DeFi 101

Curated by
DeFi Education Fund

About DeFi Education Fund

Founded in 2021, the DeFi Education Fund (DEF) is a nonpartisan research and advocacy not-for-profit organization committed to building a mainstream understanding of decentralized finance (DeFi). At DEF, we advocate for sound DeFi policy and to protect the rights of developers, users, and projects to freely create decentralized infrastructure and technology.

DEF is the bridge between DeFi and the lawmakers and regulators creating policy. We believe that DeFi has immense potential for human prosperity. In order to get there, we need clear rules so that users have the confidence to transact freely using DeFi and software developers have the clarity and freedom to innovate they need to build the future of our financial system.

To contact us, or schedule a "DeFi 101 briefing," please send a note to talia@defieducationfund.org

DEFINING DEFI

DEF is defining DeFi for policymakers, regulators, and those looking to better understand DeFi's technical nuances and overarching promise.

REPRESENTING DEFI

At the heart of our work, DEF is representing DeFi technologies, builders, and users in D.C. and wherever DeFi can use an advocate.

MOBILIZING DEFI

As the only organization exclusively focused on DeFi, DEF is mobilizing the DeFi community to present and elevate a unified "DeFi voice" in critical policy and legal discussions.

Table of Contents

Executive Summary

- The traditional financial system as we know it today is premised on trusting third-party intermediaries to execute transactions on our behalf.
- Bitcoin – the first blockchain-based digital asset – was created in response to the 2008 financial crisis, which underscored the risks that are inherent to such trust in financial intermediaries.
- Digital assets and blockchain technology allow people to engage in self-directed, peer-to-peer transactions nearly instantly, cross-border, and 24/7.
- DeFi allows people to transact without relying on or trusting an intermediary, solving some of the legacy challenges that exist in traditional finance today.

Since the launch of Bitcoin in 2009, the digital asset ecosystem has created a model for conducting financial transactions in a manner never before seen: for people to run software locally on their computers to participate in a network for communicating, validating, and recording data, and through which people can securely send value directly to their peers without an intermediary. These are known as blockchain networks, and with them came a revolution of software applications and protocols that evolved the manner in which humanity transacts in the digital age.

DeFi is a financial system built on public blockchains that allows people to engage in **self-directed, peer-to-peer financial transactions without relying on intermediaries and while maintaining custody and control over their own funds**. DeFi democratizes access to the financial system and removes barriers to entry often found in traditional finance. The ability for people to **self-custody** their assets is central to DeFi; no financial institution can restrict a person's ability to access their assets, enforcing property rights and consumer protections.

DeFi includes software protocols and applications that:
- Are built on public blockchains and open-source code;
- Have no centralized intermediaries;
- Work with people custodying their own digital assets and data; and
- Are governed by decentralized, dispersed entities not under common control.

The Benefits of DeFi

- **Enables** open and equitable access to financial services.
- **Enhances** transparency of financial services.
- **Offers** around-the-clock liquidity.
- **Lowers** transaction costs.
- **Accelerates** concrete transaction settlement.
- **Provides** users with greater freedom and privacy.
- **Protects** consumers from exposure to risks inherent with intermediaries.

DeFi Explainers

Public Blockchains

Peer-to-Peer Protocols and Networks

At the foundation of DeFi, the technology stack begins with a peer-to-peer (P2P) protocol and network. A protocol is the set of rules and standards that govern direct communication between different peers in a network, whereas the network itself consists of independent people or businesses that operate the hardware and software needed to participate in the network. Specifically, in a P2P network, there are two or more independent participants who operate computers (nodes) and share authority and storage of the data via the internet. There is no need for a central server in a P2P network, and therefore, no single entity has control over it. This differs from the more popular client-server model, where users request and receive services from a centralized server that stores, manages, and protects the data; for example, a user's device interacts with Facebook by sending a request to Facebook's servers, which then retrieves requested data—posts, likes, etc.—and runs the application. Essentially, Facebook's parent company, Meta, has complete control over who can or cannot access their data and applications.

A mechanism for storing data and communications for a P2P network is known as a *public blockchain*, which is a type of distributed ledger technology. Essentially, each node in the P2P network runs a software application that enables it to communicate with other nodes in the network, validate new transactions and blocks according to the network's rules, maintain a copy of the blockchain, and have the option to participate in the creation of blocks.

Hashing

Information stored in a block is identified by a *hash value* and includes the hash value of the previous block to link two blocks together, creating a chain—hence, the term "blockchain." A hash value is generated through cryptographic hashing, which is a mathematical process of inputting data into a *hash function* to output a unique string of alphanumeric characters used to identify blocks in a blockchain and link them together. Essentially, a hash function is an algorithm that takes the transactions in a block, the hash value of the previous block in the chain, and other relevant block data as input, and generates a bit-string that serves as a representation of that data—i.e., the hash value. Importantly, if that data were altered in the slightest way, the hash function would generate a completely different hash value.

In short, a hash value represents a block's data such that any alterations to the underlying data are readily identifiable. This plays a crucial role in maintaining the immutability of blockchain transactions because once a transaction is recorded, it cannot be altered or deleted without also altering the block's hash value and disrupting the chain of connecting hashes. Once a block is created, it is verified by a consensus mechanism, which is the process by which the network's nodes agree on the validity of transactions and the current state of the blockchain.

Consensus Mechanisms

Before a transaction reaches consensus (explained in the next section), it undergoes initial verification by the network's nodes for completion and correctness (e.g., signature validity, balance sufficiency, etc.). Once verified, the transaction is placed in a memory pool, or *mempool*—a pool of unconfirmed transactions—where it awaits inclusion in a block by a miner or validator. When a block is proposed, each node receives said block, independently validates its authenticity, and adds it to their copy of the blockchain. Through this process, the network reaches consensus on what is the correct chain of transactions—also known as *network synchronization*.

Network synchronization is an ongoing process by which all nodes in a network update their copies of the blockchain to ensure they all hold the same, most current version of the blockchain. When a new block is created or verified by a node, the node then broadcasts it to neighboring nodes in the network and the process continues as such. When a node receives a new block that is attached to a part of the blockchain that it doesn't have, it will compare this chain to its own. The node adopts the chain based on criteria for chain selection that varies depending on the consensus mechanism. The most popular forms of consensus mechanisms for blockchain networks are *Proof-of-Work (PoW)* and *Proof-of-Stake (PoS)*.

Proof-of-Work

PoW is most notably used in the Bitcoin network and requires nodes, known as *miners,* to compete to solve a cryptographic puzzle by finding a specific value known as a *nonce*. Miners combine this nonce with the block's data (e.g., previous block hash, timestamp, etc.) through a hash function, which then creates the hash value*.* The goal is to find a hash value that meets a specific criterion set by the network. Miners essentially input different nonces through the hash function until one succeeds. Then the network checks that the hash value and the block's transactions are correct. If everything is correct, the miner is rewarded with a newly minted network token, such as a bitcoin.

Mining requires computing power and energy, which is used as an incentive system and security mechanism. A bad actor attempting to introduce a fraudulent block is disincentivized by the high energy cost required to solve for the hash value that would be lost when the network does not validate their block. Essentially, the actor would incur a significant energy cost for nothing in return. In order for a bad actor to successfully implement their desired block, they would need to control over 51% of the network's computational power to validate their block. This would take a tremendous amount of energy and would cost them more than they would profit, especially as networks like Bitcoin are continuously expanding.

Nodes in a PoW network adopt the chain with the largest cumulative difficulty – *i.e.*, the greatest amount of computational work from cryptographic hashing – as a consensus for maintaining network synchronization. This computational work signals agreement among miners, and is therefore considered to contain the most valid and trusted blocks.

Proof-of-Stake

PoS, notably adopted by the Ethereum network among many others, uses a different consensus approach. PoS may divide block production into time intervals known as *slots*. For each slot, the blockchain protocol randomly selects a validator to propose a new block and broadcast it to the larger set of validators (*i.e.*, attesters), so they can then attest (vote on) the validity, or correctness, of the block and add it to the chain once it receives a threshold of attestations. Meanwhile, almost immediately, the next slot begins, and the process starts anew. As a result, the network uses less energy than in PoW, because nodes no longer need to expend computational power to compete to solve a cryptographic puzzle.

To prevent bad actors from manipulating the information stored on a network, *staking* requires providing collateral to the network in order to become a validator. Successful validators and attesters are rewarded with a newly minted network token, such as an ether on the Ethereum network. Staking also disincentivizes malicious behavior through punitive measures. If a validator acts dishonestly or negligently, their staked tokens are slashed, meaning the blockchain's underlying software automatically reduces the validator's staked tokens once the network detects the behavior. Thus, while the selection process of validators is random, the probability of being selected increases with the amount staked, because the validator has more to lose if they behave maliciously.

Unlike in a PoW network, where nodes adopt a chain based on the computational work done, nodes in a PoS network adopt a chain based on the amount of stake-weighted attestation votes backing it. When the group of validator nodes stake their tokens, they do so to participate in the validation process. And even if they are not chosen as the validator for a specific block, they attest blocks and their staked tokens remain active and could be used in future block validations. Therefore, following the most attestation votes best reflects the consensus of the network, as it represents the greatest economic commitment from network participants.

Public-Key Cryptography

A novel aspect of cryptocurrency transactions is that they are done in a P2P manner—i.e., without a third-party intermediary. This is securely done through a form of *asymmetric cryptography*—also known as *public key cryptography*—so that a user is not required to trust an intermediary or another user to transact.

A user can generate a private key by using cryptographic algorithms that produce a random string of characters. The private key is then the basis for mathematically generating the corresponding public key. Importantly, while public key generation is easily computed, it is nearly impossible to reverse-engineer the private key from the public key—hence, making it a secure cryptographic process.

Asymmetric cryptography is used in authenticating the sender's identity and the transaction's information by producing a *digital signature*. This process begins with the automatic generation of a cryptographic hash of the transaction—much like the hash generated for a block, this hash serves as an identifier and

consists of a long string of characters. The sender then uses their private key to sign the transaction's hash, producing a digital signature. Upon receiving the transaction, the network uses the sender's public key to verify the digital signature and recover the original hash. Also upon receipt, a new hash is generated in the same manner as the original hash, and because it is generated using the same transaction data, the two hashes are identical. This allows the network to compare the hashes and verify that the transaction has not been altered in transit and confirm its authenticity. Overall, this process not only authenticates the sender's identity but also ensures the integrity of the transaction.

Lastly, to make sending cryptocurrency more user-friendly, a blockchain address is mathematically generated from a public key as a shorter string of characters. This serves as a more practical representation used for securely sending and receiving transactions. With a better understanding of asymmetric cryptography, it is evident that this mechanism provides a variety of benefits such as: securing transactions and user information without needing an intermediary, enabling non-repudiation, and eliminating the need to trust other users.

Noncustodial Wallets

Fundamental to cryptocurrency transactions on a decentralized network, is the concept of self-custody. Users employ *noncustodial wallets* to control their own assets and to communicate with a blockchain network. Contrary to popular belief, assets are not actually stored in a wallet; rather, the wallet stores the cryptographic keys (public and private) that enable full control of assets. Cryptocurrency should be thought of as data packets, as they represent pieces of information – specifically ownership of a certain value – that is transferred between users. And the blockchain simply records transactions and balances, but does not store or control any assets. Users have total control over said assets, because the cryptographic keys are the only mechanism for access and transmission of the assets.

A user connects their wallet to a blockchain through the internet and can rely on a related application to provide an interface for communicating with the network. The user interface displays the user's public key or blockchain address for receiving assets, which can be displayed as a long string of characters. When sending assets, the sender specifies the recipient's blockchain address and the amount to be sent, then uses their private key to provide a digital signature. Under the direction of the user, wallet's software communicates with the associated blockchain to reflect the updated user's balance from the ledger as transactions are processed.

Noncustodial wallets generally come in two forms: "hot" and "cold." The difference between a "hot wallet" and a "cold wallet" is that while a user stores their keys locally on their own device, a "hot wallet" application maintains connectivity to the internet. In contrast, a "cold wallet" (which includes a hardware wallet, *i.e.*, a physical device used for storing keys) keeps keys isolated from internet-connected devices and internet-based attacks. With cold storage, users can connect their device to a computer to sign transactions offline before broadcasting them to the blockchain network through compatible applications, maintaining security while enabling transaction functionality.

In contrast, third-party custodians offer hosted wallets as a service for custodying users' keys, and therefore assets, on their behalf. This is similar to having an account with a traditional financial intermediary. So, in this circumstance, the user can conduct a transaction the way they would in the traditional financial system: by notifying the custodian so they can conduct a transaction on the user's behalf. These custodians have total independent control of users' assets.

Smart Contracts

Public blockchain technology serves as the foundational layer for cryptocurrency transactions, but its function is limited to the secure recording and broadcasting of data in a decentralized manner. However, the introduction of the Ethereum blockchain in 2015 extended blockchains' capabilities by allowing anyone to develop applications and systems that leverage its core functions. Among these are DeFi protocols, which go beyond just P2P transactions to a wider range of financial services. DeFi consists of sets of a blockchain-based software application known as a *smart contract* to automatically execute certain functions upon users' instructions and when predefined conditions are met, eliminating the need for an intermediary.

A common analogy for a smart contract is that of a vending machine: the vending machine automatically releases a bag of chips on the condition that it receives $2. The consumer initiates the transaction then solely relies on code to execute it, not a third party vendor. And while the smart contract automatically executes transactions, the transactions are still initiated by the user and still verified by the blockchain network and recorded on the ledger – *i.e.*, the fundamentals of a P2P blockchain transaction do not change. In other words, a smart contract is simply a software tool for users to conduct a variety of financial activities without an intermediary and employ the verifiability and security of a blockchain.

The deployment of a smart contract is no different than other blockchain transactions. Essentially, anyone can take software code and deploy it on a blockchain, and the blockchain's nodes will accept the code so long as the deployment transaction is a valid transaction. Here is how it works:

1) Developer writes the code;
2) The developer, or another user wishing to deploy the code, creates a *deployment transaction* that includes the bytecode of the smart contract and its initialization parameters, and signs the transaction with their private key to authenticate and authorize it – the sender does not specify the recipient;
3) The deployment transaction is then sent to the sender's connected nodes within the blockchain network;
4) These nodes then relay the transaction to their own connected nodes and the transaction continues to propagate across the network;
5) Each receiving node verifies and validates the transaction's digital signature and sufficient gas, and ensures that it complies with the network's rules – they do not audit the smart contract's code;

6) Once the deployment transaction has reached consensus, miners or validators include it in their new block, which finalized the deployment;
7) Once it is added to the blockchain, the smart contract is activated and is assigned a unique address on the blockchain – its bytecode and initialization parameters are stored in the contract's storage.
8) Once it is deployed, the smart contract is autonomous and immutable, and anyone can use it.

Using a smart contract to transact involves specifying details such as the sender address, recipient (i.e., smart contract) address, transaction value, and gas fees. This includes the data field which contains the instructions (*i.e.*, the function) for the smart contract's execution. Specifically, the data field consists of two elements: a function identifier and a function argument.

The function identifier signals to the smart contract which function to execute (e.g., borrowing funds, token swapping, or voting on a governance proposal). The function argument for a transaction consists of the specific data or parameters input into the smart contract function for it to execute it properly (e.g., amount of tokens or the voter's choice). The two elements ensure that a smart contract knows which operation to perform.

Constructing a transaction can be done manually by users with technical expertise; however, it is more commonly done by connecting the user's unhosted wallet to the DeFi protocol's front-end website (later discussed), as the process is much more intuitive and approachable. After constructing the transaction, the user then uses their private key, securely stored in their wallet, to sign the transaction and broadcasts it to the blockchain network. Once the transaction is included in a block and validated, it triggers the smart contract to automatically execute the logic defined in its code.

DeFi Protocols

DeFi protocols are a system of interrelated smart contracts and their decentralized governing arrangements that enable P2P financial transactions. DeFi protocols offer communication, connectivity, or software services that parties can utilize to communicate trading interests, but they do not intermediate transactions. Even when DeFi protocols originate from a single software developer or small group of developers, they can be designed to ensure distributed governing authority among a decentralized and disaggregated group of unrelated users.

It's important to recognize that while the term 'protocol' is used interchangeably between P2P networks and DeFi protocols, the two are distinct. As noted in the previous section, a P2P network is simply the governing model for communication method between two or more devices (nodes), and a blockchain is the mechanism used to store and communicate the data (transactions) between nodes; whereas, the term "protocol" in DeFi encompasses the rules, functions, and interactions defined by a collection of smart contracts that allow people to engage in specific activities.

Upgradability

Since a smart contract's code is immutable once deployed on a blockchain, which ensures security and trust, it also means that bugs and inefficiencies in the smart contract code are permanent unless mechanisms for upgradability are implemented in the protocol. This means that a specific smart contract can be replaced by a new smart contract within the protocol, "upgrading the protocol," but an individual smart contract itself is immutable and its code cannot be rewritten. One approach is to deploy a new smart contract and migrate users over to the new one. This poses a challenge of upgrading a contract's code while preserving its existing state – *i.e.*, data such as transaction history, user balances, etc. In this context, the migration from one smart contract to another involves transferring data which could lead to disruptions.

Data Separation Pattern

Fortunately, DeFi protocols can be designed to be upgradable through various architectural patterns. This has led to more innovative approaches to upgradability, such as a data separation pattern. In a general sense, a data separation pattern is a software design pattern that splits functionality between two smart contracts: one for storing data (i.e., state) and another for operational logic (i.e., how software behaves). The data contract stores all the data and includes functions that allow for other contracts to access and modify the data. This contract remains persistent and is not typically the focus for upgrades. The logic contract maintains operational functions (e.g., transferring tokens, updating balances, etc.) and it refers to the data contract when it needs to read or modify data.

When upgrading a DeFi protocol that is designed with a data separation pattern, the logic contract is the smart contract that undergoes an upgrade and the data contract remains persistent. Due to the immutability of smart contracts, this means that the protocol's governance would choose a new logic contract to deploy on the blockchain and ensure that the new logic contract refers to the existing data contract.

The problem with the data separation method is that once a new logic contract is made, any smart contract connected to the original logic contract, or any front-end providing access to it, must be updated to reference the new logic contract. Furthermore, separating the data and logic into separate contracts can be expensive, as the logic contract has to make external calls to the data contract and requires more gas to do so than a smart contract that can read or modify the data stored within itself. Given these two factors, protocol developers have opted to a proxy pattern design which also separates the data but differs in how it handles the contract logic and data storage.

Proxy Pattern

In a proxy pattern, a placeholder or intermediary (i.e., the proxy) controls access to another object (i.e., the target). In the context of a DeFi protocol, there are two smart contracts: a proxy contract and an implementation contract. The proxy contract acts as a front-facing contract for users and other smart

contracts, and delegates their calls to the implementation contract, which holds the main business logic. Importantly, the proxy contract typically stores all the contract's state.

An implementation contract contains the actual business logic and can be updated or replaced to upgrade the system. If there is an upgrade to the smart contract's logic, it is simply deployed as a new smart contract and the proxy contract is redirected to the new implementation contract. One way to understand the two contracts' relationship is to imagine the proxy contract as a universal remote and the implementation contract as a TV – the remote adds a layer of convenience and functionality to controlling what the TV does, but does not need to be changed when the TV's system is upgraded.

The proxy pattern approach allows for smart contract upgrades without changing the smart contract's address, preserving the contract's state, and ensuring continuity for the protocol's users. However, it's important to note that upgradability is typically left to smart contracts that are less foundational to the protocol's functionality such as those that handle auxiliary functions – i.e., features and operations that support the main functionality of the protocol, but are not central to the core mechanics. Smart contracts that are essential to the core mechanics of the protocol – e.g., privacy pools – are often made immutable to ensure a high level of security, as changes could threaten the integrity of the protocol.

Importantly, while a proxy pattern utilizes two smart contracts, just like a data separation pattern, it uses a specific function that allows it to execute the logic contracts code as if it were its own. In other words, users, front-ends, and other smart contracts use the proxy contract to directly execute code in the logic contract. Meanwhile, protocols that are designed with a data separation pattern require users, front-ends, and other smart contracts to interact with the logic contract that then executes external calls to the data contract, making the process more expensive and less convenient when there is an upgrade.

Decentralized Exchanges

Decentralized Exchanges (DEXs) are a subset of DeFi protocols where a variety of digital assets can be traded. As any DeFi protocol, DEXs are simply software programs that run "on top of" a blockchain, and users can employ them to conduct a variety of economic activities and financial transactions.

An important aspect to recognize is that unlike the traditional financial system that requires users to provide personal information for a third party to make transactions on their behalf, DEXs are public software that anyone can directly interact with and do not require them to share personal information to issue a transaction. Furthermore, because transactions are done via smart contracts, DEXs are non-custodial and users do not have to trust a third party with their assets.

There are two kinds of DEXs that are popularly used, the first uses an on-chain order book much like in a traditional stock exchange to match buyers and sellers. However, as the name implies, the matching process occurs on-chain – *i.e.*, on the blockchain – through smart contracts and without intermediaries. Essentially, matching is performed automatically through the software identifying compatible orders and organizing transaction information to broadcast it to the blockchain, targeting the smart contract that handles the order book's settlement.

Another popular DEX is known as an automated market maker (AMM) and that uses the ratio of two assets in a special-purpose smart contract called a liquidity pool in which users (known as liquidity providers) deposit assets for others to trade and in return receive a portion of the trading fees. The AMM uses the ratio to determine the relative price of two assets. In this formula, x and y represent the assets and k represents the constant product value. The AMM calculates the prices of each asset based on their supply and demand: as x increases in supply, its price decreases to maintain a constant product value of k. As the transactions are validated by the underlying blockchain, new prices are calculated in real-time.

The price determination is the key difference between the two types of DEXs: while on-chain order books determine price based on what is set between buyers and sellers, AMMs determine price based on the ratio formula above.

Front-Ends

Front-ends are graphical user interfaces (GUI, *i.e.*, a website or application) that facilitate communication between the user and a DeFi protocol over the internet. Essentially, a front end displays blockchain data in human-readable format, making it easier for users to communicate their transactions to the blockchain. .

When initiating a transaction, a sender specifies the recipient's blockchain address, the amount to be sent, and uses the sender's private key to sign the transaction, ensuring its security and authenticity. As the transaction is validated, the amount of digital assets associated with a given public address is updated.

For clarification, a front-end is not an intermediary. A front end is more like a "translator" from humans to blockchains, similar to the way email works. When sending an email, a person writes the email using the Roman alphabet to coherently write words and sentences. When that email is sent, the email protocol "translates" the message into a form that can be transmitted to the recipient in data packets that can be sent over the internet. Likewise, front-ends "translate" human-understandable activities into a data form that blockchains can understand.

RPC Nodes

By approving a transaction with their private key, the user directs the wallet application to broadcast the transaction via a remote procedure call (RPC) node. An RPC node is a server or computer that receives the signed transaction data from the user and then propagates it across the blockchain network so it can be validated by other nodes and eventually included in a block. There are many RPC nodes run by individuals and groups around the world, contributing to the decentralized nature of blockchain networks.

DeFi Technology Stack

Key-Storage Layer
- Self-Custodial Wallet

Application / Interface Layer
- User Interface (e.g., Wallet Applications, Protocol Front-Ends, Aggregators)
- Command-Line Interface

Broadcast Layer
- Remote Procedure Call (RPC) Nodes: Broadcasts Transactions to Network

Smart Contract Protocol Layer
- Core Smart-Contracts: Foundational, Non-Upgradable (e.g., Automated Market Makers, Lending Pools, Liquid Staking, Anonymity Pools, Governance, etc.)
- Auxiliary Smart-Contracts: Supportive, Upgradable (e.g., Aggregator Routers and Vaults, Oracles, Registries, Bridges, etc.)

Asset Layer
- Native Token & Block Reward
- Fungible Tokens (e.g., UNI, USDC, AAVE)
- Non-Fungible Tokens (NFTs)

Base Layer
- (e.g., ETH, SOL)
- Peer-to-Peer Blockchain Network (Validators, Nodes)
- Consensus Protocol / Settlement (e.g., Proof of Stake)

DeFi Transaction Flow Chart

USER SIGNS TRANSACTION TO SMART CONTRACT USING PRIVATE KEY

RPC NODE RECEIVES THE SIGNED TRANSACTION AND BROADCASTS IT TO THE PEER-TO-PEER NETWORK

TRANSACTION IS VERIFIED FOR CORRECTNESS THEN ADDED TO A MEMORY POOL OF OTHER TRANSACTIONS

BLOCK IS BROADCAST TO OTHER VALIDATORS, WHO VERIFY* TRANSACTIONS ON THEIR OWN VIRTUAL MACHINES AND ATTEST IF VALID

VALIDATOR RUNS ALL TRANSACTIONS, UPDATES THE BLOCKCHAIN, AND INCLUDES A HASH REPRESENTING THAT RESULT

VALIDATOR SELECTS TRANSACTION AND LOCALLY RUNS THE SMART CONTRACT'S BYTE CODE ON ITS INTEGRATED VIRTUAL MACHINE
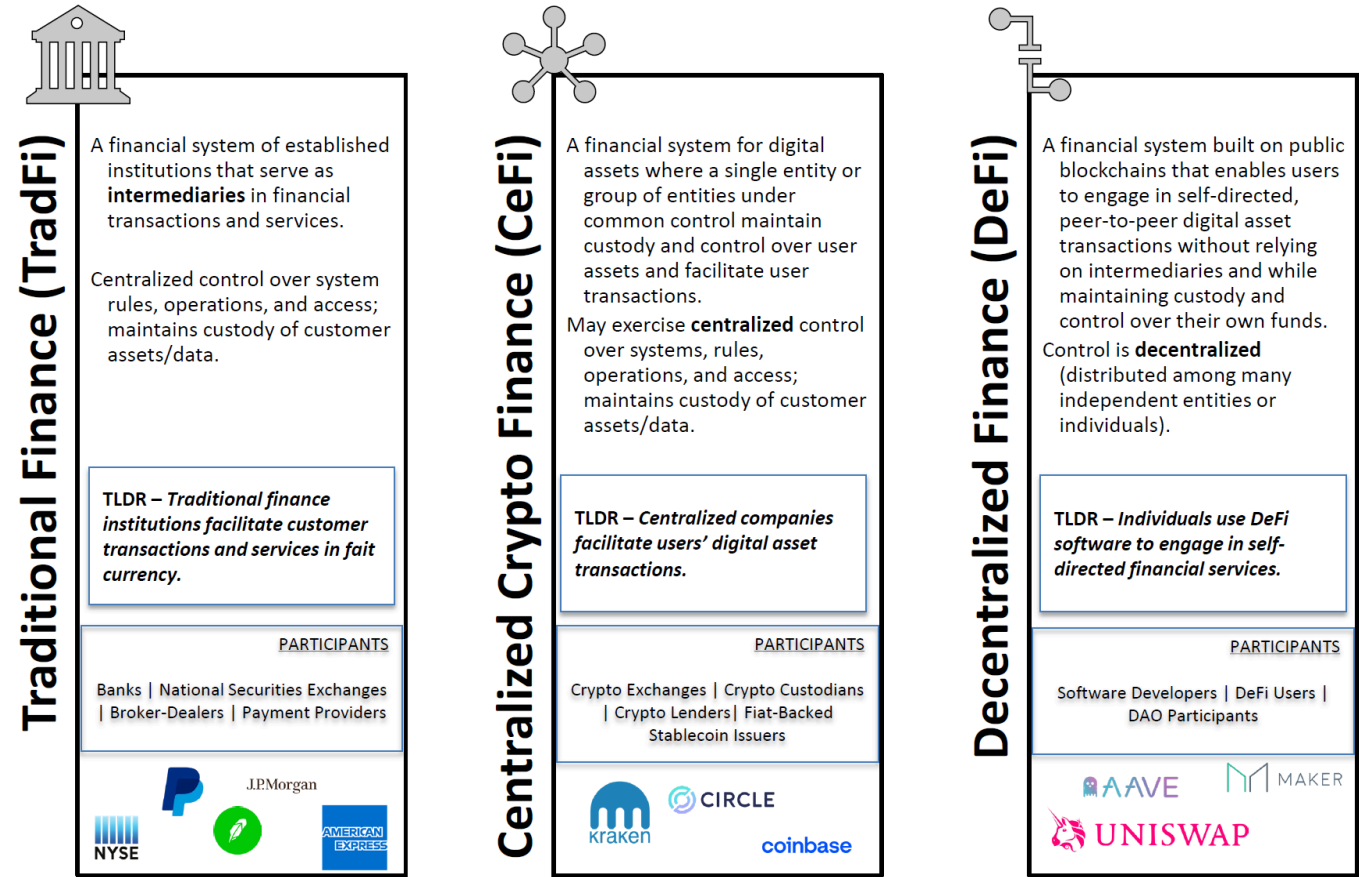
*Network nodes ran transactiont within the proposed block to they can and the block to thair copy of the blecichain if their resuits match and reach consences.

Differences Between TradFi, CeFi, and DeFi

Traditional Finance (TradFi)

A financial system of established institutions that serve as **intermediaries** in financial transactions and services.

Centralized control over system rules, operations, and access; maintains custody of customer assets/data.

TLDR – *Traditional finance institutions facilitate customer transactions and services in fiat currency.*

PARTICIPANTS

Banks | National Securities Exchanges | Broker-Dealers | Payment Providers

Centralized Crypto Finance (CeFi)

A financial system for digital assets where a single entity or group of entities under common control maintain custody and control over user assets and facilitate user transactions.

May exercise **centralized** control over systems, rules, operations, and access; maintains custody of customer assets/data.

TLDR – *Centralized companies facilitate users' digital asset transactions.*

PARTICIPANTS

Crypto Exchanges | Crypto Custodians | Crypto Lenders | Fiat-Backed Stablecoin Issuers

Decentralized Finance (DeFi)

A financial system built on public blockchains that enables users to engage in self-directed, peer-to-peer digital asset transactions without relying on intermediaries and while maintaining custody and control over their own funds.

Control is **decentralized** (distributed among many independent entities or individuals).

TLDR – *Individuals use DeFi software to engage in self-directed financial services.*

PARTICIPANTS

Software Developers | DeFi Users | DAO Participants

Important DeFi Concepts

Self-Custody

"Self-custody wallets, also known as self-hosted, unhosted, or non-custodial wallets, are software tools hosted on a person's computer, phone, or other device that allow users to store and manage their own digital assets private keys without reliance on a third-party intermediary. Self-custody wallet services ensure that individuals have full control over their digital assets, enabling transactions without intermediaries or centralized control."

"Technically, each self-custody wallet is associated with a unique pair of cryptographic keys: a public key, which serves as an address for the self-custody wallet (e.g., receiving digital assets), and a private key, which grants exclusive control over the assets within the wallet. Because the private key is never shared with any third party, including the self-custody wallet's software provider, only the wallet owner controls the private key and thus can authorize transactions, significantly reducing counterparty risk. Transactions are signed locally using the private key and broadcasted to the blockchain network, where they are verified and recorded in a decentralized ledger. In other words, in contrast to traditional financial institutions, the self-custody wallet provider does not control the private keys on behalf of users nor process transactions – this is all completely left to the user."

"The role of self-custody wallet providers is limited to supplying software that enables users to interact with blockchain networks; they do not hold funds, intermediate transfers of funds, or manage transactions, nor do they have control over or ownership of user accounts. Self-custody wallets do not involve granting any form of custody or control, direct or otherwise, to any third-party. The user retains full control over their assets, with private keys stored locally rather than entrusted to a third party. Unlike financial institutions, which are capable of debiting or crediting funds, wallet providers lack the ability to initiate or reverse transactions. This distinction is fundamental to the statutory definition and aligns with prior regulatory interpretations that require a financial institution to have a fiduciary or custodial role."

[DEF Response to CFPB EFTA Proposed Rulemaking (March 2025)](#)

Open-Source Software

"Open-source code is fundamental to the DeFi ecosystem for a variety of reasons. First, developers can build off each others' work, making it cheaper and easier to innovate. Second, it empowers diversity in the space since the code is available for anyone in the world to use, modify, and distribute – all one needs is a computer and an internet connection. Third, the code is auditable for anyone to ensure there are no bugs or backdoors, and contribute fixes – this is especially important since trust is conducted through code. Lastly, it 'enables rapid proliferation of ideas.' Furthermore, open-source code and decentralized protocols work in tandem: by making code open-source, decentralized protocols promote transparency and community involvement. If protocol developers made their code proprietary, a single entity or group would have excessive influence and control over the code."

Permissionless Networks

"... if a blockchain protocol is permissioned then it is not decentralized. Decentralization requires the distribution of authority and storage over data to a network of two or more nodes. By distributing authority, no single entity dictates who can or cannot participate in the network – i.e., the network is permissionless. A permissioned network implies that there is a central entity with the authority to be the gatekeeper."

Response to Autorite des Marches Financiers (AMF) regarding its DeFi Paper (October 2023)

Policy Considerations

DeFi Policy Foundational Principles

Protect DeFi Users

- Protect self-custody;
- Protect financial privacy – which would also protect freedom of speech and association, as users can safely fund and support political causes of their choosing without repercussions.
- Ensure consumer protections by promoting decentralization, which minimizes risk of single points of failure and of malicious third-parties.
- Promote financial inclusion and protect against financial censorship.

Protect DeFi Technology Developers

- Protect disintermediation.
- Incentivize decentralization.
- Promote safe harbors.
- Ensure that "control" is effectively defined and employed as a central element in distinguishing intermediated systems from disintermediated systems.
- Protect competition and innovation in DeFi.

Traditional Regulatory Approaches Will Not Work for DeFi

Written Testimony of DEF's Executive Director Amanda Tuminelli before the U.S. House of Representatives Committee on Financial Services' Subcommittee on Digital Assets, Financial Technology and Inclusion (September 2024)

"DeFi is an umbrella term generally used to describe blockchain-based software protocols that allow people to engage in economic activities online on a peer-to-peer basis and allow people to self-custody their assets. To do so, DeFi builds on the innovations of public blockchains, which are the software protocols that first enabled people to engage in peer-to-peer value transfer over the internet. Because there is no need for a central server in a peer-to-peer network, no single entity has control over the data stored on a public blockchain. Instead, all computers (nodes) participating in a peer-to-peer blockchain network (1) hold a record of the history of data stored on the network; and (2) reach consensus as to the validity of that data. No single entity participating in the network has control over, or can alter, the data record." (Pg. 2)

"DeFi technology was developed in response to the many challenges and risks inherent in the structure of intermediated financial services, be it CeFi or TradFi – including limited and unequal access, slow settlement cycles, inefficient price discovery, liquidity challenges, a lack of assurance around underlying assets, opaqueness, broker risk, and uptime issues. TradFi intermediaries establish trust between transacting counterparties – the knowledge that a transaction will occur as both parties expect – by

acting as a middleman between them. For example, making a payment with a credit card involves a minimum of four separate financial intermediaries in addition to the two parties to a transaction. However, instead of relying on specialized intermediaries to establish trust between counterparties, blockchains establish trust via rules-based, encoded software protocols. These novel features enable people to use public blockchains to engage in digital transactions and economic activities without reliance on third-party intermediaries. Users of DeFi protocols have open, transparent access to systems that allow people to conduct various types of financial activities without requiring specialized intermediaries or institutions." (Pg. 5)

"Because DeFi protocols are software programs whose functionality is totally different from CeFi and TradFi businesses (as discussed above and in Appendix B), public policy and regulatory approaches to DeFi should be different as well. Attempting to "shoehorn" DeFi protocols into existing public policy frameworks designed to address the risks and opportunities of TradFi and CeFi would be akin to requiring jetliners to abide by the same standards and requirements as automobiles. While both car and airline manufacturers produce vehicles for the same reason – to provide transportation – cars and airlines facilitate transportation in distinct ways. Fortunately, the requirements applicable to car manufacturers and airline manufacturers are responsive to the functional differences through which the vehicles transport people. If they were not, airplanes would never get off the ground. So too in the context of DeFi protocols." (Pg. 8)

"The United States' dynamic market economy produces all manner of novel solutions to old problems which require dynamic responses to accomplish long-standing public policy objectives. The United States' economic preeminence has been built, in part, on this "flywheel" of innovation in markets and innovation in public policy. This approach has not only benefited U.S. investors and businesses, but also "contributed to America's geopolitical standing around the globe." (Pg. 8)

"DeFi protocols join the United States' long history of innovative approaches to conducting well-established economic and financial activities. DeFi software protocols do not change the reasons why people and businesses seek financial services – to generate returns, price and hedge risks, make payments, etc. – but they have fundamentally changed how people and businesses access and conduct financial activities." (Pg. 9)

Available at: https://democrats-financialservices.house.gov/uploadedfiles/hhrg-118-ba21-wstate-tuminellia-20240910.pdf

Money Transmission

Through the Looking Glass: Conceptualizing Control and Analyzing Criminal Liability For Unlicensed Money Transmitting Businesses Under Section 1960.

Amanda Tuminelli, Daniel Barabander, and Jake Chervinsky

On December 2, 2024, the DeFi Education Fund ("DEF") published a new paper in *The International Academy of Financial Crime Litigators* written by DEF's Amanda Tuminelli and Variant's Daniel

Barabander and Jake Chervinsky entitled "Through the Looking Glass: Conceptualizing Control and Analyzing Criminal Liability For Unlicensed Money Transmitting Businesses Under Section 1960."

The paper takes a deep dive into 18 U.S.C. § 1960, a statute at the center of the Tornado Cash and Samurai Wallet cases, criminalizing the operation of an "unlicensed money transmitting business" and subjecting violators to harsh penalties, in an effort to provide clarity on who exactly the statute exposes to criminal liability.

At a high-level, the main conclusion of the paper is that in order for an entity to fall within the scope of 1960, they must be "money transmitting" – transferring funds on behalf of the public – which requires them to have control over the funds at issue.

Policy Priority

There is an urgent need to clarify the definition of "money transmitter" under Section 1960 to exclude developers of open-source, permissionless blockchain protocols. Section 1960 of the U.S. Code criminalizes operating an unlicensed "money transmitting business." Originally designed to combat illicit financial activities, recent interpretations by federal agencies like the Department of Justice and the Financial Crimes Enforcement Network (FinCEN) have overreached, targeting software developers and non-custodial protocols.

Notable Quotes

"On the definition of 'money transmitting,' we conclude that a party transmits funds for purposes of Section 1960(b)(1) when it both obtains control of funds and relinquishes control of those funds. We support our conclusion by analyzing the definition of 'money transmitting' set forth in Section 1960(b)(2), and all federal circuit court cases that substantively interpret the language of the statute, including a discussion of key Second Circuit precedent from United States v. Bah and United States v. Velastegui. We also explain the interplay between Section 1960 and the definition of 'money transmitting business,' also found in the BSA, 31 U.S.C. § 5330. We conclude that although Section 1960 does not adopt the BSA definition, Section 5330's definition is substantively similar and confirms that the plain language of 'money transmitting' means the act of both obtaining control and relinquishing control of funds." (Pg. 8)

"... the threshold question in a Section 1960 prosecution is if the defendant operated a 'money transmitting business,' and the sine qua non of 'money transmitting' is obtaining control and relinquishing control of funds. If a business does not engage in this prerequisite activity, then Section 1960 does not apply, even if the business is otherwise 'unlicensed.' For years, the blockchain industry has developed and deployed non-custodial smart contract protocols consistent with this view of the law. Although the vagueness and ambiguity of the statute has caused significant confusion, our analysis validates the industry's approach to anti-money laundering compliance and rebuts the interpretation put forward by the government and adopted by the court in Storm." (Pg. 9)

"The government did not allege, and the court did not imply, that the Tornado Cash developers created a commercial enterprise with the objective of providing money transmitting services—the first factor. In fact, the Indictment acknowledges the contrary—the software developers set out to build a privacy-preserving software protocol that would allow users to engage in self-directed peer-to-peer transactions. The protocol was always intended to be, and indeed was, self-custodial, meaning users never gave up control or custody of their funds to Tornado Cash. Therefore, as explained above, it could not have been the goal of the "business" to engage in 'money transmitting' (to 'transfer funds on behalf of the public') for the purpose of Section 1960." (Pg. 30)

"... the government has stretched Section 1960 far beyond its proper limits. Instead of confining the statute to those whom Congress intended to target—unlicensed business operators who knowingly obtain and relinquish control of customer funds—the government has sought to apply the statute to software developers who build technology that is later misused by third parties. If the government were correct, then Section 1960 would become not merely a powerful tool, but rather, an unchecked license to prosecute blockchain developers and participants who are powerless to prevent money laundering." (Pg. 42)

Available at: https://edit.financialcrimelitigators.org/api/assets/cd682a1c-1cb0-4c99-a491-ac6155f4bdc2.pdf

Square Peg in a Round Hole: Why the Bank Secrecy Act Should Not Apply to Blockchain Participants

Lizandro Pieper and Gavin Zavatone

On November 20, 2024, the DeFi Education Fund ("DEF") published a new paper written by DEF's Lizandro Pieper and Gavin Zavatone entitled "Square Peg in a Round Hole: Why the Bank Secrecy Act Should Not Apply to Blockchain Participants."

The paper investigates the history and design of the Bank Secrecy Act (BSA), its application to crypto, and explains why software providers and operators across the technology stack are not subject to the BSA.

Policy Priority

Support for legislation like the Blockchain Regulatory Certainty Act (BRCA), introduced by GOP Majority Whip Tom Emmer (R-MN), and cosponsored by Representatives Bill Huizenga (R-MI), Ritchie Torres (D-NY), and Josh Gottheimer (D-NJ), which excludes certain non-controlling blockchain developers and blockchain services providers from being defined as "money transmitters." The BSA establishes government oversight over money transmitters and other financial intermediaries that move or control money on behalf of their customers, and subjects them to stringent reporting and disclosure requirements on customers and their transactions. However, in DeFi, users maintain total control of their digital assets by simply leveraging cryptographic software and a decentralized communications network to send and receive value without a third party.

BRCA one-pager:
https://www.defieducationfund.org/_files/ugd/84ba66_82c3fe9c9a6a41bb9dab2ce6ef82ef74.pdf

Notable Quotes

"... FinCEN clarifies what it means to 'accept and transmit' funds on behalf of another person multiple times in guidance. Specifically, in the 2019 Guidance, FinCEN develops four criteria for determining the regulatory treatment of persons involved in wallet applications: '(a) who owns the value; (b) where the value is stored; (c) whether the owner interacts directly with the payment system where the [cryptocurrency] runs; and (d) whether the person acting as intermediary has total independent control over the value.' While this criteria specifically applies to wallet applications, it serves as the appropriate criteria for any participant and software protocol or application across the [cryptocurrency] technology stack because, ultimately, if there is no 'acceptance' of funds such that the provider has 'total independent control' of them, then the nature of transactions flowing through the software protocol or application do not require customer or recipient identification in the same way that traditional financial intermediaries do. Therefore, it is more accurate to deem software providers and operators as tool manufacturers and communication providers than intermediaries.

In determining the application of BSA requirements to the providers and operators of CVC technologies, it is critical to consider the nature of the technology and how its users interact with it. As explained in the next section, when CVC users custody their own assets to use decentralized networks directly, they have total independent control over their own assets and no one in the CVC technology stack accepts and transmits users' assets on their behalf, nor are they attempting to. Whether it's a wallet that provides storage; a front-end that allows access to a network; or a protocol that uses code to execute transactions upon users' instructions, full control remains with the user." (Pg. 14)

"... miners and validators have no practical way of meeting BSA obligations should they be deemed money transmitters. This is because blockchain transactions involve wallet addresses, not personally identifiable information like individual's names and addresses, which would make it difficult or impossible to identify users in block creation. Also, because these networks consist of unrelated persons from around the globe, the ability to carry out compliance is highly constrained." (Pg. 28)

"... unhosted wallet providers cannot functionally comply with BSA obligations for money transmitters either. Unhosted wallet providers do not collect identifying information of persons who choose to purchase their software products—much like a safe manufacturer does not identify persons who purchase their safes. So even with blockchains' transparency and traceability, unhosted wallet providers cannot track their customers' qualifying transactions (over $10,000) without connecting an identity to a wallet address. Imposing information collection requirements on unhosted wallet providers so they may comply with the BSA would be akin to imposing these requirements on safe manufacturers—it's nonsensical." (Pg. 28)

"... the BSA's information collection regime in general is predicated on the notion that customers voluntarily provide their personal information to traditional financial services businesses. This is quite

different from operating, providing, and using software tools, as doing so does not require users to share any information about themselves with anyone to use the technology. Should software providers and operators be required to comply with the BSA as money transmitters, users would no longer be voluntarily providing their identifying information and be forced to surrender their right to privacy. This is coercion in the strictest sense and should be met with scrutiny under the Fourth Amendment." (Pg. 28)

Available at: https://www.defieducationfund.org/_files/ugd/84ba66_a568e222f78048e2a8625abb76d3b0fc.pdf

DEF Coalition Letter calling on Congress to correct the DOJ's inconsistent, overly expansive interpretation of Section 1960, the criminal code provision regarding operating an "unlicensed money transmitting business," as applied to software developers (March 2025)

"Logically, if a person is not operating a 'money transmitting business' as defined in the statutes requiring the licensure of money transmitting businesses, that person should not be subject to criminal liability for operating an 'unlicensed money transmitting business.' This interpretation conforms with Congressional intent and common sense. As explained by Senators Lummis and Wyden: [T]he statutes and regulations are clear that direct receipt and control of assets are required elements of money transmission. Indeed, this limiting factor is essential, otherwise a wide range of additional services such as internet service providers or postal carriers could inadvertently be caught in the definition of a money transmitting business since they routinely send, receive and process information and messages regarding payments.'"

"If left unaddressed, the DOJ's departure 'from the clear, logically sound, and well-established definition of "money transmission" established by FinCEN' would expose every technology developer of non-custodial software within the reach of the U.S. to criminal liability. The resulting, and very rational, fear among developers would effectively end the development of these technologies in the United States, push U.S. innovators overseas, and tarnish confidence in the DOJ's respect for the rule of law. The federal government should not be playing a game of bait and switch. Congress should urge the DOJ to correct its misapplication of the law, and clarify Section 1960 to more clearly convey Congress's intent."

Available at: https://www.defieducationfund.org/_files/ugd/84ba66_903d8c40e59a422e81b3abe393ca9536.pdf

Securities Laws

SEC Crypto Task Force Guiding Principles for a Token Safe Harbor

DeFi Education Fund (DEF) submitted Guiding Principles for a Token Safe Harbor Framework to the Securities and Exchange Commission (SEC) Crypto Task Force. A safe harbor is a legal framework that shields good-faith actors from certain liability or penalties under defined conditions, offering regulatory clarity and peace of mind to market participants.

As background, in February 2025, SEC Commissioner Hester Peirce issued a request for comment: "There Must Be Some Way out of Here." In the request for information, Commissioner Peirce requested public feedback on a potential safe harbor from registration under the Securities Act of 1933. Back in 2021, Commissioner Peirce proposed that the Commission put in place a non-exclusive safe harbor to provide a time-limited exemption from the registration requirements under the Securities Act of 1933 for offers and sales of tokens during the development of a functional or decentralized blockchain network.

DEF supports the Commission's articulated goal of promoting a "regulatory environment that protects investors, facilitates capital formation, fosters market integrity, and supports innovation." A thoughtfully calibrated safe harbor—appropriately tailored to the realities, risks and opportunities of digital assets and blockchain technologies—will provide important clarity to the public, token holders, and projects building in this space while the longer-term legislative and regulatory policymaking processes play out.

DEF submitted five guiding principles for inclusion in the Token Safe Harbor, which are described in detail in our letter: (1) technology-agnostic rules and policies, (2) broad and inclusive eligibility criteria for the Safe Harbor, (3) appropriately calibrated disclosure and compliance considerations, (4) clear and well-defined exit criteria, and (5) appropriate treatment of secondary market activity.

Available at:
https://www.defieducationfund.org/post/defi-education-fund-submits-guiding-principles-for-token-safe-harbor-to-sec-crypto-task-force.

SEC Crypto Task Force DAO Submission

On May 27, 2025, DeFi Education Fund (DEF) and Uniswap Foundation (UF) submitted a proposal to the SEC Crypto Task Force on the treatment of Decentralized Autonomous Organizations (DAOs) under the securities laws. Our submission is in response to Commissioner Hester Peirce's February 21, 2025, request for comments, "There Must Be Some Way Out Of Here," in which she solicits comments on a proposed safe harbor exempting certain decentralized projects and tokens from securities registration. DEF previously submitted Guiding Principles for a Token Safe Harbor to the Task Force in April of 2025.

DEF and UF present two main theses for consideration: (1) dispersion of control over the governance of a network is the most workable framework for determining if a network is sufficiently decentralized for purposes of the proposed safe harbor from registration, or under the test for an "investment contract" security under Howey, and (2) there are no material information asymmetries in a sufficiently decentralized network, which reinforces that federal securities laws do not apply to network tokens or transactions in which a network token is the object. DEF and UF also argue that DAOs with truly decentralized governance should not be treated as securities issuers, as they lack traditional centralized control and the accompanying managerial efforts.

We recommend three principles that the Commission should adopt to better account for the realities of DAOs and decentralized governance:

- The Commission should treat DAOs with decentralized control over governance of the network as nothing more than disparate and dispersed groups of people, unless facts are developed that indicate otherwise.
- The Commission should recognize that DAOs with decentralized control over the governance of the network are not an identifiable and coordinated group of "others" undertaking efforts for the purposes of the "efforts of others" prong of a Howey analysis.
- The Commission should recognize that blockchain records are a uniquely transparent and immutable resource that eliminates informational asymmetries.

Available at: https://www.defieducationfund.org/_files/ugd/84ba66_0114836a70d042b893f09c731352a775.pdf

Senate Finance Committee: Selected Issues Regarding the Taxation of Digital Assets

DEF Comment Letter

Policy Priorities

In its comment letter to the Senate Finance Committee, DEF outlined key recommendations for fair and practical digital asset taxation, emphasizing the need to align tax policy with the unique economic realities of blockchain technologies. DEF argued that staking rewards should only be taxed upon sale, Section 6050I reporting requirements should be revised to avoid privacy violations, and that Congress should modernize tax rules to encourage innovation while reducing unnecessary burdens on cryptocurrency users. These recommendations aim to foster a balanced approach to taxation that supports the growth of the digital asset ecosystem.

Notable Quotes

"... validator rewards should be treated as self-sourced property because they consist predominantly of newly minted tokens, not gas fees, and newly minted tokens do not have a payer. Taxpayers are never taxed until sale when they extract minerals like gold, breed livestock, produce art, manufacture goods, or otherwise assume ownership over property for which no previous owner exists (self-sourced property). This treatment remains even if an active secondary market exists for that self-sourced property, as it does for many commodities. Validators attain newly minted tokens by running and maintaining open-source software on their computers; in effect, they are digital farmers vying to pick fruit from a tree that grows on public property. They should not be taxed until they sell the fruit." (Pg. 3)

"... there is no third-party intermediary required to collect information from transacting parties to execute a blockchain transaction; hence, there is no central server storing user data that is susceptible to hacks. Section 6050I would change that by deputizing taxpayers to collect personal information from others that would encourage the proliferation of "information honeypots" ripe for exploitation by hackers." (Pg. 5)

"... Section 6050I forces Americans to reveal their personal information to others. Associating an American's public key with their identity gives the world access to every on-chain transaction the American has engaged in, potentially exposing intimate details about them. That forced exposure is not only bad policy; it also raises serious constitutional questions." (Pg. 5)

Additional Considerations

Department of the Treasury

Office of Foreign Assets Control (OFAC): Sanctions Tornado Cash Mixer

In August 2022, OFAC sanctioned the DeFi protocol Tornado Cash for allegedly supporting cyber-malicious activities and money laundering schemes. In doing so, OFAC blocked "all property and interests in property of [Tornado Cash] that is in the United States or in the possession or control of U.S. persons" and "any entities that are owned, directly or indirectly, 50 percent or more by one or more blocked persons." Additionally, "all transactions by U.S. persons or within (or transiting) the United States that involve[d] any property or interests in property of designated or otherwise blocked persons [were] prohibited unless authorized by a general or specific license issued by OFAC, or exempt. These prohibitions include[d] the making of any contribution or provision of funds, goods, or services by, to, or for the benefit of any blocked person and the receipt of any contribution or provision of funds, goods, or services from any such person."

In *Joseph Van Loon v. Department of Treasury*, the Fifth Circuit Court of Appeals ruled that the "immutable smart contracts at issue in this appeal are not property because they are not capable of being owned." The Fifth Circuit went further, pointing out that "because these immutable smart contracts are unchangeable and unremovable, they remain available for anyone to use and 'the targeted North Korean wrongdoers are not actually blocked from retrieving their assets,' even under the sanctions regime." As the Fifth Circuit noted, users are interacting with software that is not controlled by a third party.

In March 2025, OFAC officially announced the delisting of Tornado Cash from its Specially Designated Nationals (SDN) and Blocked Persons List following years of litigation on the issue. This included the delisting of the Tornado Cash front-end website, as well as smart contracts making up the protocol. In April 2025, upon the instructions of the Fifth Circuit, the U.S. District Court for the Western District of Texas held that OFAC acted unlawfully when it added Tornado Cash's smart contracts to the SDN list and permanently enjoined the agency from enforcing those specific sanctions.

Nonetheless, while Tornado Cash is now free from being redesignated, the government's sanctions have raised key issues about how they are regulated: Can autonomous, open-source software be treated as a sanctionable entity? Does this approach jeopardize financial privacy and innovation by criminalizing the use of neutral tools? These actions have sparked a critical debate over the limits of government authority in regulating decentralized systems.

DEF District Court Amicus Brief re. Joseph Van Loon v. Department of Treasury

DEF argued that OFAC's sanctions on Tornado Cash lack a statutory basis and overextend the agency's authority. DEF emphasized that sanctioning immutable smart contracts punishes a neutral tool rather than any individual or entity misusing it, creating a dangerous precedent for decentralized technologies.

Available at: https://www.defieducationfund.org/_files/ugd/84ba66_9052b828ba2d4eefac43aa13bf93d022.pdf

DEF Fifth Circuit Amicus Brief re. Joseph Van Loon v. Department of Treasury

DEF argued that OFAC's sanctions improperly extended to domestic transactions, exceeding the agency's legal authority under the International Emergency Economic Powers Act (IEEPA). DEF highlighted that Tornado Cash's legitimate uses for financial privacy outweigh its potential misuse, urging the court to overturn the sanctions to protect innovation and privacy rights.

Available at: https://www.defieducationfund.org/_files/ugd/e53159_dc5e8345b3d34bd4af4d06663c12d413.pdf

Financial Crimes Enforcement Network (FinCEN): Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class of Transactions of Primary Money Laundering Concern, Docket No. FINCEN-2023-001

DEF Comment Letter

DEF's January 2024 comment letter to FinCEN raises concerns about the agency's proposed rule on convertible virtual currency (CVC) mixers, arguing that its overbroad definitions could label nearly all crypto transactions as "high risk." DEF contends that this approach misunderstands the legitimate uses of mixers for financial privacy and imposes disproportionate compliance burdens on the industry. Instead, DEF recommends that FinCEN focus on enforcing existing regulations rather than creating new rules that risk driving innovation offshore and infringing on users' privacy.

Available at: https://www.defieducationfund.org/_files/ugd/84ba66_a5bb9050d8414cbab3f0285202464a29.pdf

Notable Policy Wins for DeFi

IRS Broker CRA Signed into Law

H.J. Res. 25, legislation to disapprove of the DeFi-focused portion of the Treasury Department's Internal Revenue Service's (IRS) Broker Rule "'Gross Proceeds Reporting by Brokers That Regularly Provide Services Effectuating Digital Asset Sales

The finalized "broker" rulemaking by the IRS and Department of Treasury would have imposed sweeping obligations on software developers and unhosted wallet providers, raising critical questions about the boundaries of regulatory authority. The rule could have required software developers to collect and report user data they cannot access, potentially stifling innovation and driving blockchain development outside the U.S.

Put simply, the DeFi broker rule attempted to achieve tax-reporting in DeFi by forcing website developers or anyone "assisting customers in initiating" a transaction to be treated as a "broker," undermining the disintermediated nature of the technology. Specifically, Treasury purported to redefine the statutory term "broker" – which Congress defined to reach only those who, "for consideration . . . effectuat[es] transfers of digital assets on behalf of another person," to reach anyone who provides a "trading front-end service" or "other effectuating services," even if they do so for free and even if the service does not itself effectuate transfers.

In other words, the finalized rule was so broad as to capture any service that is supposedly "assisting customers in initiating" a transaction as a "broker," including front-ends and even web browsers, and internet-service-providers (ISPs). The rule fundamentally exceeded the Treasury's statutory authority, disregarded the technological realities of DeFi, and would have violated the privacy of millions of DeFi users.

In April 2025, President Trump signed into law House Joint Resolution 25, legislation to disapprove of the decentralized finance-focused portion of the Treasury Department's Internal Revenue Service's (IRS) Broker Rule "'Gross Proceeds Reporting by Brokers That Regularly Provide Services Effectuating Digital Asset Sales," which would have had devastating effects on DeFi technology in the United States. With President Trump's signature, the rule is officially disapproved and voided, and the United States has passed its first ever crypto legislation – a watershed moment for DeFi. On March 4, 2025, the Senate voted on Senate Joint Resolution 3 (S.J. Res. 3), Senator Ted Cruz's (R-TX) CRA resolution. In a heavily bipartisan 70-27 vote, the resolution passed.

The CRA victory is significant in that it was the first time Congress explicitly recognized the difference between DeFi and centralized intermediaries. Through the CRA, both the Administration and the intent of Congress was expressed to formally disapprove of the flawed rule and to protect Americans' right to transact through decentralized software protocols and maintain self-custody of their digital assets.

Blockchain Association, Texas Blockchain Council, Defi Education Fund v. Internal Revenue Service, United States of America, United States Department of The Treasury, and Janet Yellen

On December 27, 2024, the DeFi Education Fund, the Blockchain Association, and the Texas Blockchain Council filed a lawsuit in the U.S. District Court for the Northern District of Texas, challenging the Internal Revenue Service's ("IRS") and Treasury Department's final "broker" midnight rulemaking on the basis that the rulemaking exceeds the agencies' statutory authority, violates the Administrative Procedure Act ("APA"), and is unconstitutional.

During the rule's comment period, the public warned the IRS and Treasury that moving forward with the rule would cripple the digital asset industry. But the government ignored this feedback, leaving the digital asset sector with a rule that puts unlawful compliance burdens on software developers who build so-called "trading front-end services." This midnight rule would have stifled innovation and burdened American entrepreneurs.

Available at: https://www.defieducationfund.org/_files/ugd/84ba66_b6af3a8d9414462d8a34897cfec39c5e.pdf

DEF Comment Letter

DEF's June 2024 response to the IRS's comment request on digital asset proceeds from broker transactions highlighted significant flaws in the proposed reporting framework. DEF argued that the broad definitions of "broker" and "digital asset middleman" would create impractical compliance burdens for decentralized finance participants by requiring data collection that is inaccessible in decentralized systems. These rules risk undermining innovation, violating user privacy, and discouraging blockchain development in the U.S.

Available at: https://www.defieducationfund.org/_files/ugd/84ba66_3d28a7b618dc49cda4f661fa795eed6f.pdf

DEF Comment Letter

In its November 2023 comment letter to the IRS, DEF criticized the agency's proposed broker rulemaking, warning that its overly broad definitions of "broker" and "digital asset middlemen" could impose unworkable compliance burdens on decentralized technologies. DEF argued that requiring participants in DeFi systems to collect and report user data they cannot access or secure risks violating privacy rights and creating undue barriers for innovation. The letter urged the IRS to develop rules that align with the decentralized nature of blockchain systems, protecting both users and developers while ensuring compliance.

Available at: https://www.defieducationfund.org/_files/ugd/e53159_40d4255857d142f2a1744be79f1dab3f.pdf

GENIUS Act Signed into Law

In July of 2025, the Guiding and Establishing National Innovation in U.S. Stablecoins (GENIUS) Act was signed into law following a bipartisan supermajority vote in both chambers of Congress. GENIUS is significant for DeFi in that it recognizes decentralized blockchain networks as base layer infrastructure in a dollar-backed global financial system, protects peer-to-peer transactions in stablecoins, and explicitly treats DeFi differently than centralized intermediaries, securing affirmative language for the future of DeFi infrastructure. Whether used in swapping tokens on decentralized trading protocols; providing DeFi liquidity, remittances, spending; or transacting peer-to-peer, stablecoins play a critical role in onchain digital asset markets.

While the GENIUS Act is limited to establishing a regulatory framework for centralized payment stablecoin issuance, some provisions of the bill regulate secondary trading on centralized venues. As DEF has emphasized, decentralized protocols and developers of such protocols should not be treated like centralized intermediaries. Particularly critical in GENIUS is the definition of "digital asset service provider," which regulates the secondary trading of payment stablecoins on intermediated venues.

Importantly, the definition of digital asset service provider (DASP) is limited to centralized actors who custody and control user assets, including those who engage in the business of exchanging, transferring, custodying, or issuing digital assets on behalf of customers or users in the U.S. The definition critically excludes decentralized distributed ledger protocols and self-custodial software interfaces, ensuring that DeFi is protected from regulation suited for centralized financial intermediaries. This validates that the government views secondary transactions in stablecoins as peer-to-peer, and, if passed, will be the first time the U.S. government has codified this recognition into federal law.

DEF GENIUS blog:
https://www.defieducationfund.org/post/genius-act-signed-into-law-ushering-in-first-federal-digital-assets-framework
Full text of GENIUS: https://www.govinfo.gov/content/pkg/BILLS-119s1582es/pdf/BILLS-119s1582es.pdf

SEC "Exchange" and "Dealer" Rulemakings Dropped

Notice of Proposed Rulemaking to further define the phrase "as a part of regular business" as used in the statutory definitions of "dealer" and "government securities dealer" under Exchange Act 3(a)(5) and 3(a)(44); File No. S7-12-22

In August 2022, the SEC proposed a rulemaking that would more broadly define which securities market participants are considered "dealers." The rulemaking created a qualitative test to determine which liquidity providers need to register as dealers. Under the proposed rule, an active trader that does not have any clients may still be considered a "dealer" and be required to register with the SEC.

In November 2024, the U.S. District Court vacated the SEC's Dealer Rule after a lawsuit by the Blockchain Association and Crypto Freedom Alliance of Texas. The court ruled the SEC exceeded its authority, protecting DeFi participants and liquidity providers from overreach.

DEF Comment Letter

DEF's May 2022 response to the SEC's "Dealer" Rulemaking raised concerns that the proposal could unintentionally classify large DeFi market participants and liquidity pools as dealers under securities laws. This overreach would subject these participants to arbitrary enforcement actions and compliance requirements designed for traditional financial intermediaries, creating significant legal uncertainty. DEF argued that the rule's vague language fails to account for the unique nature of decentralized systems and could harm innovation and liquidity in the DeFi ecosystem.

Available at: https://drive.google.com/file/d/1GC4QPms1JxzrBr7sLDlSzoVVk3EcTsNP/view

Notice of Proposed Rulemaking on Amendments to Exchange Act Rule 3b-16 Regarding the Definition of "Exchange"; Regulation ATS for ATSs That Trade U.S. Government Securities, NMS Stocks, and Other Securities; Regulation SCI for ATSs That Trade U.S. Treasury Securities and Agency Securities; File No. S7-02-22

In January 2022, the SEC proposed "Amendments to Exchange Act Rule 3b-16 Regarding the Definition of Exchange," and included an overly broad definition of an "exchange" that would have included DeFi protocols. Then, in 2023, the SEC doubled-down, re-opened its rulemaking, and proposed an expanded definition of "exchange" that would regulate any entity that "makes available" a "communication protocol system" that individuals use to trade securities. This definition would have had near unlimited reach and was fundamentally incompatible with DeFi technology. Specifically, it would have required DeFi protocols and software developers to register as trading systems, which would have been inappropriate and in some cases, impossible. DEF filed three comment letters relating to the proposed rule in April 2022, June 2022, and June 2023.

On June 12, 2025, the SEC officially dropped their proposed "exchange" rulemaking, ending a failed attempt to expand the law beyond its statutory limits by capturing decentralized trading protocols under the proposed regulation.

SEC Final Rule:
https://www.sec.gov/rules-regulations/2025/06/substantial-implementation-duplication-resubmission-shareholder-proposals-under-exchange-act-rule#33-11377final

DEF First Comment Letter

DEF's April 2022 response to the SEC's proposed Exchange Rulemaking warned that the rule's overly broad language could unintentionally include DeFi protocols and participants under its scope. By redefining "exchanges" to potentially encompass decentralized platforms, the proposal risked stifling

innovation and driving blockchain development offshore. DEF highlighted the lack of clarity in the rule, which failed to address how it would apply to decentralized systems and omitted specific mentions of crypto, DeFi, or digital assets.

Available at: https://drive.google.com/file/d/1cjQIDH3VE9303k-r55lQFfn1v-tH5l0n/view

DEF Second Comment Letter

DEF's June 2022 response focused on the proposal's failure to adapt to the unique and evolving nature of decentralized finance. The letter argued that the SEC's static regulatory framework would impose disproportionate burdens on DeFi protocols, harm U.S. competitiveness, and fail to provide consumer protections that align with blockchain's decentralized structure. DEF emphasized that a one-size-fits-all approach to regulating exchanges undermines innovation and risks misapplying securities laws.

Available at: https://drive.google.com/file/d/1inWXw7MSO8VjrbuPro8izeewgmRGNC9r/view

DEF Third Comment Letter

DEF's June 2023 response criticized the SEC's attempt to expand the definition of "exchange" under Rule 3b-16, arguing that the agency exceeded its statutory authority and procedural rulemaking requirements. DEF contended that applying centralized regulatory models to decentralized platforms ignores their unique characteristics and creates significant uncertainty for the industry. The letter emphasized that these changes could lead to a de facto ban on DeFi in the U.S., discouraging participation and development.

Available at: https://www.defieducationfund.org/_files/ugd/84ba66_f997b07bbb6d43b8a3b6c0626f57cdf3.pdf