamble to the Proposed Regulations admits, the purpose of these Proposed Regulations is to create a system wherein multiple parties are responsible for reporting the identity of each participant in a DeFi transaction. The impact of this is that there will be multiple points where a user's PII can be leaked, hacked, or otherwise accidentally disseminated to the public. Not only is the proposed reporting system inefficient, it also makes the DeFi environment much more dangerous for users.

These Proposed Regulations give a very short amount of time for brokers and middlemen to develop systems for reporting digital asset transactions, and also to create systems to store and securely maintain user PII. Mistakes will be made in the implementation of these regulations by protocols. These mistakes will result in damage to users in the form of identity theft and theft of assets.

Furthermore, users will be bombarded with requests for PII from protocols which will be treated as brokers and middlemen. This will present an opportunity for scammers to create honey-pots, i.e. fake services or websites which demand PII for nefarious purposes under the guise of tax compliance. The IRS generally takes precautions regarding identity theft and other PII issues for taxpayers. Identity theft is not discussed, and was apparently not considered, when promulgating the Proposed Regulations. The Treasury Department should, at minimum, review the impact that the reporting requirements, including the acknowledged duplicative reporting requirements, will have on taxpayers prior to finalizing the Proposed Regulations.

Broader Implications

Although we have focused our discussion on "wrapping" and "unwrapping" ETH, this is not an isolated issue–but rather exemplifies systemic problems with the Proposed Regulations as applied to a broad range of very similar blockchain transactions. This comment focuses on the wrapping contract for ETH as a symbol for a myriad of other transactions. The following transactions can be conceived of as having the same tax reporting issues which arise in the context of wrapping ETH:

- All Layer 1 ("L1") blockchains which utilize smart contracts have some form of wrapping contract for the native gas token. These wrapping contracts, for the most part, function similarly to the wETH contract.

- Many protocols use a form of wrapped ETH as the preferred form of ETH to be used in their platform smart contracts. These contracts function similarly to the wrapping contract described herein, and give rise to a similar set of legal issues with respect to reporting. The same questions regarding whether converting ETH to wETH constitutes a disposition exist when converting ETH to the form of ETH preferred to be used on platforms such as AAVE, Frax and Compound among many others. NB, the wrapped form of ETH on these platforms should not be confused with ETH derivatives that represent yield bearing tokens.
- Many Layer 2 ("L2") blockchains use a form of ETH as a gas token that is a separate asset from ETH as it is used on the Ethereum network. An L2 blockchain is a blockchain which processes and validates transactions separately from the L1, or base, blockchain, and posts only the proofs of the final transactions to the L1 blockchain. Some L2s, such as Arbitrum and Base, use a form of ETH as the native gas token for processing transactions on the L2 blockchain. Other L2s, such as Optimism and Polygon, have their own native gas token. Regardless of whether an L2 uses ETH as its gas token, each also has a form of wETH that exists on that chain only for the purposes of utilizing ETH in smart contracts.

The Proposed Regulations will require, according to its own estimates, approximately 8 billion 1099-DAs to be generated, with each transaction creating a reporting requirement for multiple entities. One conclusion to draw from these duplicative reporting requirements is simply that the Treasury Department is using third party reporting requirements to create disincentives for offering any blockchain related software to U.S. users or in the United States.

Whether intentional or not, the impact of the Proposed Regulations will be to create hurdles for software developers creating blockchain software and dangers for users using blockchain software. The Proposed Regulations will not clarify the major substantive issues facing taxpayers who are required to report digital asset transactions on their returns. Therefore, the Treasury Department should examine whether these Proposed Regulations will facilitate tax compliance, or simply discourage the use of blockchain software.

At a minimum the Treasury Department should allow additional time to allow compliance with these regulations and issue appropriate substantive guidance on digital assets prior to their effectiveness.

Terminology

DeFi transactions are quite complex, and it is worth defining the terms used in this comment in clear, non-technical manners.

A "wallet" is a piece of software that facilitates sending transactions to a blockchain network.

A “transaction” is a message to a blockchain network that a user wants to execute an action.

An “address” refers to the alphanumeric identifier, or public key, of a wallet (this type of address is known as an “EOA” or “externally owned account”) or a smart contract on a blockchain.

An “EOA” or “externally owned account” refers to a wallet address that is controlled by one private key. An EOA may be controlled by any person who has access to the related private key.

A “smart contract” refers to an executable program that can be accessed on a blockchain through a public address. Smart contracts can also be thought of as a species of web services that operate on blockchains.

A “blockchain” is a decentralized, distributed, public ledger that records transactions through network consensus mechanisms.

A “block” refers to the unit on the blockchain in which a set of transactions that occur contemporaneously are stored. Blocks are identified by time stamps and unique hashes, and each block refers to the previous block, thereby forming the blockchain.

A “node” is a blockchain stakeholder, usually a computer, which stores the information submitted to a blockchain network and validated by validators.

A “validator” is a type of node on a blockchain network which validate new transactions and blocks through cryptographic proofs.

A “proof of stake” or “PoS” blockchain refers to a blockchain which uses randomly selected validators to confirm transactions submitted to the blockchain.

A “proof of work” or “PoW” blockchain refers to a blockchain which uses a competitive method between validators to validate transactions submitted to the blockchain.

A “remote procedure call” or “RPC” is a type of communication software which allows a user to call processes on a remote system, such as a blockchain. In the context of blockchain, an RPC allows a user to interact with a blockchain in a myriad of ways, including querying information from the blockchain, sending transactions to a blockchain, and executing smart contracts.

“Administrative permission” in the context of a smart contract, refers to the ability of a person, by use of a private key, to edit or change the functioning of the smart contract. A person with administrative permissions for a smart contract can be considered an owner of that smart contract.

An “immutable” smart contract is a smart contract which does not have administrative permissions. It can be called publicly, but it cannot be modified.

A “front end” refers to a web interface which handles some or all of a transaction initiated by a user to interact with a blockchain.