The Growth and Regulatory Challenges of Decentralized Finance

TAC Virtual Currency Subcommittee
December 14, 2020

Aaron Wright, Cardozo Law School
Gary DeWaal, Katten Muchin Rosenman LLP

Overview Decentralized Finance

Decentralized finance (“DeFi”) is a fast-growing sector of the blockchain ecosystem.

DeFi protocols use smart contracts to create financial services and other products that are non-custodial in nature.

They ideally do not rely on one central party, but in practice many still do.

DeFi Lexicon

DeFi applications are administered via online portals, called "**dApps**," and are often supported by individuals that pool together assets in a "**liquidity pool**."

Those that deposit assets in a liquidity pool "**lock their assets**" and often earn fees and/or automatically receive digital assets in the form of "**governance tokens**."

The practice of submitting assets to a DeFI protocol is increasingly referred to as "**liquidity mining**." The process of earning fees and/or governance tokens is referred to as "**yield farming.**"

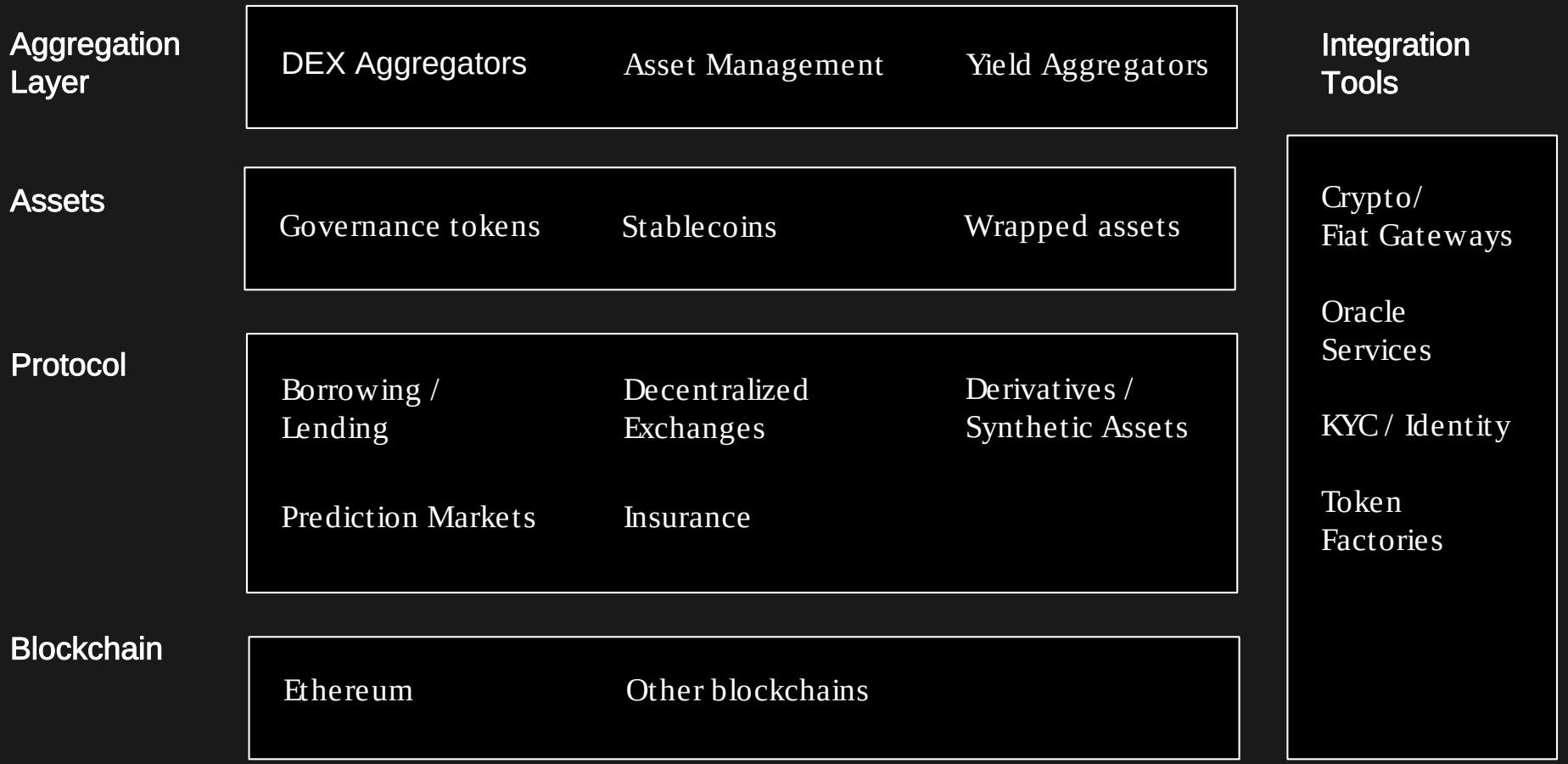
Decentralized Finance is Growing

Digital assets are developing a yield curve, an arguable basis for value, which is dependent on the time value of locked assets.

Decentralized Finance Landscape

The landscape of DeFi is growing with both smart contract-based protocols and centralized aggregation tools.

- **Emerging DeFi Protocols**
  - Decentralized Exchanges (“DEXes”)
  - Borrowing / Lending Protocols
  - Derivatives / Synthetic Asset Protocols
  - Insurance
  - Prediction Markets
- **Aggregation Tools**
  - DEX Aggregators
  - Yield / Asset Management Protocols


Aggregation Layer
DEX Aggregators
Asset Management
Yield Aggregators
Assets
Governance tokens
Stablecoins
Wrapped assets
Protocol
Borrowing / Lending
Decentralized Exchanges
Derivatives / Synthetic Assets
Prediction Markets
Insurance
Blockchain
Ethereum
Other blockchains
Integration Tools
Crypto/ Fiat Gateways
Oracle Services
KYC / Identity
Token Factories

Potential Benefits

Creators or supporters of DeFi services often cite certain benefits to smart contract-based financial protocols:

- Lower costs,
- Greater accessibility / permissionless access,
- Greater financial inclusion,
- Composability and interoperability,
- Ability to have community-run financial infrastructure, and
- Higher degrees of security (and potentially privacy).

Potential Risks

These protocols, however, present a number of risks and limitations:

- High barriers to entry
  - Users need to be tech savvy to use these services safely.
  - The software is more complex than otherwise already complex blockchain applications.
- Use of leverage
- Runs on liquidity
- Entropy and complexity created by composability, and
- Regulatory questions

Growing Pains

DeFi is growing at an exponential rate, but there are still technical and practical barriers that have yet to be solved:

- Limited ability of blockchains to process transactions (which are potentially addressed with innovations like Ethereum 2.0),
- Comparatively low levels of liquidity, and
- Security and smart contract vulnerabilities, leading to hacks and other thefts.

DECENTRALIZED EXCHANGES

Overview

DEXes rely on automated market maker (“AMM”) smart contracts, which enable users to trade digital assets without using an order book.

Decentralized exchanges have daily trading volumes that are beginning to rival custodial exchanges (like Coinbase).

Technical Aspects of Decentralized Exchanges

The most popular DEXes often have two different types of smart contracts:

Exchange Contract

Holds a pool of one or more tokens that users can exchange.

Factory Contract

Creates new a exchange contract and registers various token addresses to the exchange contract's address

Importance of These Smart Contracts

Why do these two contracts matter?

- The use of a liquidity pool lessens the need for an order book.
- There is no central administrator of the pool; it's maintained by the smart contract.
- The open and permissionless aspect of the factory and exchange contracts enables anyone to list a token for exchange.
- These smart contracts are "**alegal**"; they do not necessarily incorporate regulatory compliance.

Pricing on Decentralized Exchanges

Pricing on DEXes is accomplished algorithmically:

- When exchanging one token for another token using a DEX, users don't need to be matched with a counterparty via an orderbook. A purchaser receives the requested token nearly instantaneously from an underlying **liquidity pool**. In other words, it's pool-to-peer and not peer-to-peer. The exchange smart contract acts in a manner akin to a counterparty.

- The amount of a token that is returned from an exchanged is based on the AMM formula, which often factors-in the number of tokens in the pool at any given time.

Challenges with Pricing

At least today, the larger an order relative to the size of a liquidity pool, the worse rate a party will receive under applicable algorithmic formulas.

Thus, larger liquidity pools of a given token pair (or set) allow for bigger trades, with less impact on the price.

Maintaining Stable Pricing and Liquidity

Pricing stability is achieved through third party arbitrageurs that profit on any price disparities surfacing for a given liquidity pool.

To incentivize larger pools of liquidity, a DEX's underlying smart contracts award fees to those that provide liquidity. The smart contracts also award liquidity providers with governance tokens, giving holders the right to weigh in on decisions related to the protocol's operation.

Interacting with Decentralized Exchanges

Currently DEX's have functional user interfaces that serve as a portal to the underlying smart contract.

These dApps tend to read information from the underlying smart contracts or token lists maintained and/or created by third parties.

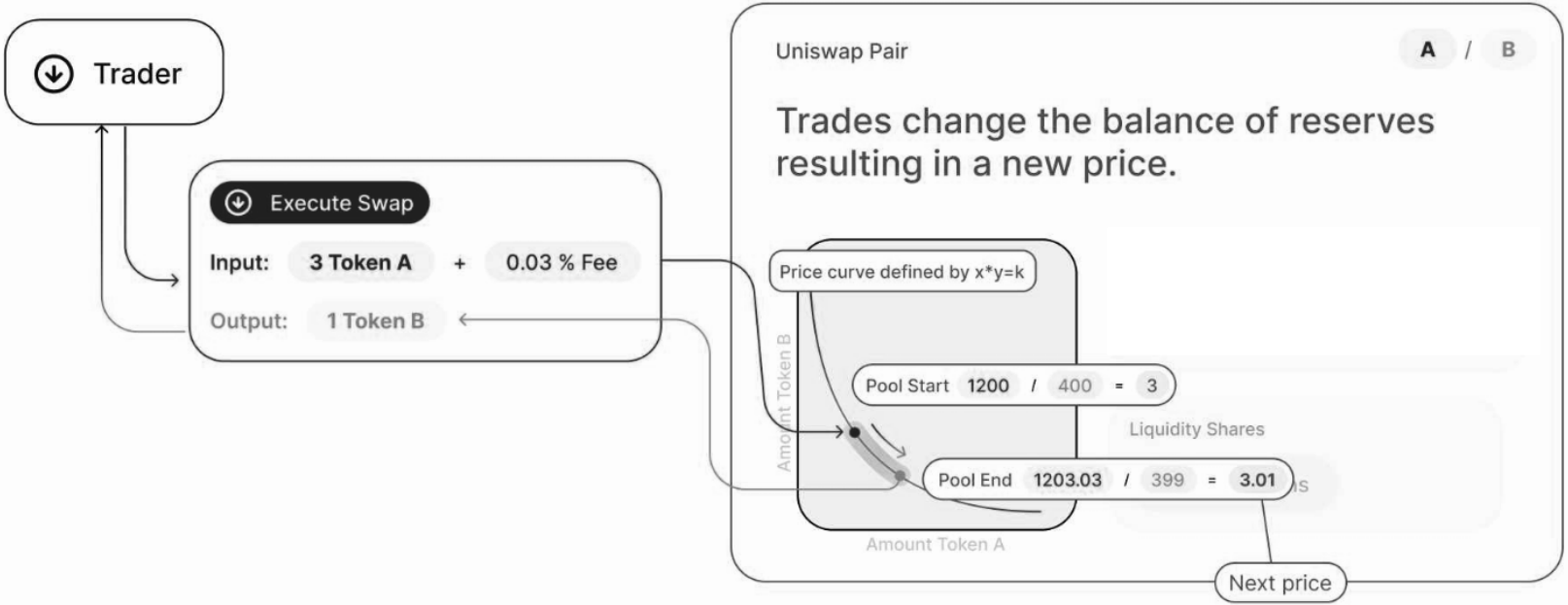
Some dApps are hosted by the original smart contract developers; others are hosted on decentralized file storage solutions and maintained by others.

Low Barriers to Entry

The underlying smart contracts are generally licensed under open source licenses, leading to competing “forks” or implementations of similar services.

Liquidity providers appear to demonstrate low loyalty to a particular decentralized exchange, suggesting that DEXes may become commoditized over time.

Example Uniswap



Example Uniswap (Cont'd)

The formula works as follows:

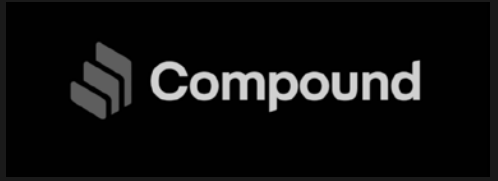
- The liquidity pool starts at 1,200 units of Token A and 400 units of Token B.
- Under Uniswap's AMM formula, this would be represented as: 1,200 Token A (x) * 400 Token B (y) = 480,000 (k).
- If buyer wants to swap 3 units of Token A for 1 unit Token B and is willing to pay Uniswap's current 0.3% fee, a new price can be calculated by keeping the variable k constant.
  - In other words, 480,000 (k) / 1,203.03 Token A (x) = 399 Token B (y).
  - The relative price of Token A to B before the trade was 3 (1,200 / 400).
  - After the trade, it is 3.01 (1,203.03 / 399).

LENDING PROTOCOLS

Decentralized Lending Protocols

Another category of DeFI protocols provides lending-related functionality. Many of these protocols enable users to deposit digital assets into a vault (e.g., ether) and borrow another token (e.g., DAI).

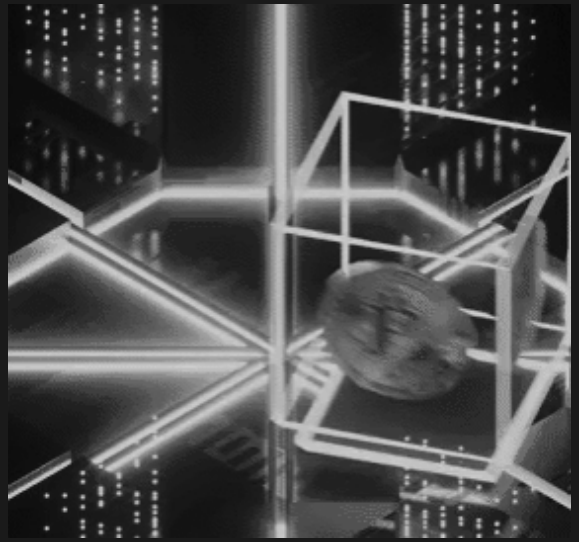
Some of these protocols create (or aim to create) a stable digital token through borrowing / lending functions and some generate a rate of return.



Mechanics of Decentralized Lending Protocols

To use a DeFi lending protocol, borrowers deposit one digital asset into a smart contract and receive receive back another token, usually valued at an amount below what has been provided as initial capital.

The loan thus is denominated in another asset (e.g., cDAI, DAI) at an amount typically between 50-75% of the deposited collateral.



Decentralized Lending Protocols

To ensure that a DeFi lending protocol has a sufficient amount of collateral, deposited collateral is auctioned or otherwise sold if the value of a given borrower's collateral drops below a liquidation ratio.

Lending protocols often rely on outside data feeds ("oracles") to determine the value of collateral deposited by users into the smart contract-based system and further set the liquidation ratio through community-run governance votes.

Flash Loans

Some decentralized lending protocols also enable **flash loans**, or a loan that is only valid within one blockchain transaction.

On platforms like Ethereum, a blockchain transaction can be reverted during its execution if certain conditions are not met.

Flash loans take advantage of this functionality and fail automatically, if a condition of a repayment is not satisfied before the end of a relevant blockchain transaction.

Traders use flash loans to generate a profit in a variety of trading scenarios, including arbitrage opportunities.

DECENTRALIZED DERIVATIVES AND SYNTHETIC ASSETS

Derivative / Synthetic Asset Protocols

DeFI protocols are not limited to exchanges and lending. Some also enable the creation of “synthetic assets” that derive their value from an underlying digital or real world asset.

Many of these protocols rely on overcollateralization and/or **oracles** to maintain price stability.

In some protocols, synthetic assets can be generated by any users of the platform.

Example- Synthetix

For example, Synthetix is a protocol that has a native token (SNX) that enables holders to create synthetic assets (or "**synths**"), which can mimic any asset, including other digital assets and fiat currencies.

To generate synths, a user must acquire SNX and deposit the token into the Synthetix smart contracts. In return, the Synthetix protocol creates a new synth token of the user's choice.

Under the rules of the protocol, the value of any SNX locked needs to remain at or above 750% of the value of the synth created. For example, if a user wanted to mint a synthetic U.S. dollar, the user can deposit $1,000 worth of SNX and receive back $133 worth of sUSD. Pricing data for various assets is provided by a third-party oracle solution.

Aggregation Layer

Types of Aggregators

DeFi protocols are becoming easier to interact with and new types of services are being built on top of these protocols to perform different functions. These includes:

- DEX aggregators,
- Yield aggregators, and
- Asset managers.

DEX Aggregators

DEX aggregators enable traders to access liquidity pools found on multiple decentralized exchanges.

Key Characteristics of DEX Aggregators

Better Pricing - Instead of aggregating news content or social media accounts, as with other types of online aggregators, a DEX aggregator combines token pricing information from multiple DEXes, aiming to offer people the best price for a trade.

Non-Custodial - DEX aggregators often do not custody the underlying asset held by a user. They connect different DEXes together.

Point of Centralization: If DEXes become commoditized, DEX aggregators could serve as the "search" function for DeFi, although the aggregators themselves may be decentralized.

Yield Aggregators

Users of DeFi protocols often look to maximize their total digital asset returns through **yield farming** and are turning to yield aggregators to streamline the provision of liquidity and the earning of tokens or other fees.

Example- Yearn Finance

For example, with Yearn Finance:

- Participants deposit digital assets into the protocol's smart contracts and receive back a YFI governance token.
- The token provides holders with the ability to vote and invest in digital assets through community generated trading strategies.
- The smart contract returns proceeds from these strategies directly back to holders of the YFI governance token (minus a fee).
- There are "multi-sig" holders that ensure the security of any collected assets before they are distributed to YFI holders.

Decentralized Asset Managers

With the growth of DeFI protocols, new tools have developed to give people the way to either track, manage, or hedge exposure to various different tokens. Some of these protocols bundle together different assets to manage risk or simplify interacting with underlying smart contracts.

MELON

Key Characteristics of Decentralized Asset Managers

Non-custodial – Control of the underlying assets is never transferred; it can interact with a user's wallet.

Composable – These tools connect to a wide number of DeFi projects, ultimately creating an end-to-end user experience.

Automated – Some services automatically rebalance and liquidate assets without additional user interaction.

Globally Accessible – These tools are accessible to anyone connected to the Internet with a wallet.

REGULATORY CONSIDERATIONS

Regulatory Risks for DeFi Protocols

DeFI protocols aim to thin the need for centralized custodians and other central actors, creating regulatory challenges. Many of today's regulations look to these actors to apply applicable rules and regulations.

However, to the extent DeFi applications implicate requirements or prohibitions under the Commodity Exchange Act or related regulations, these laws will still apply.

The question becomes who should be liable. These are similar issues to what the Securities Exchange Commission faced when analyzing The DAO in its 21(a) Report from 2017.

DeFi Protocols May Implicate Financial Laws

Commodity Exchange Act

- Unregistered FCMs or DCM/SEFs
- Anti-fraud provisions
- Anti-manipulation provisions
- Commodity pool / commodity trading advisor requirements
- Unregistered DCOs
- Failure to supervise issues

AML/KYC/Other

- Bank Secrecy Act
- State money transmission laws
- BitLicense

Securities Act, Securities Exchange Act, and Investment Advisor Act

- Classification of governance tokens
- Investment Advisor Act issues with asset managers

Direct Liability Against Developers

Nevertheless, as decentralized finance grows, it may become increasingly difficult to impute liability on the creators of decentralized protocols.

In the US, software development is often a protected activity under the First Amendment, unless there is no lawful purpose to the software.

Note, this is not a complete bar and, in fact, courts have, in the past, imputed liability against software developers. *See, e.g.* United States v. Mendelsohn, 896 F.2d 1183 (9th Cir. 1990).

Direct Liability Against Developers (Cont'd)

Bringing enforcement actions against developers creates challenges. Once a smart contract-based protocol is deployed, it is difficult to remove or shut down the smart contracts due to the tamper-resistant nature of a blockchain. That means users can still interact with the software, even if developers are held liable.

These challenges were acknowledged by Commissioner Quintenz, in remarks made on October 16, 2018, where he noted that "[e]nforcing CFTC regulations against [smart contract developers] does not immediately stop the activity from occurring, because individual users could continue to use the software . . . ."

Direct Liability Against Developers (Cont'd)

Due to these challenges, Commissioner Quintenz noted that liability may only attach if smart contract "developers could reasonably foresee, at the time they created the code, that it would likely be used by U.S. persons in a manner violative of CFTC regulations."

Direct Liability Against Developers (Cont'd)

Activities adjacent to developing a DeFI protocol also may create liability, including:

- Maintaining the sole interface to the underlying smart contract,
- Maintaining centralized control over some core mechanic of how the service operates, and
- Potentially deploying the smart contract itself.

Direct Liability Against Developers (Cont'd)

The Securities Exchange Commission referenced some of these activities *In the Matter of Zachary Coburn*, Release No. 84553 (November 8, 2018), when holding Coburn liable for building and operating EtherDelta, a smart contract based exchange.

Amongst other things, Coburn:

- Deployed the underlying smart contracts,
- Maintained the website that users accessed, and
- Helped select the tokens available for trading through the service.

Secondary Liability for DeFi Protocols

Given the challenges of imposing direct liability on developers of more decentralized DeFi protocols, there may be ways to find secondary (vicarious) liability for actors participating or interacting with these protocols under different legal theories. This includes:

- Aiding and abetting liability, and
- Controlling person liability.

Aiding and Abetting Liability

Commodity Exchange Act 13c(a):

"Any person who commits, or who willfully aids, abets, counsels, commands, induces, or procures the commission of, a violation of any of the provisions of this chapter, or any of the rules, regulations, or orders issued pursuant to this chapter, or who acts in combination or concert with any other person in any such violation, or who willfully causes an act to be done or omitted which if directly performed or omitted by him or another would be a violation of the provisions of this chapter or any of such rules, regulations, or orders may be held responsible for such violation as a principal."

Controlling Persons

Commodity Exchange Act 13c(b):

“Any person who, directly or indirectly, controls any person who has violated any provision of this chapter or any of the rules, regulations, or orders issued pursuant to this chapter may be held liable for such violation in any action brought by the Commission to the same extent as such controlled person. In such action, the Commission has the burden of proving that the controlling person did not act in good faith or knowingly induced, directly or indirectly, the act or acts constituting the violation.”

Aiding And Abetting Liability (Cont'd)

For example, in *Commodity Futures Trading Comm'n v. Edge Fin. Techs.*, No. 1:18-CV-00619 (N.D. Ill. Aug. 13, 2020), the CFTC entered into a consent order of permanent injunction against Edge Financial Technologies, LLC ("Edge Financial") for providing customized software for aiding and abetting spoofing and use of a manipulative and deceptive schemes under Section 13(a) of the Commodity Exchange Act.

Actors Potentially Subject to Secondary Liability

The universe of actors who arguably aid, abet, or control unlawful activity, potentially include:

- **Aggregators**, which "aid and abet" unlawful transactions.
- **Liquidity providers or end users** that directly participate, or disproportionately facilitate, unlawful behavior.
- **Holders of Governance Tokens** that have a "controlling" interest over the direction of the underlying software.
- **Multisig Holders**, for applicable projects, that have the ability to control unlawful activity.
- **Validators/Miners**, that execute the smart contracts used by end users.

Trade Offs with Imposing Secondary Liability

- **Incomplete Solution:** Imposing secondary liability may only serve as a deterrent and will not necessarily stop the use of a DeFI protocol, due to the hard to modify nature of smart contracts.

- **Encourages More Unregulatable Solutions**. Secondary liability will encourage developers to use more advanced forms of cryptography to obscure transactional records.

- **Enforcement Costs**. Secondary liability cases likely will be more complex to litigate, and depending on the legal theory, could implicate more defendants.

Trade Offs with Imposing Secondary Liability (Cont'd)

- **Innovation** . Miners/validator are not in a position to know and assess the legality of each particular transaction executed on a blockchain. Due to the way public blockchains currently operate, these parties cannot monitor the activity of other blockchain users.

  If miners/validators are held responsible, it would push control of these networks to other jurisdictions and thus likely quell innovation in the US.

SAFE HARBOR

Encouraging Compliance

An alternative approach could be to provide software developers--and potentially users of DeFI protocols--a regulatory incentive to build and support compliance through a “safe harbor.”

Conceptually, a safe harbor could excuse direct liability for software developers and other DeFi participants, if the protocol:

- Has a lawful purpose and entails no fraud,
- Interacts or excludes addresses and/or jurisdictions encouraging OFAC compliance, and
- Limits or bars margin trading.

Encouraging Compliance (Cont'd)

The safe harbor could also contemplate requiring that protocols are able to implement any future CFTC-authorized software systems to enforce commodities related laws (i.e., use “code as law”).

Lessons from “Copyright Wars”

The above approach is grounded in analogous legal battles involving questions concerning copyright enforcement.

During the first wave of the Internet, copyright law evolved via the common law to grapple with peer-to-peer networks.

This resulted in expanded theories of secondary copyright liability and the introduction of various safe harbors.

Expanded Secondary Copyright Infringement

Through various decisions, at both the Supreme Court and Circuit Courts, vicarious liability is now imputed if an online platform: (1) exercises "requisite control" over the direct copyright infringer; and (2) derives a direct financial benefit from the direct infringement.

"Requisite control" has been determined to be a "legal right to stop or limit the directly infringing conduct, as well as the practical ability to do so." It attaches even if a platform lacks knowledge of the direct infringement.

Expanded Secondary Copyright Infringement (Cont'd)

Contributory liability also has been imputed through theories of “inducement,” in situations where an online platform intentionally encourages copyright infringement.

Contributory liability has further attached when operators have actual knowledge of copyright infringement and fail to “take simple measures to prevent further damage.”

DMCA Safe Harbor

At the same time, the Digital Millennium Copyright Act ("DMCA") has resulted in the development of a "notice and takedown" regime that, *inter alia*, shields online services from liability if a platform expeditiously removes works identified by copyright holders.

The notice and takedown regime has enabled large platforms like YouTube, Spotify, Wikipedia, and other services to grow, while attempting to balance copyright owners' concerns.

A Similar Approach Could be Adopted Here

Decentralized finance could be regulated using theories of secondary liability under the Commodity Exchange Act.

At the same time, a safe harbor could ensure responsible development to protect consumers' interests without limiting innovation.

Conclusion and Considerations

Given the emerging nature of DeFi, the subcommittee is considering recommending to the TAC to recommend to the CFTC. The subcommittee's current thoughts include:

- Adopt a wait and see approach to see where risks manifest with these protocols.
- Carefully consider whether to impose direct liability on smart contract developers or miners/validators to prevent spillover effects.
- Research and explore theories of secondary liability.
- Continue to engage with blockchain developers to stay up to date on new services and ongoing innovation.
- Consider having the staff memorialize a safe harbor in a no action letter.