DeFi 101

Curated by the DeFi Education Fund

DeFi Education Fund

defieducationfund.org

About the DeFi Education Fund

The DeFi Education Fund is a nonpartisan research and advocacy group working to explain the benefits of DeFi, achieve regulatory clarity for the future of the global digital economy, and help realize the transformative potential of DeFi for everyone.

We exist because DeFi has immense potential for human prosperity, but that can only be realized with buy-in from governments and appropriate policy. We work to help realize DeFi's promise by educating regulators and policymakers and advocating for smart approaches.

To contact us, or schedule a “DeFi 101 briefing,” please send a note to max@defieducationfund.org

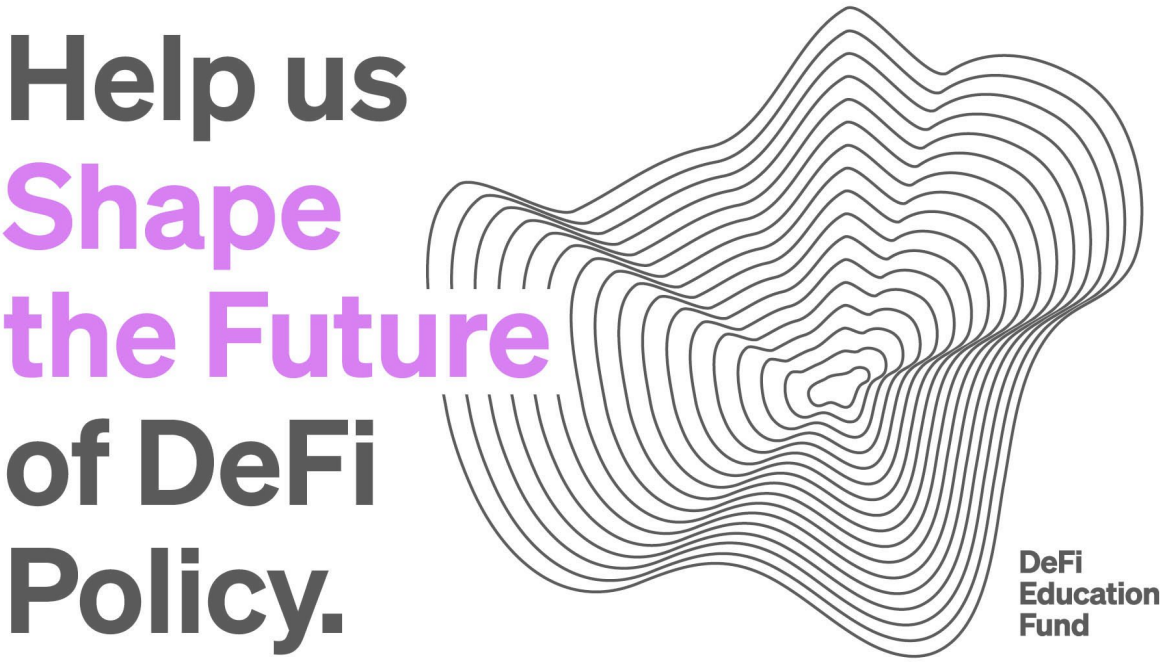

Table of Contents

DeFi Explainers

Public Blockchains

Peer-to-Peer Protocols and Networks

At the foundation of decentralized finance (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 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 people or businesses 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 a P2P network's data and communicating information between nodes 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 or summarizes 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 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 state of the blockchain.

Consensus Mechanisms

Before a transaction reaches miners or validators (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 rapidly expanding.

Nodes in a PoW network adopt the longest chain as a consensus for maintaining network synchronization. This is because the longest chain has accumulated the most proof of work, indicating that it has the highest level of computational effort and 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, takes a different consensus approach. In PoS, Ethereum divides block production into time intervals known as *slots*. For each slot, the blockchain protocol randomly selects a single node validator to propose a new block and broadcast it to the entire

network. Once broadcasted, the larger set of validators 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 and the nodes notify each other. 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—i.e., participants are willing to stake their assets on its validity, signaling their confidence in that chain.

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". Keys kept in hot storage are connected to the internet. In contrast, users of cold storage wallets store keys offline, adding another layer of security to them as keys are not exposed to internet-based attacks. To perform transactions with cold storage, a user signs transactions offline with their private keys, and then the signed transaction is transferred to an online device (e.g., computer or mobile phone) to be broadcast to the blockchain network. For example, if a user had a hardware wallet—i.e., a physical device used for cold storage—and wanted to send a transaction, the user could connect the wallet to a computer and open an application compatible with the hardware wallet to input the transaction details.

In contrast, third-party custodians offer hosted wallets as a service for custodying users' assets on their behalf. For a hosted wallet, the custodian maintains the private key instead of the user. 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 program known as a *smart contract* to automatically execute certain actions when a user initiates the transaction and 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 upon receiving the transaction. 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 that need to be provided to 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 the governing arrangement designed to ensure distributed authority among a decentralized and disaggregated group of unrelated users. DeFi protocols offer communication, connectivity, or software services that parties can utilize to communicate trading interests, but they do not intermediate transactions. Hence, even when DeFi protocols originate from a single software developer or small group of developers, they maintain their decentralization.

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.

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. 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.

Upgradability

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 separates the state (i.e., data) from the business logic (i.e., code that dictates how the smart contract behaves). This is done by having one smart contract solely for data and one contract for logic. 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. Essentially, when a buyer's order matches a seller’s order, the smart contract automatically executes the transaction and it is then validated and recorded on the blockchain. These transactions are executed by software (smart contracts) and not a centralized entity overseeing the exchange, ensuring a trustless and P2P trading environment.

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 exchanges are validated by the underlying blockchain, new prices are calculated in real-time. One benefit of this is that an exchange cannot manipulate asset pricing as it is mathematically formulated.

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 their price based on the ratio formula above.

Front-End Websites

Accessing a DeFi protocol for those with less technical expertise begins with obtaining a wallet. As previously explained, the wallet provides a front-end interface (i.e., a website or application) that facilitates communication between the user and the DeFi protocol over the internet. It displays the user’s public key for receiving assets in a variety of ways, such as a long string of characters or a QR code.

When initiating the transaction, the wallet 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 transactions are validated, the amount of digital assets associated with a given public address is updated. To further simplify the process, front-end websites have been developed for users to easily connect their wallets and perform actions on a DeFi protocol.

For clarification, the front-end does not intermediate the transaction itself, it acts more as 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, DeFi front-ends "translate" human-understandable activities into a data form that blockchains can understand.

Relayers

Generally, relayers are a third party service—i.e., a software application typically run by an individual or group—that organizes transactions on behalf of users. Essentially, after a front-end generates the transaction data required to interact with the relevant smart contracts, it sends the data to a relayer. The relayer verifies that all the data is complete and correct before it optimizes the transaction. What this means is that the relayer determines the optimal gas fee for the transaction based on the current network conditions. While relayers recommend the optimized gas fees, users still have to approve the gas fee, as they have to approve the transaction overall. For complex transactions involving multiple steps, the relayer ensures that the steps are organized in the correct sequence to mitigate the risk of error. Overall, relayers are used for gas optimization and for organizing complex transactions. Importantly, relayers do not take custody of users' assets and those assets remain in the user's possession throughout an interaction with a relayer. Users still approve the transaction with their private key before it is broadcasted to the network. In other words, a relayer does not control the movement of funds.

RPC Nodes

After a user approves a transaction with their private key, the wallet application broadcasts 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 wallet 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. Importantly, the difference between an RPC node and a relayer is that a relayer organizes data for the RPC node to broadcast to the network. Even in the case of a privacy-enhancing relayer, the relayer still uses an RPC node to broadcast the transaction.

Important Concepts

Open-Source

“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.”

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

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

Bank Secrecy Act (BSA)

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 Crime 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 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 in 2023 by Representative Tom Emmer (R-MN), which excludes "a blockchain developer or provider of a blockchain service" from being subject to the BSA. The BSA establishes government oversight over banks 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.

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

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

DEF Comment Letter

Lizandro Pieper

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

Internal Revenue Service (IRS): Gross Proceeds Reporting by Brokers that Regularly Provide Services Effectuating Digital Asset Sales

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

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 will stifle innovation and burden American entrepreneurs—if it stands.

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

DEF Comment Letter

Miller Whitehouse-Levine and Amanda Tuminelli

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

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.

The government's sanctions against Tornado Cash posed serious threats to decentralized technologies, raising 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 First 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 First Amicus Brief re. Joseph Van Loon v. Department of Treasury

DEF contended 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 Crime 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

Miller Whitehouse-Levine, Amanda Tuminelli, and Lizandro Pieper

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

Securities and Exchange Commission (SEC)

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 new 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

Miller Whitehouse-Levine

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 August 2022, the SEC issued a proposed rule purportedly to “include significant treasury markets platforms within regulation ATS.” The “proposal would enhance investor protections and cybersecurity for alternative trading systems that trade treasuries and other government securities,” the SEC’s press release explained.

DEF First Comment Letter

Miller Whitehouse-Levine

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

Miller Whitehouse-Levine and Jake Chervinsky

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

Miller Whitehouse-Levine and Jake Chervinsky

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

Regulation by Enforcement

The crypto community had been under attack for years by the SEC, which had refused to publicly clarify basic rules for digital asset transactions and sidestepped Congress to engage in a destructive enforcement crusade based on its "poorly conceived crypto policy." The agency's freestyle policymaking during Chair Gary Gensler's tenure meant that anyone seeking to do anything with a digital asset had to fear being the SEC's next target.

Beba LLC and DeFi Education Fund v. Securities and Exchange Commission

DEF, alongside Beba LLC, argued that the SEC's approach violates the Administrative Procedure Act by imposing significant regulatory burdens without proper notice or public input. DEF contended that treating token airdrops as securities stifles innovation and creates unnecessary barriers for blockchain businesses, advocating instead for clear and balanced regulatory guidance.

Available at: https://www.defieducationfund.org/_files/ugd/84ba66_3f7a8f2ca6614d7381122cb1beeed4a8.pdf

DEF Amicus Brief re. SEC v. Coinbase

DEF filed an amicus brief supporting Coinbase's motion for judgment on the pleadings, arguing that the SEC's application of securities laws to digital assets is inappropriate and stifles innovation. DEF contended that the SEC's approach lacks clear guidelines, creating uncertainty for the industry.

Available at: https://www.defieducationfund.org/_files/ugd/84ba66_05b10d3583a647b08dd071727ab8b7f1.pdf

DEF Amicus Brief re. SEC v. Kraken

DEF argued that applying traditional securities regulations to decentralized staking services is inappropriate and stifles innovation. DEF contended that staking, as a fundamental blockchain process, should not be subjected to the same regulatory framework as traditional financial securities.

Available at: https://www.defieducationfund.org/_files/ugd/84ba66_7c5fd096e8234f9bb66e4629d5f31b60.pdf