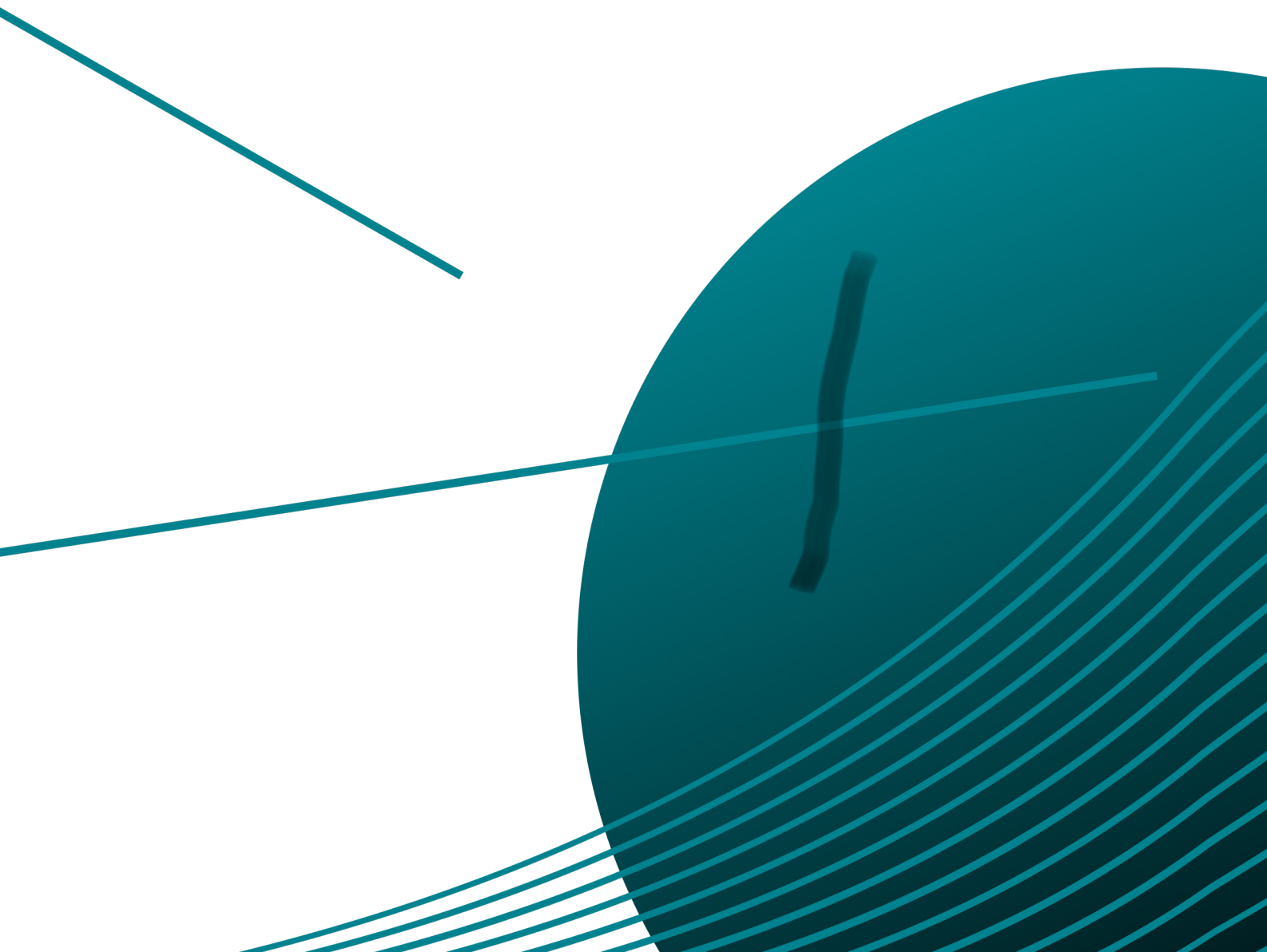
ELLIPTIC

DeFi

Risk, Regulation, and the Rise of DeCrime



Contents

Executive Summary

Decentralized Finance (DeFi) looks set to revolutionise financial services, by replacing centralised intermediaries with software running on blockchains.

Because it is built on an open infrastructure, DeFi can be used by anyone with an internet connection, promising far broader access to the financial services that are currently enjoyed by a privileged few. It also means that anyone is free to innovate and build their own financial services for a global market - greatly increasing choice and competition.

Growth in the use of DeFI over the past two years has been staggering:

- The total capital locked in DeFi services, a measure of liquidity, has grown by more than 1,700% over the past year to **$247 billion**
- Monthly trading volumes on decentralised exchanges (DEXs) have surged by more than 1,500% over the past year, to more than **$300 billion each month**
- Outstanding loans issued through DeFi lending protocols have increased at an annual rate of over 800% to **$23 billion**.

The same openness and innovation that makes DeFi so powerful also brings with it new risks. The relative immaturity of the underlying technology has allowed hackers to steal users' funds, while the deep pools of liquidity have allowed criminals to launder proceeds of crime such as ransomware and fraud. This is part of a broader trend in the exploitation of decentralised technologies for illicit purposes, which we refer to as ***DeCrime***.

- DeFi users and investors has suffered more than **$12 billion** in losses due to theft and fraud
- These losses are accelerating, with losses totaling **$10.5 billion** in 2021 to date, up from **$1.5 billion** in 2020
- DeFi is also being used to launder proceeds of crime - with DEXs, decentralised mixers and cross-chain bridges being exploited
- However the unprecedented transparency of DeFi provides law enforcement with new opportunities to follow the money and apprehend criminals.

In traditional finance stringent regulation aims to protect consumers and prevent money laundering - however these regulations were not designed for decentralised financial services. We are currently seeing regulators grapple with the consequences of DeFi as they attempt to apply traditional regulatory principles to the unique risks and challenges presented by decentralization.

As DeFi grows to become an increasingly significant part of our financial system the risks inherent in it will also impact traditional financial institutions. These risks can not be mitigated through industry abstention alone. The interconnected nature of the global financial system, perpetuated through payment networks and correspondent banking relationships, ensures that the fiat financial sector is already systemically connected to decentralized finance. Only through the implementation of DeFi-tailored KYC, AML and transaction monitoring policies and procedures can traditional financial institutions adequately assess and mitigate the new risks and exploit the exciting opportunities that decentralized finance presents.

01

Introduction to DeFi

What is DeFi?

If you need to borrow money for a house, obtain insurance for your car or send money to your family overseas, you generally have to do so through one of a relatively small number of intermediaries — be it a bank, money remittance company or insurance broker. These intermediaries provide efficiency and convenience, but they also stifle innovation and restrict access to those who need financial services the most.

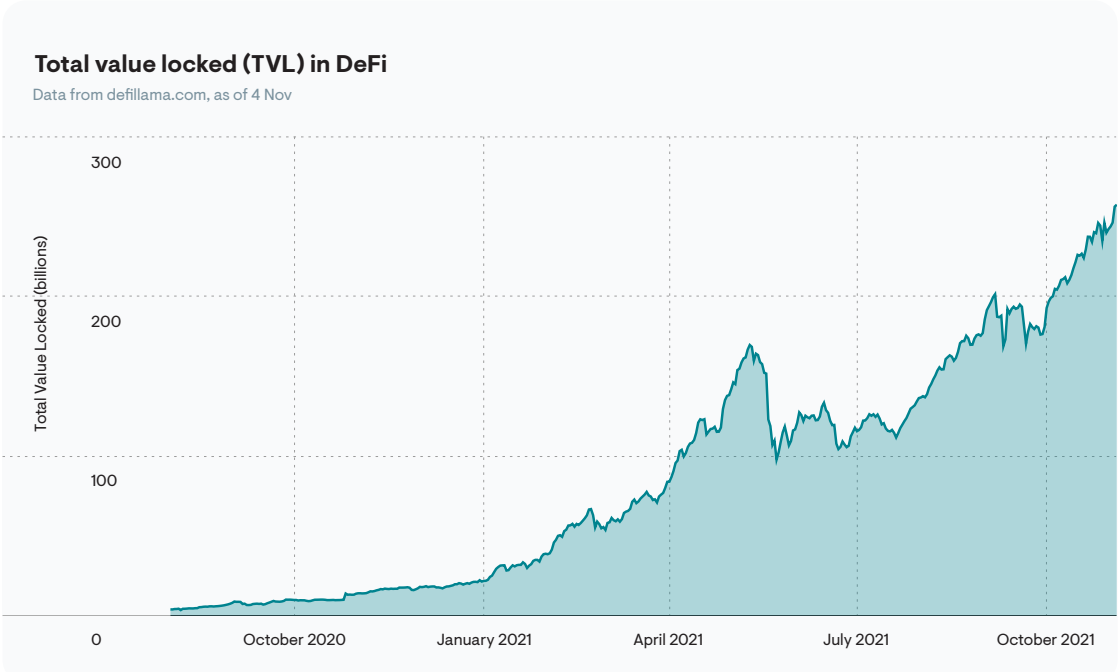
Bitcoin was originally conceived in 2008 as a solution to this problem. It provides a means of payment that is accessible to anyone, without the need to go through an intermediary such as a bank or remittance company. However Bitcoin has struggled as a payments system due to the volatility of its unit of account, and because of its limited functionality — payments are just one small component of a financial system. Services such as Bitcoin exchange and lending remained intermediated by centralized service providers, just as in the traditional financial system.

Enter Ethereum in 2015. Ethereum combines the open, permissionless financial infrastructure of Bitcoin, with much richer, flexible functionality that is enabled through the concept of smart contracts. These allow complex financial services to operate as software, directly integrated into the settlement infrastructure.

The DeFi ecosystem has flourished in recent years with total value locked increasing from $500million in 2019 to $247 billion today

Decentralized Finance (DeFI) refers to the use of platforms such as Ethereum to offer an alternative financial system that is open for anyone to use, and which allows centralized intermediaries to be replaced by decentralized applications (DApps).

Over the past two years the DeFi ecosystem has flourished, with DApps offering decentralized lending, exchange, asset management and derivatives gaining significant traction. The "total value locked" (TVL), a measure of the liquidity of DeFi services, has increased from $500 million in November 2019 to just over $247 billion today.



Benefits of DeFi

Security

Users retain full control of assets, rather than entrusting them with a third party service provider. User assets can only be moved according to rules encoded within smart contracts, visible to the user. This reduces the risk of fraud or other loss of assets by centralized custodians.

Innovation and choice

Enabled by the open, programmable settlement infrastructure. Anyone can build a DApp, and instantly offer financial services to anyone with an internet connection, including many "unbanked" with no current access to such offerings. The use of open source code also allows the "forking" of projects so developers can build on existing work, rather than starting from a blank sheet.

Composability

Otherwise known as the "money lego" concept. DApps are open for anyone to use, and are interoperable on the same settlement layer. This means that existing DApps can be combined in new ways to create new, increasingly sophisticated financial services. For example asset management DApps combine multiple stablecoin, decentralized exchange and lending DApps to provide a new service.

DeFi Services

Decentralized financial services are offered through decentralized applications (DApps) operating on blockchains such as Ethereum. Each DApp is itself made up of one or more smart contracts.

Stablecoins

Stablecoins are blockchain-based tokens whose value are tied to some underlying asset — most commonly the US Dollar. The most widely used stablecoins, including Tether and USDC, do not qualify as DeFi services since the assets that back them are held by a centralized provider. However two other types of stablecoin do operate through DApps:

- ***Algorithmic stablecoins*** aim to maintain a "peg" between their value and the value of the underlying asset (eg USD), by controlling supply. They automatically issue more stablecoins when their price increases, and buy them off the market when the price falls. Leading examples include Ampleforth, Terra and Frax.

- ***Non-custodial, asset-backed stablecoins are*** similar to the likes of Tether and USDC, except the asset backing the coin is held in a smart contract rather than by an off-chain asset issuer. This means that the asset backing the stablecoin must itself be a cryptoasset, but this does not prevent these stablecoins from being pegged to fiat currencies such as the US Dollar. Leading examples include DAI and RenBTC.

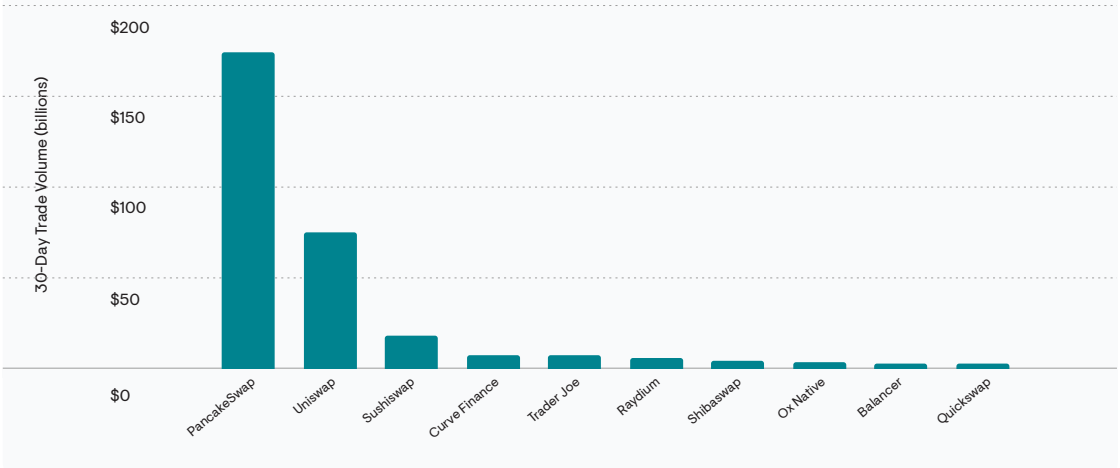
Exchanges

Exchanges allow one cryptoasset to be traded for another. Conventional, centralized exchanges such as Coinbase or Binance take custody of their users' assets and operate an order book to match buyers with sellers.

Decentralized exchanges (DEXs) offer a decentralized alternative, where asset custody and order-matching take place on a blockchain rather than on centralized servers. In practice DEXs can operate in various ways and with varying levels of decentralisation. The likes of dYdX offer

30-day trade volumes on the the ten leading decentralized exchanges (DEXs)

Data from Nomics, Dune Analytics, as of 4 Nov 2021.



centralized order-matching for speed, while the settlement of trades takes place on-chain in a decentralized way. Automated market makers (AMMs) such as Uniswap and Curve Finance are almost fully decentralized, with an order book replaced by an algorithm that prices assets based on orders and the volume of assets stored in "liquidity pools".

Over the past year DEX trading volumes have surged from $18 billion to more than $300 billion each month, becoming real competitors to their centralized counterparts.

DEX aggregators have also emerged — DApps that automatically route funds to the one or more DEX that offer the best exchange rate for a given trade. These include 1inch and Paraswap.

Over the past year DEX trading volumes have surged from $18 billion to more than $300 billion each month, becoming real competitors to their centralized counterparts

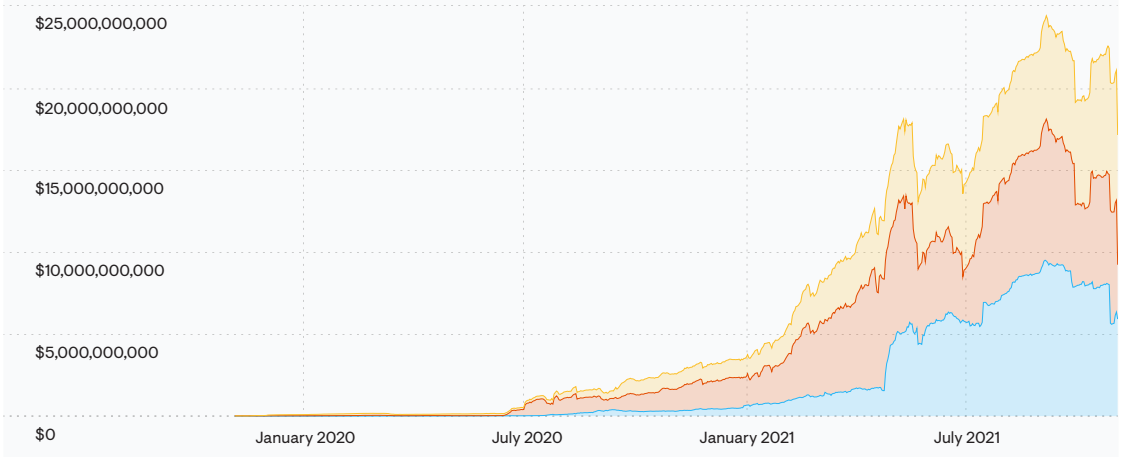
Credit

The credit markets underpin the global economy. Banks themselves earn more than half their revenues by acting as intermediaries in these markets — taking assets from those willing to lend and giving them to those wanting to borrow them.

DeFi lending and borrowing allows centralized intermediaries such as banks to be replaced with automated, decentralized, non-custodial DApps. Leading credit DApps include Aave, Compound and InstaDApp. Some credit DApps match specific lenders to buyers, whereas others operate through liquidity pools. Loans are generally collateralized with cryptoassets that are stored in smart contracts and which are only released on repayment of loans.

As of November 2021, outstanding loans provided by these DApps total $23 billion – up from $2.5 billion in November 2020.

Debt outstanding in the three largest lending DApps: MakerDAO, Compound and Aave, as of 4 Nov 2021.



Many lending DApps also offer flash loans, uncollateralized loans that are taken out and repaid (with interest), over the course of a single blockchain transaction. The risk is low for the lender because if they aren't repaid, the conditions of the flash loan smart contract are not met and the transaction is reversed — with the funds returned to the lender as if nothing ever happened. Flash loans have been used in numerous DApp exploits and the theft of hundreds of millions of dollars worth of cryptoassets, as described in the next chapter.

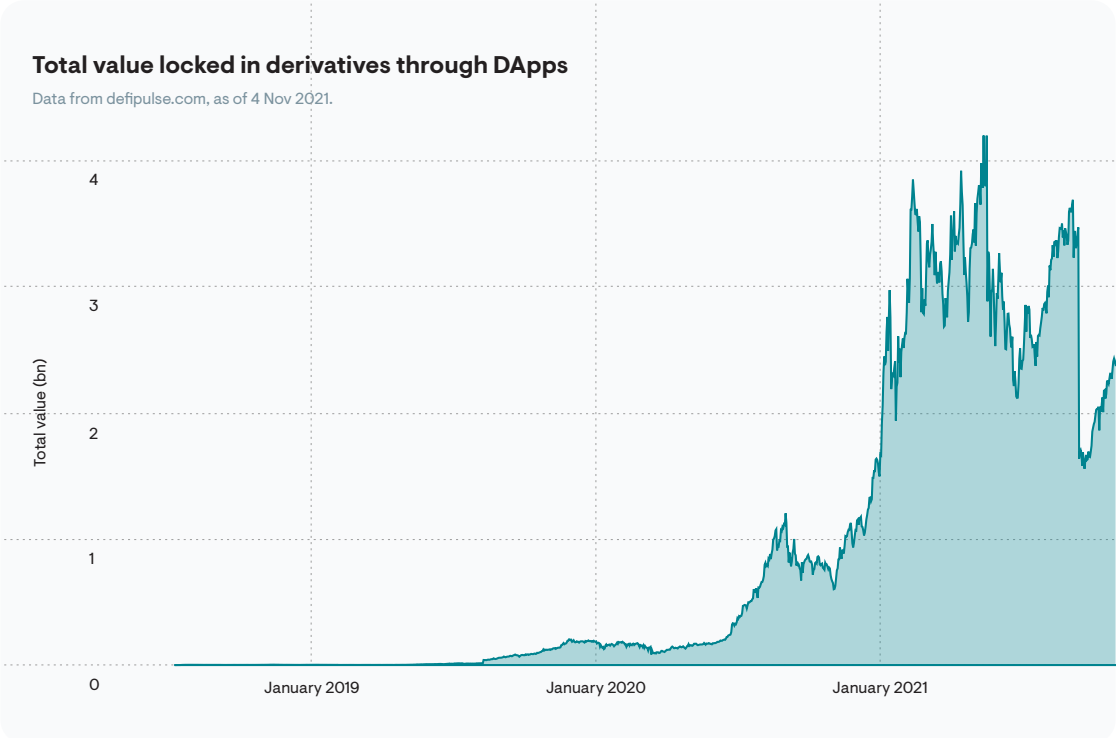
Derivatives

Derivatives are contracts that derive their value from the performance of an underlying asset, group of assets, or benchmark. Trillions of dollars worth of derivatives are used to hedge against price movements or increase exposure to price movements for speculation. Common financial derivatives include futures and options, which pay out based on the value of an asset at some time in the future or deliver the underlying asset.

DApps can be used to create decentralized derivatives that follow the price movements of stocks, commodities, swaps or other digital assets (even NFTs) according to their smart contract code. Where the asset or benchmark is off-chain (eg stock prices or interest rates), oracles are used to bring this information onto the blockchain to be used by smart contracts.

Importantly, this brings non-blockchain-based asset exposure to the crypto ecosystem, helping to create a more mature financial market within DeFi.

The leading derivatives DApp is Synthetix, which enables the minting of "Synths" — tokens that track the price of any asset with a reliable price feed. Synths exist for cryptoassets, currencies, commodities, stocks, or indices. Even inverse Synths exist that track the inverse of the underlying asset, giving traders an easy way to get short exposure or hedge existing holdings. Synths are backed by the Synthetix Network Token (SNX) or ETH, which is staked as collateral at a ratio of 750%.



Asset Management

In traditional asset management, investors rely on specialized institutions and financial advisors to manage their portfolio based on parameters such as their risk appetite and time horizon. Investment products such as mutual funds and ETFs might be used. Fees are paid to each intermediary.

In DeFi asset management the underlying investments can be cryptocurrencies, synthetic derivatives tokens, or the provision of liquidity to lending DApps or DApp. Manual portfolio management is replaced with a DApp that can automatically reallocate assets based on the current market conditions..

One of the most popular asset management DApps is Yearn Finance. Their “vault” product allows users to deposit cryptoassets to a pool which is dynamically allocated to other DApps in order to maximise yield. Users do not need to have an understanding of the underlying DApps or constantly monitor them for the best investment opportunities. The pooling of assets also means that fees as a proportion of investments can be kept low — an important factor when transaction fees when interacting with DApps can be very high.

DeFi Governance

DApps are typically designed to be self-sufficient and not reliant on a central authority. However in practice decisions often need to be made about changes in the operation of DApp and those changes need to be implemented.

Many DApps solve this through the use of admin keys, which allow certain individuals to update the underlying smart contracts. However this introduces security risks and also undermines a DApp's level of decentralization, which can have regulatory consequences.

A common solution is to allow holders of a DApp's governance tokens to vote on key decisions. These tokens are typically issued to users of the DApp, based on their level of activity. A smart contract-based decentralized autonomous organization (DAO) is established as part of the DApp, which automatically executes the governance decisions of the token holders — removing the need for "admins".

These tokens are tradeable on exchanges (including DEXs), with their value presumably linked to the ability to influence the operation of a specific DApp. Governance tokens can attract very high valuations — for example the total issuance of UNI, the governance token of the Uniswap DEX, has a current market capitalization of $16.6 billion.

DeFi Incentives

Another benefit of governance tokens is that they incentivize the adoption of a DApp, and the provision of capital that is essential to their operation. This includes providing liquidity to DEXs or collateral for lending DApps. The mechanism of rewarding liquidity providers with tokens specific to the DApp (usually governance tokens) is known as ***liquidity mining***.

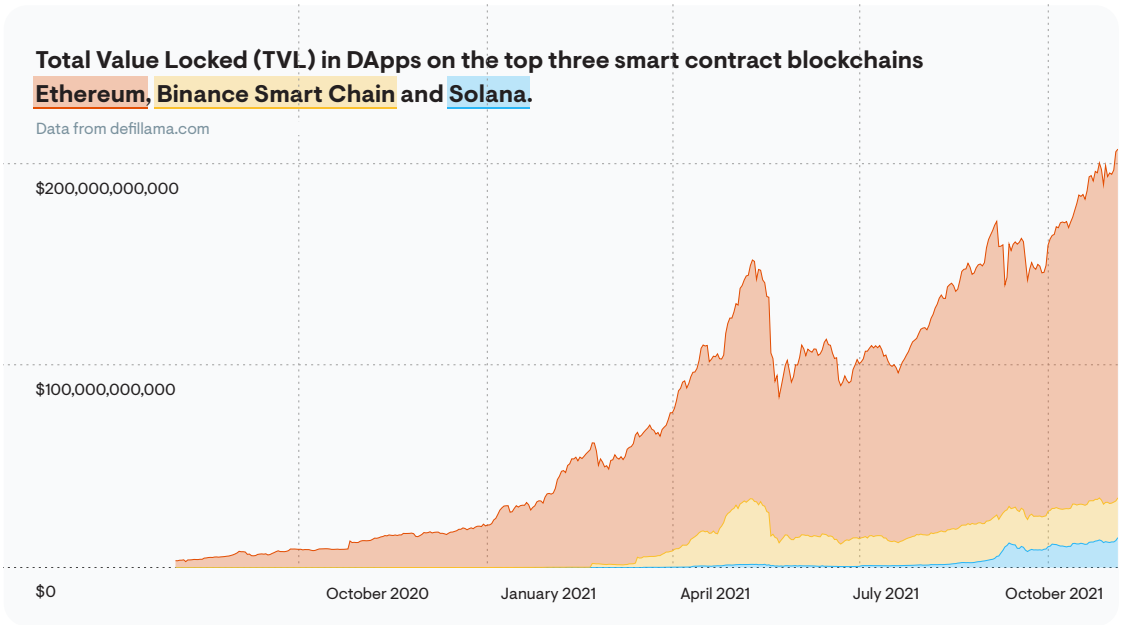
A related incentive mechanism is ***lock-up yields*** where a DApp pays interest or a share of trading fees to users that commit cryptoassets to polls where they serve as liquidity or collateral for the DApp.

Yield farming refers to the strategy of allocating cryptoassets so as to maximise returns from DApps through the various incentive mechanisms. Asset management DApps such as Yearn Finance execute yield farming in an automated way.

DeFi Platforms

DeFi refers to a general approach to the provision of financial services, rather than being specific to any blockchain. DApps first appeared on Ethereum, which remains the dominant platform, however a range of competing blockchains have emerged.

In general, these platforms must make a trade-off between security, scalability and decentralization. Achieving a high level of all three properties is believed to be extremely challenging or impossible to achieve — a concept originally described by Ethereum founder Vitalik Buterin as the Scalability Trilemma. [1]



Ethereum

Launched in 2015, Ethereum was the first blockchain to be launched with extensive smart contract functionality. For a number of years it was the only practical option for those launching DApps, and this has contributed to a continuing strong network effect, such that Ethereum is by some margin the leading platform for DeFi, with $173 billion locked in DApps. Ethereum is also considered to excel in security and decentralization, thanks to a very large and diverse community of miners that validate transactions.

However Ethereum has faced significant scaling challenges as DeFi adoption and transaction volume have increased, leading to very high transaction fees. The "ETH2" upgrade will seek to improve scalability over the coming years, as will layer-2 solutions built on top of Ethereum such as Arbitrum and Optimism.

[1] https://vitalik.ca/general/2021/04/07/sharding.html

Binance Smart Chain

Binance Smart Chain (BSC) was launched in September 2020 by Binance, one of the leading cryptocurrency exchanges. Its primary design goal is to increase transaction throughput and reduce transaction cost when compared to Ethereum. It achieves this primarily by changing the consensus mechanism that is used to verify whether transactions are valid, including reducing the number of validators (miners) to just 21.

The tradeoff is that this leads to much higher centralization, and concerns [2] have been raised about Binance's level of control over BSC.

BSC has seen strong growth, with $19.7 billion now locked in DApps — up from $50 million in November 2020.

Solana

Solana, first launched in March 2020, seeks to achieve scalability and low fees, while still achieving reasonable levels of decentralisation. To achieve this, it implements a novel consensus mechanism known as proof of history, enabling transaction throughputs of around 65,000 per second — far exceeding Ethereum's current limit of around 16 transactions per second. There are currently around 1,100 transaction validators on Solana.

However, concerns remain about the security and stability of Solana, with a total outage in September 2021 lasting for 17 hours.

Solana has also seen very strong growth, with $13.9 billion now locked in DApps — up from around $100 million in March 2021.

[2] *https://twitter.com/WilsonWithiam/status/1381420702918664194?s=20*

02

Criminal Exploitation of DeFi

Wherever there are concentrations of value, there will be crime — and DeFi is no exception. More than $247 billion is now stored in DeFi protocols, a tempting honeypot for hackers and a deep pool of liquidity that can be taken advantage of by money launderers.

Despite the large sums being entrusted to these protocols, the underlying technology is relatively immature and untested. While DApps might be "trustless" in that they are designed to eliminate any third-party control of users' funds, you must still trust that the creators of the protocol have not made a coding or design mistake that could lead to a loss of funds. Unfortunately, such mistakes are commonplace. Elliptic's research shows that more than $12 billion has been lost as a result of DeFi exploits and scams. In the first section, "Theft in Defi" we describe the main types of DeFi exploit, and explore some significant case studies.

As well as an appealing target for criminals, DeFi protocols are increasingly being used as a tool for money laundering. Funds derived from criminal activity outside of the DeFi ecosystem are being funnelled into DEXs and other DApps, to avoid seizure and hide the money trail. In the second section, "*DeFi Money Laundering*", we describe how DApps such as DEXs, cross-chain bridges and decentralized mixers are used to launder proceeds of crime.

Theft in DeFi

Billions of dollars worth of cryptoassets have been stolen from centralized services such as exchanges. Many are startups with relatively immature cybersecurity, and the irreversible nature of crypto transactions make it very challenging to recover these funds. This has made them tempting targets for attackers ranging from lone hackers to nation states.

One of the main motivations behind DeFi has been to eliminate third party control of users' assets. Instead of a service provider taking custody of your funds in order to provide financial services, they are instead held by a smart contract. The funds can only be moved according to the rules set out in the contract's code, which can itself be audited by the DApp's users.

Nevertheless billions of dollars in cryptoassets are still being stolen from DApps. Some DApps have bugs or design flaws, which can be exploited by third parties. Others are fraudulent from the outset — with backdoors introduced by their creators in order to steal users' funds. Both types of theft are explored in more detail in the following sections.

The monetary losses resulting from this theft fall into two categories:

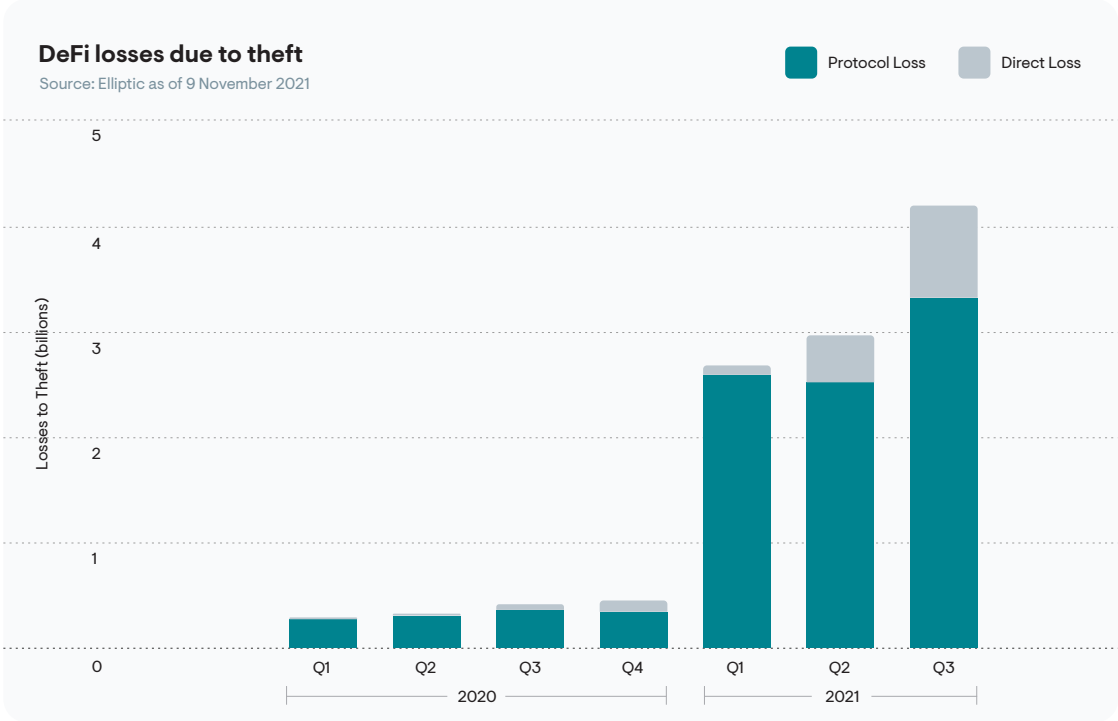
1. Direct losses – funds stolen from a DApp, resulting in losses for its users

2. Protocol losses – losses in the value of tokens linked to a DApp (eg governance tokens) as a result of the fraud. These losses are suffered by holders of these tokens, and typically reflect lower confidence in the DApp. [3]

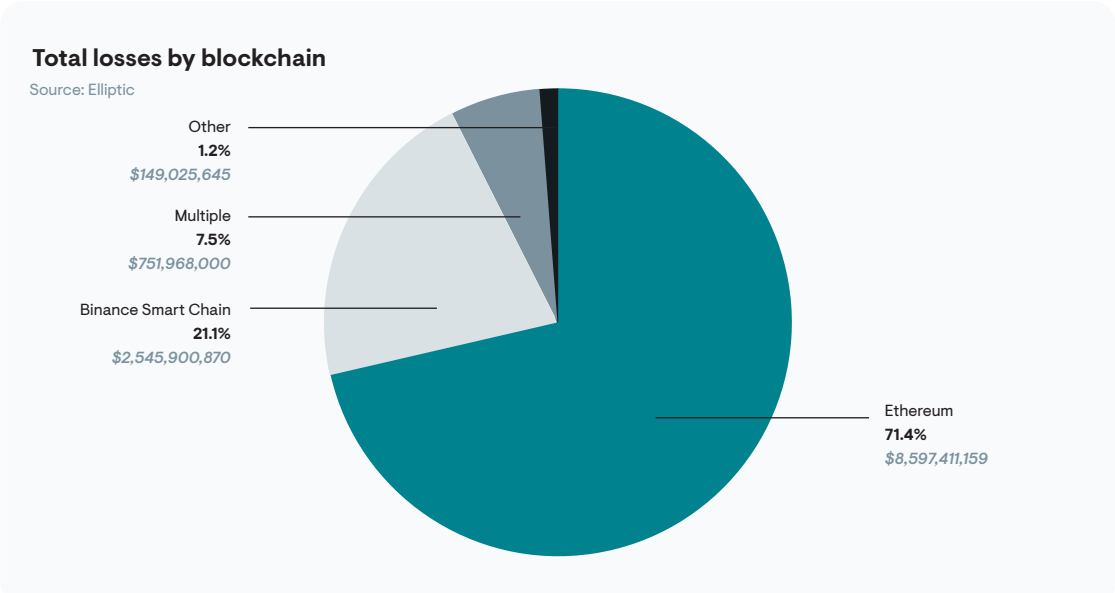
[3] *Protocol losses are estimated from any decreases in the fully-diluted market cap of tokens linked to the affected DApps that are clearly correlated to the fraud event.*

In total, just over $12 billion in losses have been suffered as a result of DeFi theft – $2 billion in direct losses and $10 billion in protocol losses. $721 million of these direct losses were subsequently recovered.

These losses are accelerating, with $10.5 billion of losses in 2021 (to 9 November), up from $1.5 billion in 2020.



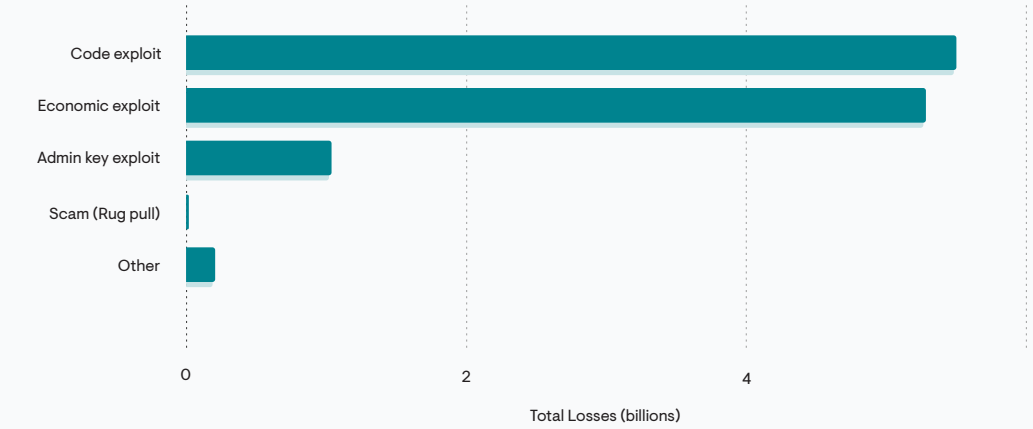
DApps on Ethereum have seen the bulk of these losses, at $8.6 billion, reflecting its current status as the blockchain of choice for DeFi. However, Binance Smart Chain (BSC) has also seen significant theft and fraud, totaling $2.5 billion.



The majority of DeFi losses stem from code exploits ($5.5 billion) and economic exploits ($5.3 billion). Admin key exploits account for $1.0 billion in losses, while scams ("rug pulls") account for $18 million. However it should be noted that scams/rug pulls are challenging to identify and distinguish from exploits, and may account for a larger share of losses.

Total losses by exploit type

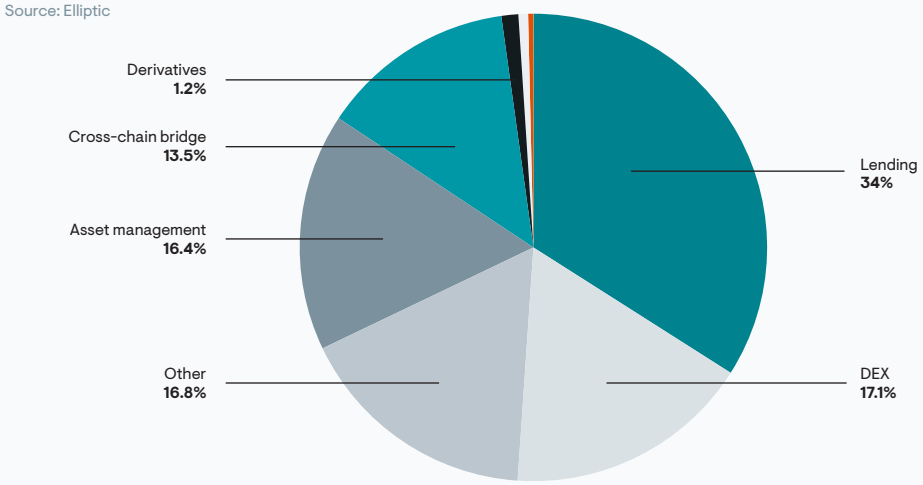
Source: Elliptic



DApps of various types have been exploited and have suffered losses, including lending (34%), decentralised exchange (DEXs) (17.1%), asset management (16.4%) and cross-chain bridges (13.5%).

Total losses by DApp type

Source: Elliptic



Bug Exploits

DeFi aims to reduce user losses when using financial services, by eliminating the need to entrust assets to third parties. Instead, user funds are stored in DApps that are governed by smart contract code rather than humans. However, custody risk is simply replaced by another type of risk — that errors in the DApp or the smart contract code can be exploited to steal users' funds. In fact the vast majority (90%) of losses suffered by DeFi users are caused by bugs within DApps that have been identified and exploited by hackers.

There are two main types of exploits — *code exploits* and *economic exploits* — as described in the next sections.

Code Exploits

The first type of bug is a coding error in one of the smart contracts that make up a DApp. As with other types of software, a single character out of place can have huge consequences — and in the case of DeFi, loss of users' funds.

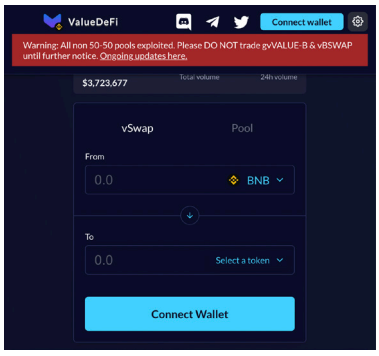
Losses of cryptoassets due to exploitation of these bugs are known as code exploits. Case Study 1 describes the theft of $11 million of user funds from vSwap, a decentralized exchange – made possible due to a coding error in one of its smart contracts. The risk of this type of bug can be minimized by conducting audits of the code, but even this cannot eliminate the risk entirely.

A common type of code exploit is the use of "evil contracts", in which an attacker 'tricks' a contract into thinking a hostile contract should have access or permissions.

Much of the code used in DeFi is open source, and many DApps use code that has been forked from that used by a single DApp. This means that a bug in the code of the original DApp can cascade and lead to losses from a number of different DeFi services.

CASE STUDY 1

vSwap — a missing line of code allows an $11 million theft



vSwap is a decentralized exchange (DEX) operating on the Ethereum and Binance Smart Chain blockchains. In May 2021 a VSwap account, holding user funds in the form of the protocol's own vBSWAP tokens, was emptied — resulting in a $11 million loss.

A post-mortem [4] of the incident identified that the omission of a single line of code was to blame. The affected contract included an initialize() function that should have been activated after deployment. A single line of code:

```
initialized = true;
```

was missing from the function, allowing anyone to initialize it and set themselves as the owner of the account, taking control of it and allowing them to move the funds contained within it.

[4] *https://medium.com/valuedefi/vstake-pool-incident-post-mortem-4550407c9714*

Economic Exploits

The second type of bug, which together with code exploits represent the bulk of DeFi losses, involves errors in the design of a DeFi service rather than the actual code. By exploiting "loopholes" in the way that DApps operate, users can secure profits when using them — these are typically known as economic exploits. DApps are often designed to be "composable" and used in combination with other Dapps to create new services (also known as the "money lego" concept). Such combinations can create new loopholes that didn't exist for the individual DApps.

Economic exploits are often complex and take a variety of different forms. One of the most common types of economic exploit involves manipulating asset prices in order to take advantage of arbitrage opportunities on DeFi services that would not otherwise have existed. The arbitrage is often conducted using assets obtained through large "flash loans" — unsecured crypto loans that can be borrowed and repaid very quickly — over the course of a single transaction.

Case Study 2 describes just such an exploit that took place in October 2020, with Harvest Finance users losing $33.8 million to an attacker making use of a flash loan.

CASE STUDY 2

A one minute flash loan used to steal $630k from bZx

9504634	608 days 10 hrs ago	0x2e05b36f4e1afd92366...	call	bZx Exploiter 2: Contract	→	bZx Exploiter 2	2,378.153715421627764 Ether
9504627	608 days 10 hrs ago	0x762881b07feb63c436...	call	bZx Exploiter 2: Contract	→	Wrapped Ether	7,500 Ether
		0x762881b07feb63c436...	call	0x3b5bdccdfa2a0a19119...	→	bZx Exploiter 2: Contract	6,796.012817135270528 Ether
		0x762881b07feb63c436...	call	Synthetix: Old Depot	→	bZx Exploiter 2: Contract	2,482.140898286357235 Ether
		0x762881b07feb63c436...	call	bZx Exploiter 2: Contract	→	Synthetix: Old Depot	6,000 Ether
		0x762881b07feb63c436...	call	bZx Exploiter 2: Contract	→	Kyber: Proxy	20 Ether
		0x762881b07feb63c436...	call	bZx Exploiter 2: Contract	→	Kyber: Proxy	20 Ether
		0x762881b07feb63c436...	call	bZx Exploiter 2: Contract	→	Kyber: Proxy	20 Ether
		0x762881b07feb63c436...	call	bZx Exploiter 2: Contract	→	Kyber: Proxy	20 Ether
		0x762881b07feb63c436...	call	bZx Exploiter 2: Contract	→	Kyber: Proxy	20 Ether

bZx is a decentralized margin trading and lending protocol, which allows cryptoassets to be borrowed, using other cryptoassets as collateral. In February 2020 an attacker was able to steal $630k from an under-collateralized loan by manipulating the price feeds used by the protocol.

1. The attacker takes out a flash loan of 7,500 ETH ($2 million).
2. Of this, 3,518 ETH ($940k) is used to purchase 940k sUSD (a stablecoin).
3. The 940k sUSD is deposited at bZx as collateral.
4. 900 ETH from the flash loan is used to bid the price of sUSD up to $2, on relatively illiquid markets such as Kyber.
5. The 940k sUSD (now "worth" around $1.9 million) on bZx is used to borrow 6,796 ETH
6. The 7,500 ETH flash loan is repaid.
7. The attacker is left with 2,378 ETH ($630k) as profit. The 6,796 ETH bZx loan is never repaid (and when the sUSD returns to $1, the collateral does not cover the loss).

Like other economic exploits, the individual smart contracts behaved exactly as intended. However a flaw in the design of the protocol, and the assumptions made about the accuracy of external price feeds, led to a loophole that could be exploited.

Admin Key Exploits

Some DApps have "admin keys" that allow trusted individuals to make updates to the underlying smart contracts or manage cryptoasset reserves. When such a key is used to steal funds from DApps, it is known as an admin key exploit.

Of course one of the main motivations behind DeFi is to prevent such an exploit from being possible, by not entrusting assets to any third party. Indeed some would argue that any DApp relying on admin keys would not constitute "DeFi" at all.

The common alternative is to allow holders of a DApp's governance tokens to vote on key decisions. These tokens are typically issued to users of the DApp, based on their level of activity. A smart contract-based decentralized autonomous organization (DAO) is established as part of the DApp, which automatically executes the governance decisions of the token holders — removing the need for admins.

Exit Scams (Rug Pulls)

Exit scams have been part of the cryptocurrency landscape for many years. The (often anonymous) operators of services ranging from crypto exchanges to darknet marketplaces have disappeared, taking their users' funds with them. DeFi promised to make this impossible, by ensuring that users' funds are never under the control of a service administrator who could steal them.

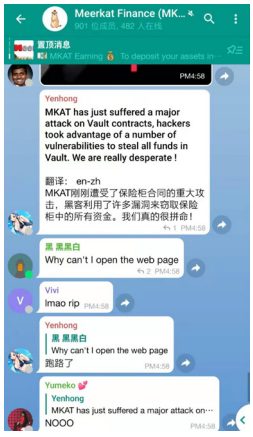
Nevertheless DeFi exit scams (otherwise known as rug-pulls) still take place. This is because bugs are being intentionally introduced into DeFi protocols, by their creators. These "backdoors" can be very difficult to spot due to the complexity of many DApps. These backdoors generally allow the DApp creator to steal user funds and perpetrate exit scams.

Exit scams differ from the code exploits described in the previous section, in that the bugs are intentional and were included in the DeFi service in order to steal users' funds. The pseudonymous nature of crypto means that it is sometimes difficult to distinguish a rug-pull from a bug exploit by a third party hacker.

CASE STUDY 3

Compare the Meerkat

Meerkat Finance was launched in March 2021 as a decentralized asset management protocol operating on Binance Smart Chain (BSC), modeled on the highly-successful yearn.finance. Disaster struck just one day later with $31 million drained from its accounts. The Meerkat team claimed that they had been the victim of an external hacker but observers pointed out that, shortly before the attack, the smart contracts had been updated to allow the vaults to be drained. The disappearance of Meerkat's website and Twitter account appeared to confirm that an exit scam had taken place.



Subsequently, the majority of the stolen funds were returned to users. This is commonly seen with this type of exploit, since the high degree of public attention and the ability to trace the stolen funds on public blockchains means that they are often left with no alternative.

DeFi Money Laundering

As we saw in the previous section, DeFi theft and fraud is big business, with billions of dollars in cryptoassets stolen from DeFi protocols each year. But this isn't the only way in which criminals make use of DeFi. DApps of various kinds are also used to launder proceeds of crime from other sources — particularly from hacks of centralized exchanges.

DeFi presents criminals with the opportunity to launder proceeds of crime by exchanging it for other assets or hiding the blockchain money trail — all without having to use centralized service providers that might alert law enforcement or seize their funds. In this section we describe how three types of DApp are used to do this:

- Decentralized exchanges (DEXs);
- Decentralized mixers; and
- Cross-chain bridges.

In practice, multiple DApps might be used by a criminal, in the same way that multiple money laundering techniques might be employed across traditional financial instruments. Often this activity constitutes "layering" — the addition of artificial complexity to transactions in order to make the tracing of funds more challenging. As we shall see in section 3, funds can often be traced through DApps thanks to the transparency of blockchain, however this can be technically challenging in practice especially when multiple complex DeFi protocols are used.

Decentralized Exchanges - Evading Token Seizure

Many cryptoassets, do not have their own blockchains but are instead issued on existing blockchains alongside other assets. These make up the majority of all cryptoassets, including all stablecoins, and are known as tokens. Ethereum pioneered this concept, with its ERC-20 token standard used to issue many thousands of assets.

These tokens are governed by smart contracts, created by the token's issuer. For example, a company launching a stablecoin on Ethereum will create a smart contract that follows the ERC-20 standard. This smart contract specifies how many tokens exist and keeps track of which Ethereum accounts hold them. The contract can also include functionality that allows the stablecoin issuer to freeze the stablecoins in a specific account. The issuer might use this in response to a law enforcement request, because the account is controlled by a sanctioned entity, or because they are aware that the account is being used for illicit purposes.

```
554     /**
555      * @dev Checks if account is blacklisted
556      * @param _account The address to check
557      */
558     function isBlacklisted(address _account) external view returns (bool) {
559         return blacklisted[_account];
560     }
561
562     /**
563      * @dev Adds account to blacklist
564      * @param _account The address to blacklist
565      */
566     function blacklist(address _account) external onlyBlacklister {
567         blacklisted[_account] = true;
568         emit Blacklisted(_account);
569     }
```

Fig 1: "Blacklist" functionality within the USDC stablecoin smart contract, which can be used to freeze tokens in certain Ethereum accounts.

The stablecoin issuer Tether has frozen accounts on a number of occasions. For example, in September 2020 the crypto exchange KuCoin suffered a hack that led to the loss of just over $280 million in cryptoassets — including $33 million of Tether's USD stablecoin. In response, Tether invoked the smart contract function that allowed it to freeze the accounts containing the stolen assets, preventing them from being moved or spent by the thief.

This means that a token thief, or any criminal holding tokens, faces the risk that their proceeds could be frozen at any time. Their solution to this is to urgently convert them into native blockchain assets such as Ether or Bitcoin. Unlike tokens, native blockchain assets are not issued by any central authority and cannot be unilaterally frozen — they are said to be "censorship resistant".

The conversion of criminally-derived tokens to native assets could be performed at a centralized exchange, but these businesses are now tightly regulated. Crypto service providers in most jurisdictions must now verify their customers' identities and perform rigorous anti-money laundering checks. Instead, criminals have turned to decentralized exchanges (DEXs) to convert tokens to native assets such as Ether. Most DEXs do not impose any restrictions on who can use them, keep records of user identities or check deposits for proceeds of crime — making them an attractive tool for criminals.

This tactic has been particularly popular among crypto thieves. Once tokens have been stolen, the thief will often rush to convert them to Ether at a DEX, before the token issuer has been made aware of the theft and has time to freeze the thief's account. The case study below describes this in the context of the KuCoin hack.

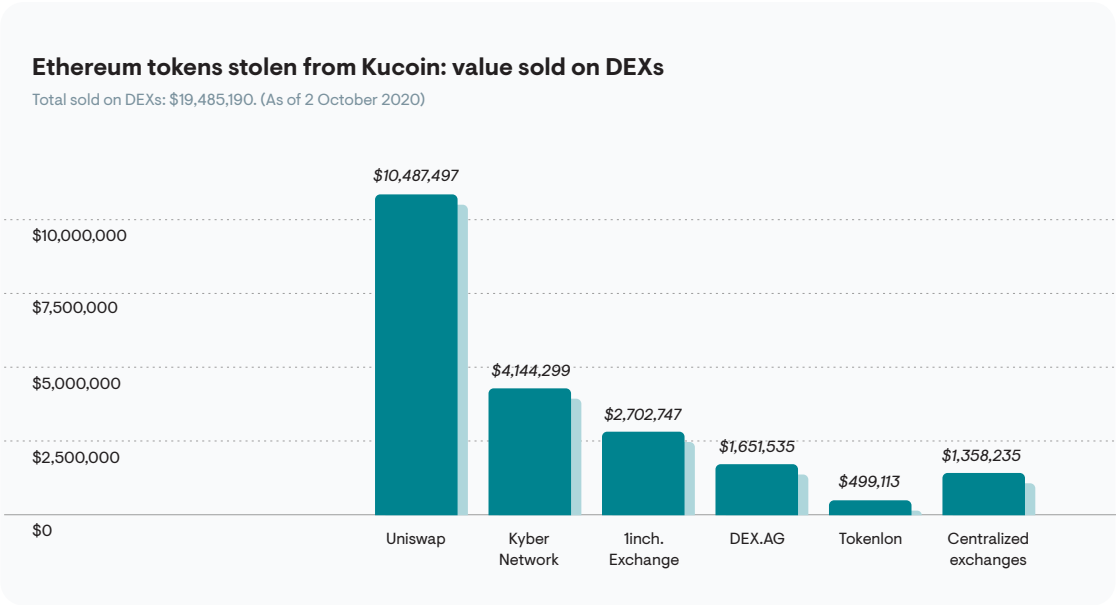
CASE STUDY 3

The KuCoin Hack - $19.5 million in stolen tokens converted to ETH through DEXs

In September 2020 hackers stole $281 million in cryptoassets from KuCoin, a Singapore-based crypto exchange. A wide range of assets were taken, including Bitcoin, XRP, Litecoin, and Ethereum-based tokens worth $152 million — including Tether (USDT), Chainlink (LINK) and Ocean Protocol (OCEAN).

In response to pleas from KuCoin, the token issuers, such as Ocean Protocol and Tether, began to freeze the accounts holding the stolen assets. Faced with the prospect of losing the proceeds of the hack, the thief began to cash-out the cryptoassets through centralized exchanges. However these exchanges used blockchain analytics tools to identify that the funds originated from the hack, and blocked this activity.

Instead, the thief began to send the stolen tokens to decentralized exchanges (DEXs). There, the tokens were converted to Ether, the native cryptoasset of the Ethereum blockchain. By doing this, they swapped the stolen tokens, which were at risk of being frozen, for a censorship-resistant cryptocurrency outside of the reach of authorities.



Decentralized Mixers - EvadingBlockchain Tracing

The transparency of blockchains means that proceeds of crime in cryptoassets can be traced from wallet to wallet. This means that the age-old law enforcement technique of "follow-the-money" is much more effective in cryptoassets than it has been in traditional payment mechanisms such as cash, for which there are no transaction records.

In many law enforcement investigations, criminals have been identified by tracing their crypto transactions to regulated service providers such as exchanges. These businesses are generally subject to AML regulations that require them to verify their customers' identities — allowing law enforcement to link a cryptocurrency transaction to a known individual.

In order to prevent their funds from being traced, criminals make use of mixers — online services that break the blockchain transaction trail by mixing together funds belonging to different people — in return for a fee. For example a ransomware gang might deposit their proceeds into such a service and withdraw crypto that has originated from legitimate sources. An investigator following the criminal's transaction trail would hit a dead end at the mixer.

These centralized mixers have a number of drawbacks. Their operators are usually anonymous and have full custody of users' funds, allowing them to potentially steal these funds and perform exit scams. Users must also trust that the operator is not keeping records that might allow law enforcement to trace transactions through the mixer — indeed there is a chance that the mixer might itself be operated by law enforcement.

Just as DeFi has brought us decentralized versions of centralized exchanges in the form of DEXs, it has also enabled the creation of decentralized mixers. These DApps eliminate custody risk by never allowing a third party to control user funds, and operate according to a verifiable smart contract so users can ensure that no transaction records are being kept, which could be shared with authorities.

The leading decentralized mixer DApp is Tornado Cash, which operates on a number of smart contract platforms. On the Ethereum version of Tornado Cash, users can deposit Ether or tokens (including stablecoins) to a smart contract, where the funds are pooled with those deposited

by other users. At a later time, a user can withdraw their funds to a different account, once they provide the Tornado Cash smart contract with a private note that was generated during the deposit process.

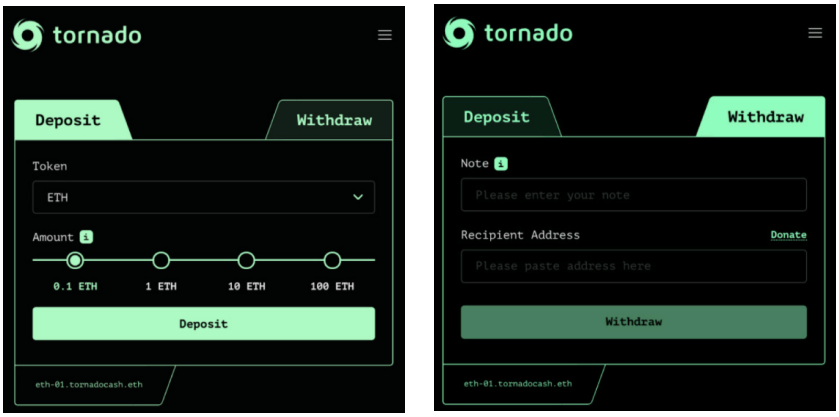


Fig 2: Tornado Cash user interface

In most cases DApps are completely transparent, with details of their inner workings available for anyone to monitor on the blockchain. This means for example that it is possible to trace a flow of funds through a DEX as one asset is exchanged for another. Of course this type of transparency and traceability is exactly what mixers are trying to avoid. Tornado Cash therefore makes use of a type of cryptography known as "Zero-Knowledge Succinct Non-Interactive Argument of Knowledge" (zk-SNARKs) to conceal details of the flow of funds through its smart contracts. This means that a Tornado Cash user can break the on-chain link between source and destination addresses without entrusting their cryptoassets to a third party that has knowledge of their transactions, or who might steal their funds.

As with other mixers, Tornado Cash has legitimate uses in preserving financial privacy for those making legal purchases with cryptoassets. However it has also become heavily used by criminals. Criminals seeking to cash-out their proceeds in ether or tokens at centralized exchanges face the risk of being identified and their assets seized, because their funds can be traced back through the blockchain to their illicit source. By passing these funds through Tornado Cash they can conceal the illicit origin of funds, making it easier to cash out through a regulated exchange.

Decentralized Cross-Chain Bridges - Moving Criminal ProceedsBetween Blockchains

All of the assets that operate on a given blockchain can be used in DeFi protocols. For example, one asset can be swapped for another using a DEX, or one asset can be used as collateral to borrow another asset using a lending protocol. However most blockchains are not interoperable — assets cannot move between blockchains. For example, Bitcoin cannot be transferred directly to an ethereum account and used on a DEX.

Cross-chain bridges offer a solution to this by allowing an asset on one blockchain to be represented as a token on another blockchain. Some bridges are centralized, for example Wrapped Bitcoin (WBTC) is an ERC-20 token that is backed 1:1 with bitcoins held by a centralized custodian (BitGo). If you want to transfer your Bitcoins to ethereum in order to make use of DeFi services, you can use your BTC to purchase WBTC tokens on a centralized, regulated exchange. WBTC can be converted back to BTC in a similar way.

Decentralized cross-chain bridges also exist, where custody is decentralized and use of

a centralized service provider is not required. For example a protocol called renVM acts as a decentralized custodian for Bitcoins used to back the renBTC ERC-20 token. Bitcoins can be converted to renBTC and used on ethereum by sending them to an address generated by renBridge, a DApp — without having to use a centralized, regulated services provider such as an exchange.

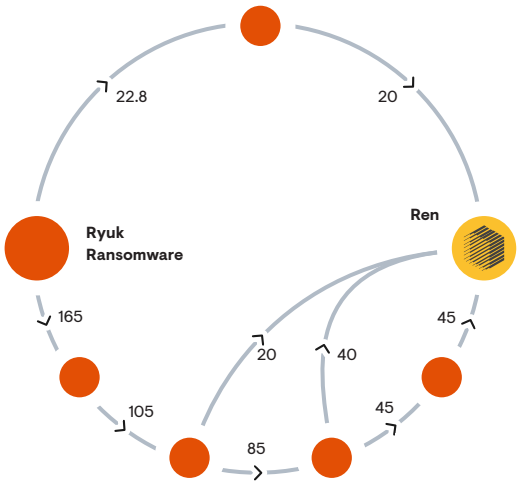
This property makes decentralized cross-chain bridges attractive to criminals. Proceeds of crime can be transferred between blockchains without going through a centralized service provider such as an exchange, where users' identities are verified and funds linked to illicit activity might be seized. Decentralized cross-chain bridges have been used to transfer proceeds of hacks, ransomware, darknet market sales and other criminal activity

CASE STUDY 5

Laundering the Ryuk Ransoms

Emerging in 2018, Ryuk ransomware has been used by multiple criminal groups to extract tens of millions of dollars in Bitcoin ransom payments from organisations around the world. Their proceeds have been laundered in multiple ways, including the use of mixers, non-compliant exchanges and privacy wallets.

In July 2021 Bitcoin from Ryuk began to be sent to RenBridge, the decentralized cross-asset bridge. At least 125 BTC, then worth around $4 million, in funds from ransom payments was "wrapped" through Ren, allowing it to be used on another blockchain such as ethereum.



Elliptic Forensics - the flow of Bitcoin from Ryuk to Ren

Fighting Financial Crime in DeFi — Leveraging Blockchain Transparency

In the previous sections we have seen that DeFi protocols are targets for fraud, and are being used to launder proceeds of crime to avoid their seizure.

Cryptoassets have always been susceptible to illicit use because they are outside of the control of authorities and they can be used without providing an identity. However their transparency and traceability have meant that the age-old "follow-the-money" investigative techniques can still be used by law enforcement to identify criminals through their crypto transactions, and bring them to justice.

Where this technique faces challenges is when cryptoassets move into centralized service providers, such as exchanges. When this happens the funds go "off-chain" — the cryptoassets are pooled together or converted into other assets, and it is no longer possible to follow the money trail on the blockchain. Instead law enforcement must rely on records kept by these service providers in order to continue following the money.

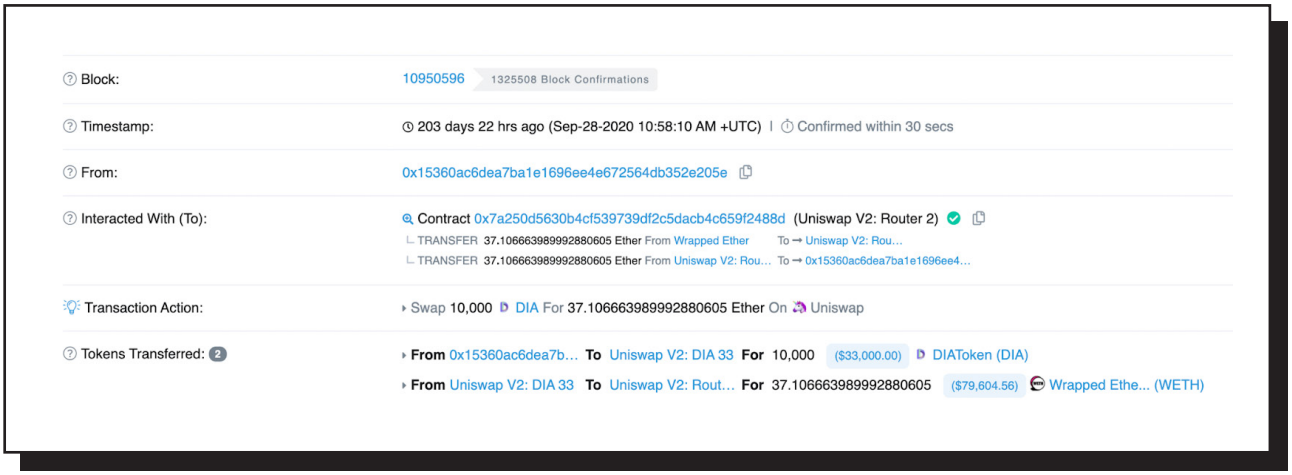


Fig 3: Records from the public Ethereum blockchain showing the conversion of DAI tokens to ether using Uniswap, a DEX. The DIA was stolen from the KuCoin exchange. The flow of funds is visible and perfectly traceable by law enforcement. Source: Etherscan.

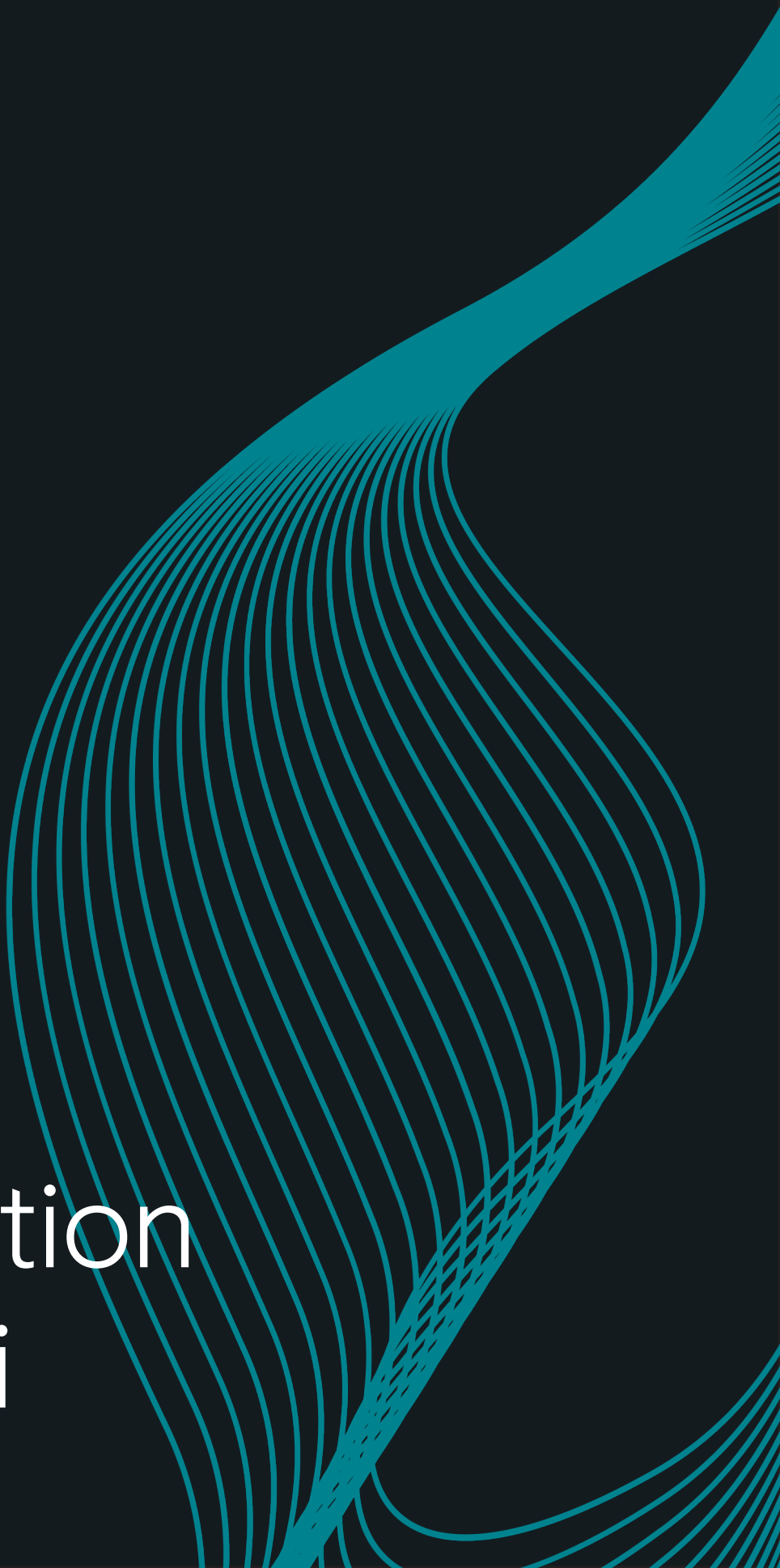
In most jurisdictions these businesses are regulated and compelled to maintain these records, however there are still many service providers that do not do so. These businesses act as magnets for proceeds of crime in crypto and present law enforcement with a significant challenge.

By contrast in DeFi, assets do not go off-chain and they usually remain traceable. For example if Bitcoin is sent to Coinbase, a centralized exchange, and converted to Litecoin, all that is visible on the blockchain is the deposit to Coinbase. Contrast this with converting Tether to Ether on a decentralized exchange such as Uniswap. The deposit of Tether at Uniswap, its conversion to Ether, and the withdrawal of Ether are all visible for all to see on the Ethereum blockchain. This is a huge advantage for law enforcement when tracing proceeds of crime, who must otherwise rely on a centralized service provider to provide the information that allows them to continue tracing funds.

Of course some services such as decentralized mixer DApps do not offer such transparency, but in general DeFi offers higher levels of traceability that can be leveraged by both law enforcement and regulated financial institutions in order to detect and fight financial crime.

03

The Regulation of DeFi



The opportunities presented by decentralized finance (or DeFI) are undeniable. The ability to engage in sophisticated financial transactions with no (or minimal) third party intermediation represents a wholesale shift in product and service access and presents perhaps the greatest opportunity for global financial democratization in modern history. The nearly boundless possibility presented by this movement is not, however, without its pitfalls. The regulatory landscape is unclear and ill-defined; even the applicability of core financial regulations related to licensure, risk management, AML, and KYC has been called into question. The nascency of the industry means that we must rely on a combination of the limited number of guidance documents, rules and regulations, enforcement actions, and fiat financial sector parallels to intuit where regulators might go next.

Is DeFi Regulated?

On November 9th, SEC Commissioner Caroline A. Crenshaw released a guidance letter seeking to clarify the challenges faced by regulators and industry participants, while providing an overview of the risks attendant to the decentralized economy. When discussing who bears the responsibility of regulating DeFI, the Commissioner wrote:

> *"[M]ultiple federal authorities likely have jurisdiction over aspects of DeFi, including the Department of Justice, the Financial Criminal Enforcement Network, the Internal Revenue Service, the Commodity Futures Trading Commission, and the SEC. State authorities likely have jurisdiction over aspects as well. In spite of the number of authorities having some jurisdictional interest, DeFi investors generally will not get the same level of compliance and robust disclosure that are the norm in other regulated markets in the U.S. [...] no DeFi participants within the SEC's jurisdiction have registered with us, though we continue to encourage participants in DeFi to engage with the staff."* [5]

The acknowledgement that a panoply of regulators may be responsible for different aspects of regulatory oversight and that DeFi protocols and related entities often operate in non-compliant manners reveals a significant problem: there is a disconnect between regulators and the industry as to:

- what constitutes a regulated activity; and
- what type of regulatory regime should apply.

What is clear, however, is that the current "caveat emptor" system of self regulation is not sustainable.

Notably, Commissioner Crenshaw stated that:

> *DeFi participants' current "buyer beware" approach is not an adequate foundation on which to build reimagined financial markets. Without a common set of conduct expectations, and a functional system to enforce those principles, markets tend toward corruption, marked by fraud, self-dealing, cartel-like activity, and*

[5] https://www.sec.gov/news/statement/crenshaw-defi-20211109

> *information asymmetries. Over time that reduces investor confidence and investor participation.*

This quote makes clear that functional regulation of the DeFI space is inevitable and, for honest actors, will be a largely positive development. By promoting the safety and soundness of this new sector, the SEC may increase user trust while reducing instances of fraud and financial crime.

What are the Major Forms of DeFi?

The term "Decentralized Finance" encompasses a great number of interconnected pseudo-financial services propelled by smart contracts and recorded on a blockchain. Regulators have taken a particularly keen interest in three types of DeFi-related products:

1. Decentralized exchanges
2. Stablecoins (both asset backed and algorithmic)
3. Debt products

In looking at decentralized exchanges and stablecoins, it's important to consider the current state of regulation and where regulators are likely to go next. This means determining the applicable industry-specific and financial crime regulatory risks likely to apply to a given DeFi protocol and how regulators expect (or may expect in the future) that they be mitigated. When examining DeFi debt products, one should understand the contentious regulatory issues facing the industry and the judicial tests that may ultimately be applied to resolve them.

Decentralized Exchanges

Decentralized exchanges represent a shift in the way that virtual assets change hands. In the past, parties had to either rely on a centralized third party to facilitate an exchange of virtual assets, or else rely on peer-to-peer connection services with dubious reputations. With a decentralized exchange, users can securely swap tokens through the use of liquidity pools, in which pairs of tokens are placed into pools by liquidity providers and exchange users are able swap one coin or token in a pair for the other, by paying a fee to the liquidity providers.

Control and Ownership

There are a variety of risks and compliance requirements associated with the implementation of a decentralized exchange. At the most basic level comes the question of control and who is ultimately responsible for the activities of the exchange. The developers of the software powering decentralized exchange implementations have argued vociferously that they merely create software and as such, *per* the Financial Action Task Force's Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers, should not be subject to attendant regulatory requirements. [6] Though this may be true, some person, legal or natural, may own and operate a domain from which an implementation is accessed. Though the decentralized app may be accessed through any functioning implementation/access portal, a particular responsibility may fall on those who control and maintain an overwhelmingly popular means of accessing the underlying protocol. This notion was reinforced through the October 28th publication of updates to the FATF Guidance, which state that when an entity or individual has "control or sufficient influence over assets or over aspects of the service's protocol, and the existence of an ongoing business relationship between themselves and users, even if this is exercised through a smart contract or in some cases voting protocols" they should be subjected to regulatory oversight and may appropriately be classified as VASPs.

In the world of traditional finance, financial institutions must understand the beneficial owners of 25% or more of their legal entity customers. These persons are thought to exercise significant control over the operations of the entity or, at least, materially benefit from it. In the United States, this is codified under the Financial Crime Enforcement Network's (FinCEN's) Customer Due Diligence Rule (the CDD Rule). [7] In searching for a test to determine how control and ownership of a decentralized exchange may be determined, it makes sense to look to this rule for guidance and expect that a similar threshold be applicable in the DeFi world.

Though no person can be said to "own" an implementation of a decentralized exchange protocol, there are those who own the rights to make significant decisions for said implementation and, under the recently released FATF guidance [8] may potentially exercise "sufficient influence in the DeFi arrangements" to meet the definition of a VASP: governance token holders. Governance tokens are virtual assets that carry attendant rights, such as the ability to determine fee structures, liquidity rules, and/or other financial infrastructure decisions. Borrowing from the CDD Rule in the US — and similar beneficial ownership disclosure requirements globally, requiring token holders of 25% or more of the total supply to disclose their name, date of birth, government ID number, and physical address (piercing through layers of legal entity ownership when necessary) — would provide for far greater clarity as to who ultimately maintains significant decision making authority within the implementation.

[6] *https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf*

[7] *https://www.fincen.gov/resources/statutes-and-regulations/cdd-final-rule*

[8] *https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf*

Governance token holders are not solely responsible for the administration of a DeFi protocol and should not bear the responsibility for compliance alone. Perhaps the most directly responsible third-parties are the domain owners/operators referenced above. By providing the public with access to means by which they may exchange virtual assets, the entities or individuals maintaining the platform may meet the FATF definition of a Virtual Asset Service Provider (VASP), even though one specific website is unlikely to be the only method by which the protocol may be accessed.[9] Entities operating within the US likewise meet the FinCEN definition of a Money Services Business and must register as such. This obligation springs from the fact that, while "custody" of the asset has been the traditional litmus test FinCEN has used when determining registration requirements, the term itself has not been well defined. It may well (and likely will be) the case that liquidity locked within a DeFI protocol may be presumed to be held in custody by that protocol, with the compliance obligations flowing vicariously to the VASP responsible for the specific protocol implementation.

Financial Crime Regulatory Requirements

FinCEN registration, though necessary, is not adequate in meeting regulatory obligations for VASPs operating within the United States. The implementation of an adequate AML program and the collection of required KYC information is vital to meeting the minimum standards set by US federal functional regulators. Interestingly, though decentralized exchanges have strongly argued against the notion that mere domain ownership and maintenance of the DeFi protocol implementation is enough to bring them into scope as VASPs, some have nonetheless attempted to meet minimal VASP regulatory obligations, perhaps in an effort to head off regulation by keeping their own house in order.

Of particular note is the fact that certain decentralized exchanges have implemented bare-bones sanctions screening to prevent their tools from being used by the most obviously "bad" actors in a given ecosystem. As regulatory pressure increases, it is likely to become clear that, though certain aspects of governance may be truly decentralized, there is typically some relevant third party who can be appealed to and scrutinized, in order to ensure that the virtual asset world can be brought in line with the financial crime expectations of the fiat world.

If decentralized exchanges are, in fact, deemed to be VASPs, they will also have to contend with requirements under the Travel Rule. The Travel Rule is a regulation promulgated by the FATF and implemented in individual jurisdictions requiring the transfer of virtual assets between VASPs, financial institutions, or between VASPs and financial institutions to include information related to the originator's and beneficiary's personally identifying information, along with the details of the transactions. Decentralized exchanges would then be required to investigate whether any liquidity providers on their platform are VASPs or financial institutions, and if so whether such entities are paired against each other creating a Travel Rule obligation. The question of who might qualify as the decentralized exchange's customer is also germaine. If all platform users are deemed to be customers, then Travel Rule requirements would be applicable to all platform transactions, as there is no carve out or exception to the Travel Rule for transactions occurring within the walls of a single VASP or financial institution.

Industry-based Regulatory Requirements

The risks posed by financial crime and ownership concerns are not the only factors that need to be taken into consideration when evaluating a decentralized exchange's regulatory obligations. The

[9] *https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf*

actual products offered must also be categorized and, when appropriate, subjected to category-based regulations. Such categories may notably include securities and commodities, each of which have long standing and experienced attendant regulatory agencies with deep subject matter expertise. Regulatory pressure was notably felt by the main implementation of the most famous decentralized exchange protocol, Uniswap, this July, when 120 coins were removed from the platform.[10] The coins removed represented what appeared to be potential commodity derivatives, under the purview of the Commodity Futures Trading Commission (CFTC) and tokenized securities, falling under the regulatory ambit of the Securities and Exchange Commission (SEC). Though no public comment was made about any specific nexus to a given US regulator, the timing of the removal was notable. A month later, reports surfaced of an SEC investigation into Uniswap Labs, the company responsible for developing the Uniswap DeFi protocol.

One of the most notable features of the mass removal of coins from the popular Uniswap implementation was the total absence of community guidance or governance token-holder engagement in the decision making process. This action made clear that, when the proverbial rubber hits the road, centralized actors can (and will) exercise significant control in a potentially undemocratic manner, so as to shield themselves and their interests from regulatory enforcement actions or prosecution. The whole incident revealed that a truly decentralized exchange remains somewhat of Platonic Ideal, yet unachieved in the real world. So long as there are consequences that may be brought to bear on entities and individuals with the power to change or modify how people use a given DeFi protocol implementation, one can be sure that such power will, in fact, be used to avoid those consequences.

Given the interest that's been seen from securities and commodities regulators with regard to decentralized exchanges, one can expect that market regulations similar to those seen in those two markets are likely to be adopted in the virtual asset space as well. Specifically, market manipulation and insider trading are unlikely to continue unabated in the world of virtual assets. The commonplace occurrence of pump and dump scams and "rug pulls" has become a stain on the industry —drawing comparison more akin to dispretuable penny stocks than to blue chip companies or sophisticated financial instruments. Insider trading is also rampant, with information about projects and token economics shared among small groups of interested parties at the expense of the broader virtual asset community. By prohibiting this activity — along with market abuse such as wash trading, painting the tap, churning, and front running — a safer and more sound virtual asset ecosystem may be created so that institutional and retail investors alike can take comfort in knowing that they are playing a fair game.

Regulatory Challenges of Decentralization

In the future, there may be significant challenges to regulators as the potential for actual decentralization increases. If, for instance, one were to use a privacy oriented operating system to create a privacy oriented software wallet, receive coins to that wallet from a mixer, use said coins to purchase a decentralized domain from a service provider, and operate an implementation of a decentralized exchange DeFI protocol anonymously from that domain, it may be very difficult to censor the activity or identify the underlying entities or individuals responsible for the implementation. Not to say that it's impossible — regulators, law enforcement, and (particularly) intelligence agencies are extremely proficient at identifying bad actors when they put their minds to it, and a large unregulated decentralized exchange may attract exactly that type of keen interest and attention. Regulators must focus on identifying the natural and legal persons behind such opaque operational models, and determine whether they are operating in a compliant manner. If such identities cannot be ascertained, and there is a reasonable basis to believe that unknown

[10] *https://github.com/Uniswap/interface/blob/main/src/constants/tokenLists/unsupported.tokenlist.json*

operators of a given implementation of a protocol may be bad actors, regulators may have no choice other than to block access to these implementations and pursue regulatory or legal actions against those who would seek to impermissibly access them.

The type and scope of regulation will also vary substantially depending on the underlying technology used to develop and maintain a decentralized exchange. Certain exchanges rely on total (or near total) decentralization. This means that an automated system sets and maintains pricing, facilitates transfer, and operates autonomously without human intervention, purely (or almost purely) on the blockchain.These exchanges will likely argue that the responsibility for controlling and maintaining the protocol is so well diffused among stakeholders as to limit the regulatory liability of any one actor. Though this argument may initially appear compelling, noting the revised guidance promulgated by FATF, one must believe that some third party may ultimately be identified as having sufficient control as to bear responsibility for the regulatory compliance of the exchange service itself. Global regulators have been clear: pleading decentralization is not enough; if a service cannot be adequately regulated, its legal viability must be allied into question,

Contrarily, other ostensibly "decentralized" exchanges may, in fact, rely entirely on a centralized third party to maintain a trade order book on a server. In these instances, there may be a clearer indication of who is responsible for the regulatory administration of the exchange, and the "decentralized" aspect of the app may relate more to the technical means by which trades occur rather than to platform governance and decision making. Given the clearer nexus of such hybrid exchanges to a central party responsible for the ongoing business concern of the platform, there should be an expectation that VASP regulatory compliance requirements have been assessed and that controls have been devised and/or implemented. Unlike the more overtly "decentralized" exchanges, hybrid exchanges cannot rely on the (already weak) argument that regulatory compliance responsibility sits with the community at large, rather than with a team of exchange protocol promoters.

Stablecoins

Stablecoins have attracted tremendous interest from both the traditional financial sector and virtual asset-native enterprises. Stablecoins are designed to maintain a fixed price and are most often pegged against a fiat currency or asset. Stablecoins come in two flavors, asset-backed and algorithmic. Asset-backed stablecoins are kept stable through the maintenance of reserves — such as gold, dollars, pounds, or euros — in proportion to the number of coins issued. Algorithmic stablecoins maintain stability through the use of a DAO These smart contracts may, in some instances, implement a collateralized lending protocol in which a coin or token is locked into a contract as collateral and the algorithmic stablecoin is issued in return. This protects coin stability while neatly sidestepping the accounting and banking challenges faced by asset-backed stablecoins.

Asset-backed Stablecoins

Asset-backed stablecoins, though neither created nor maintained through decentralized protocols, represent the common currency of the DeFi economy. Their ubiquitous usage is the result of their lack of volatility and their perceived trustworthiness, springing from the reserves of adequate backing instruments purportedly held by coin issuers. Such coins face particular regulatory challenges, as fraud and misrepresentation of asset backing have proven to be major issues. Perhaps the most notable incident resolved this year occured with stablecoin issuer Tether, whose coin has a current overall issuance valued at roughly $70 billion. Tether settled with the New York Department of Financial Services over allegations that the stablecoin issuer made loans to its sister company, crypto exchange BitFinex, that caused Tether to become significantly undercapitalized, failing to meet its claim of one-to-one dollar backing. Though Tether did not admit wrongdoing, they did agree to pay an $18.5 million fine to settle the matter and drew significant mainstream attention to the issue of stablecoin backing.

Although the Association of International Certified Public Accountants had previously issued guidance on certain aspects of accounting treatment for stablecoins [11], only true government-issued guidance can create the type of regulatory certainty needed for large scale institutional engagement and mainstream adoption. In the US that guidance arrived in September 2020 with the publication of Office of the Comptroller of the Currency (OCC) Interpretive Letter 1172, OCC Chief Counsel's Interpretation on National Bank and Federal Savings Association Authority to Hold Stablecoin Reserves [12]. That letter specified that:

> *a national bank may hold such stablecoin "reserves" as a service to bank customers [...] this letter only addresses the use of stablecoin backed on a 1:1 basis by a single fiat currency where the bank verifies at least daily that reserve account balances are always equal to or greater than the number of the issuer's outstanding stablecoins.*

This guidance gave some degree of comfort to federally regulated banks, allowing them to hold reserves for stablecoin issuers without facing any immediate regulatory reproach. The flip side, though, is that the guidance is only applicable to coins backed on at least a one-to-one basis by a single fiat currency and that the bank ensures the veracity of this claim on a daily basis. This can be particularly tricky if a given bank does not hold the entirety of the reserves of a given stablecoin, which — given the risk of holding multibillion dollar sums for what is effectively a low-governance

[11] https://us.aicpa.org/content/dam/aicpa/interestareas/informationtechnology/downloadabledocuments/accounting-for-and- auditing-of-digital-assets.pdf
[12] https://www.occ.gov/topics/charters-and-licensing/interpretations-and-actions/2020/int1172.pdf

tech startup with lots of third party flows — they may not want to. In such a case, the bank would have to rely on financial statements, audit reports, and cooperation from other financial institutions in order to verify the totality of reserves of the stablecoin. This lack of directly performed due diligence creates a troubling potential information asymmetry between the issuer and its banking partners, and introduces significant new regulatory and risk management concerns.

In January of 2021, the OCC revised its previous stablecoin guidance with OCC Interpretive Letter 1174, *OCC Chief Counsel's Interpretation on National Bank and Federal Savings Association Authority to Use Independent Node Verification Networks and Stablecoins for Payment Activities*, [13] stating:

> *We therefore conclude that a bank may validate, store, and record payments transactions by serving as a node on an INVN [Independent Node Verification Network]. Likewise, a bank may use INVNs and related stablecoins to carry out other permissible payment activities. A bank must conduct these activities consistent with applicable law and safe and sound banking practices.*

This guidance clarifies that federally regulated US banks may leverage stablecoins in the use of payment activities, further bridging the gap between the decentralized and traditional financial services industries. The inherent technical benefits of leveraging a fast and secure blockchain based system made adoption for international payment settlements inevitable; that one of the lead regulators in the US has recognized this and adapted its regulatory approach and guidance in response is encouraging. By embracing regulation and looking to better protect stablecoin investors from the risk of value fluctuation, stablecoin issuers may promote mass adoption and broaden the community using the coin.

Though not formally a regulator, the President's Working Group on Financial Markets has provided notable guidance that was further highlighted and echoed by the OCC. Specifically, they were clear that stablecoin arrangements "should have the capability to obtain and verify the identity of all transacting parties, including for those using unhosted wallets." [14] The implications of this statement are vast. There would seem to be an imputed responsibility on those involved in stablecoin "arrangements" (an undefined term) to conduct KYC on all parties leveraging the stablecoin. This would effectively force market participants to develop controls able to censor transactions to wallets without known owners. Setting aside the philosophical concerns related to privacy and the international financial system, the technical challenges loom large. A control would have to be built into the coin preventing it from being passed from an identified party to the transaction (perhaps a KYC'd individual who purchased the stablecoin at an exchange) to an unidentified party (potentially the holder of an unhosted wallet). This would extend Travel Rule-like requirements onto transactions with natural persons and impose strictures that go far beyond those applicable in the fiat universe. Though there is certainly room for enhanced controls and financial crimes compliance related to stablecoins, imposing such a significant burden on stablecoin users would severely stifle the industry and create a far more burdensome requirement than is applicable to equivalent dollar or euro based transactions. With the recent joint guidance [15] released by the President's Working Group on Stablecoins, The OCC, and the Federal Deposit Insurance Company (FDIC), it is unclear if this expectation remains intact, as the document did not directly address whether all transacting parties must truly be identified by those involved in stablecoin arrangements.

In a more recent development, the SEC has asserted regulatory authority over stablecoins, creating tremendous uncertainty as the details of the forthcoming regulatory augmentation

[13] https://www.occ.gov/news-issuances/news-releases/2021/nr-occ-2021-2a.pdf
[14] https://www.occ.gov/news-issuances/news-releases/2021/nr-occ-2021-2a.pdf
[15] https://home.treasury.gov/system/files/136/StableCoinReport_Nov1_508.pdf

remain unknown. There is significant speculation that, under the SEC, stablecoins will be forced to adopt policies and controls similar to demand deposit accounts or money market funds, with the underlying assets closely monitored and reported on. The SEC, under current Chairman Gary Gensler, has been particularly piqued in its criticism of the virtual asset sector and of stablecoins in particular. If the SEC's assertion of regulatory oversight proves to bring forth a stricter and more punitive regulatory environment, there may be heightened faith in the actual stability of the coins, but significant barriers to entry for new market participants may also be created. The fact that a securities regulator (rather than a banking regulator) will oversee the industry is an interesting development, as it's a clear indicator that stablecoins will be viewed more similarly to funds composed of currencies than to currencies themselves. The payment functionality appears to be taking a back seat to the pooled investment vehicle-like nature of the underlying structure of the coins.

The proposed STABLE Act, [16] which seeks to regulate the market for stablecoins in many of the ways previously endorsed by Chairman Gensler and favored by many progressive voices in the US congress, is likely to be revised or replaced given the recent decision by the SEC to assert itself in the sector. We expect to see legislation in support of the Chairman's regulatory goals proposed in the near future, as political pressure may necessitate expediency.

Algorithmic Stablecoins

While asset backed stablecoins are tremendously popular within DeFi ecosystems, representing a large portion of paired coins available on decentralized exchanges, it's algorithmic stablecoins that represent the purest DeFi play and that require the least interaction with the traditional financial sector. From a regulatory perspective, algorithmic stablecoins are unlikely to be treated in the same way as asset backed stablecoins, as they have an entirely different risk profile and technical implementation.

Much of the risk in popular algorithmic stablecoins such as DAI lies within the technical implementation and security of the algorithm underpinning the DAO and within the value of the collateral provided prior to the coin issuance. If the protocol is easily hacked or otherwise exploited, it's conceivable that a large amount of stablecoins may be issued to a person without that person having to provide the required collateral to receive the stablecoins as a loan. When receiving a loan denominated in an algorithmic stablecoin and collateralized by a virtual asset, there's also significant risk that the value of the collateral dips below the value of the loan. If, for example, a DAO requires a 200% collateralization rate, an individual might deposit $200 worth of a virtual asset in exchange for $100 worth of an algorithmic stablecoin as a loan; when the stablecoin loan is repaid, the collateral is returned. If the value of the virtual asset deposited as collateral were to crash by 90%, the stablecoin's value would drop dramatically, as the outstanding loan balance would significantly outweigh the provided collateral, dramatically reducing the incentive to repay.

Credit-like regulations and standards must be applied to the collateral posted by borrowers, to ensure that said collateral, which is used to receive a stablecoin loan, is high quality and unlikely to plummet. Such a control may ultimately prevent the collapse of a stablecoin. It's also important that loan terms are fair and confirm with accepted debt issuance standards. Interest rates should be clearly disclosed and any rate adjustments should be presented to the debtor. If algorithmic stablecoins are to gain the type of mainstream acceptance that asset backed stablecoins currently seem poised to gain, they must maintain a track record of stability and usability as both a store of value and a method of payment intermediation.

[16] *https://tlaib.house.gov/sites/tlaib.house.gov/files/STABLEAct.pdf*

Debt Products

Speaking of credit products, debt issuance in the DeFi world has been a major topic of conversation during 2021. The newness of the industry and the constantly evolving nature of the regulatory landscape make it difficult to prognosticate as to what regulators and the Courts might eventually decide. Rather than guess at what may or may not ultimately happen in any given case, we should instead look to understand the determining factors at play and why each side holds the opinion that it does.

Howey Test Analysis

In determining whether any given activity represents the establishment of a security, there are two potential tests that may be applied by US Courts. The first, the *Howey Test*, [17] specifies when an investment contract is formed, thus creating a regulated security. This test considers whether there has been an investment of money, in a common enterprise, with the expectation of returns, resulting from the efforts of another. If a given DeFi debt product implementation were to result in a debt-to-equity conversion scheme, by which profits springing from the target of the investment might materially affect the financial situation of the investor, a security may be deemed to exist. Likewise, if the purchase and lending of a virtual asset is deemed to be an investment in a pooled investment vehicle operated by some third party sponsor (such as a DAO or exchange), a security may potentially exist under a Howey analysis.

Reves Test Analysis

Though a Howey analysis may potentially determine whether a security exists based on the nuances of a given DeFi debt product, the likely more applicable test is derived from the *Reves* case. [18] The *Reves Test* looks specifically at whether a particular note may constitute a security offering. The standard set in Reves states that there is a rebuttable assumption that a note represents a security. The four-prong test that assesses whether such rebuttal is valid evaluates the motivations of the buyer and seller, the plan of distribution, public expectations, and the presence of any relevant risk reducing features. While the test described by the Court is helpful, the lack of guidance as to the weight of each individual factor leaves a great deal of room for interpretation and debate.

If the motivation of the seller is to raise money to find a business opportunity or to finance operations and the buyer seeks to earn profit, weight is added to the argument for the existence of a security. In a DeFi debt scenario, one must determine whether the lending of a virtual asset to a third party custodian, exchange, DAO, or other entity is done to finance the said entity's operations, or instead for some other purpose. Similarly, an analysis must be performed to understand whether the lender in such a scenario expects to earn profits from the loaned assets.

The plan of distribution of the instrument must also be considered when determining whether the note may represent a security. If there is "common trading" of the note, irrespective of whether or not a secondary market exists for said instrument, the argument that a security exists is strengthened. If the notes are issued to a broad segment of the public, it is likely that common trading exists. The Courts must determine whether the distribution model implemented through

[17] *https://supreme.justia.com/cases/federal/us/328/293/*
[18] *https://supreme.justia.com/cases/federal/us/494/56/*

a given DeFI product offering is sufficiently broad as to materially affect the argument that the product is representative of a security,

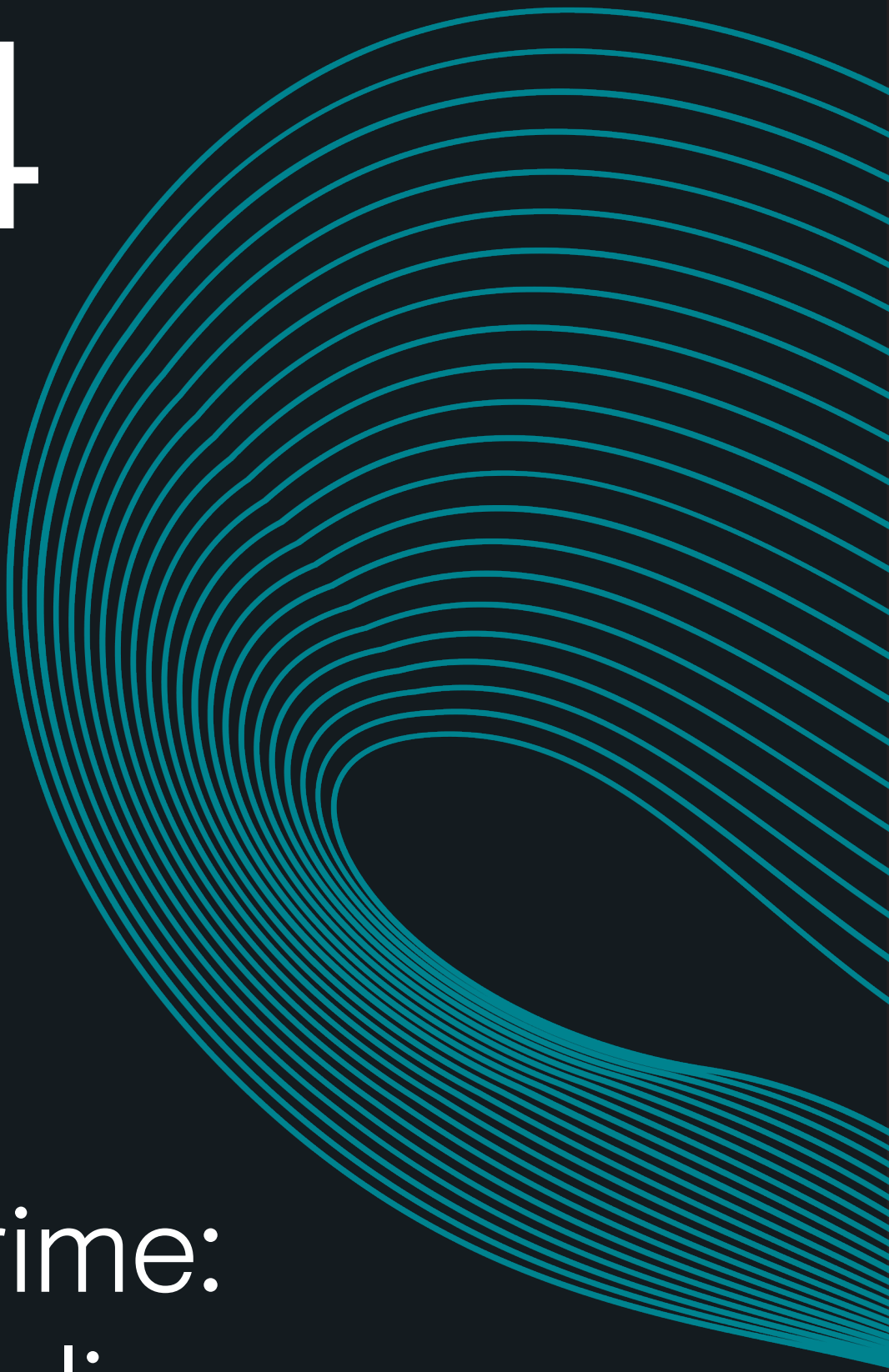
Even if the above factors are inapplicable, a note offered via a DeFi protol may nonetheless wind up being a security should the public expectations factor apply. If the public may reasonably believe that a security exists, even if the technical circumstances of the product suggest otherwise, a security may, in fact, exist. The lack of clear public sentiment as to the nature of DeFi debt products and the relative newness of the industry makes it unclear whether there is a reasonable public expectation that these products are securities. This regulatory and judicial uncertainty creates substantial risk that public understanding may drive the determination of whether or not a security exists.

Finally, the Court will consider whether any feature reducing the risk of the note exists. Such features include coverage under other regulations which would negate the need for protection under applicable securities laws. It may be important to consider whether features that may scope the note into other regulatory regimes, such as collateralization or insurance of the note, exist within a given DeFi debt implementation. If assets are covered by another regime, there is less of a likelihood that a security will be deemed to exist.

Closing Remarks

The creation of DeFi-specific regulator initiatives has just begun, yet there has already been substantial progress made. In the US federal regulators have taken a proactive approach to scrutinizing the industry and have proposed various regulatory models to address various types of DeFi protocols and their attendant risks. By focusing on maintaining the principles of market fairness, financial crime mitigation, safety, and soundness, regulators and industry participants may successfully partner to continue the expansion of the DeFi universe while protecting consumers and effectively curtailing financial crime.

04



DeCrime: Compliance and Controls

Know Your Customer

The implementation of controls related to KYC in the DeFi space has proven to be a contentious issue. The very notion that the underlying identities of the persons — both natural and legal — must be disclosed to third party intermediaries and, when required, reported to regulatory and law enforcement bodies, seems to go against the zeitgeist of the sector. That said, there is little doubt that in order for the industry to mature and thrive, there will be requirements attendant to identify verification and disclosure of beneficial ownership or its equivalent. The appropriate effectuation of these requirements will depend on the specifics of the protocol in question and the service that it offers, as the attendant risks will vary based on the activity undertaken.

KYC for Decentralized Exchanges

Decentralized exchanges bear perhaps the greatest KYC burden in the DeFi space, as they have thus far been popular vehicles through which an exchange of virtual assets may be effectuated without any person having to disclose their identity and personally identifying information. Decentralized exchange operators, specifically those persons deemed to exercise "control of sufficient influence in the DeFi arrangements" as defined under the revised FATF Guidance, [19] should (and in the future, will likely be required to) collect information appurtenant to the CIP and CDD Rules promulgated by FinCEN. This means that liquidity providers, exchange users, and potentially significant governance token holders should be compelled to disclose their names, physical addresses, dates of birth, government identification numbers, and, where there is a legal entity customer, beneficial ownership information to the exchange. This information should be verified through documentary or non-documentary (such as a third-party database) sources and provided to regulators and law enforcement officials when required. The difficult question that will naturally arise is: "what about existing customers/liquidity providers/governance token holders/ etc?" Decentralized exchange protocol operators deemed to be VASPs should initiate some sort of periodic or *ad hoc* review cycle to uplift these customers to complaint status. Non-compliant customers should be subjected to a risk exit.

KYC For Asset-backed Stablecoins

Asset-backed stablecoin issuers have a different set of KYC concerns to consider, as they may not always deal with direct customers. Depending on the method of issuance, stablecoin issuers may only interact with established VASPs and financial institutions, to whom the responsibility for conducting KYC would likely pass. In this case, the issuer should partner with the entities providing retail access to its coins and ensure that they have adequate KYC processes in place, designed to comply with (and ideally exceed) regulatory requirements related to customer identification. When the issuer sells a stablecoin directly to a customer, on the other hand, the responsibility to conduct appropriate KYC will apply. In addition to the CIP Rule and CDD Rule requirements discussed earlier, it's also important to consider risk-based factors when evaluating the KYC program of a stablecoin issuer. Such factors should include: country of domicile (and incorporation when applicable), association with negative media, political exposure, and history of known AML events.

KYC for Algorithmic Stablecoins & Debt Products

Algorithmically-issued stablecoins and DeFi lending protocols present a separate set of challenges, specifically those related to the lenders and borrowers utilizing the DeFi debt protocol. These

[19] *https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf*

transactions may take place purely to facilitate lending, or alternatively may underpin the issuance and stability of algorithmic stablecoins. The identities of persons borrowing and lending within a debt protocol ecosystem should be properly identified and subjected to risk based compliance due diligence. Further, the source of wealth for lenders should be confirmed, so as to ensure that the funds being entered into the protocol are explicable and do not represent potentially suspicious activity. Unique local due diligence issues should also be considered, such as potential usury laws, credit market regulations, and consumer protection regulations that may affect the virtual debt market.

Anti-Money Laundering

If they are to comply with emerging regulations and help to reduce the instances of financial crime occuring in the decentralized economy, anti-money laundering controls must be implemented by the VASPs behind DeFi protocol implementations. The VASPs operating decentralized exchanges may implement adequate AML programs by following the traditional "Five Pillars'' approach to financial crime mitigation. [20] These include:

- having written policies and procedures related to money laundering detection and prevention;
- ongoing training of employees or other responsible parties;
- ongoing customer due diligence on users requiring KYC;
- appointing an AML officer responsible for the financial crime compliance of the protocol; and
- independent testing of the compliance program.

AML for Decentralized Exchanges

The larger and more sophisticated the decentralized exchange platform, the more rigorously the pillars should be applied. These emerging compliance requirements are likely to prove to be challenging for decentralized exchange implementation operators, as the growing pains related to becoming a regulated VASP are felt. Determining what degree of AML compliance is actually possible is the first step, and an assessment of traditional AML typologies (such as structuring, placement, layering, and integration) should be undertaken to evaluate a given protocol's vulnerability. Further, compliance mechanisms related to the Travel Rule must be implemented for all VASPs supporting transactions with financial institutions or other VASPs, so that the transaction details and personally identifying information of the originator and beneficiary may be accessed by regulatory authorities and law enforcement agencies when needed.

AML For Stablecoins

Stablecoins are an integral part of the DeFi sector. This fact was reinforced by the President's Working Group on Stablecoins, The OCC, and the FDIC, when they stated in their recently released joint paper:

> *Stablecoins are central to the functioning of DeFi, as they are often used in DeFi arrangements to facilitate trading or as collateral for lending and borrowing. For example, stablecoins often are one asset in a pair of digital assets used in a so-called "automated market maker" or "AMM" arrangements.* [21]

Asset backed stablecoin issuers face a two pronged challenge when considering AML compliance program implementation. First, they must ensure that the issuance of a coin is not used to directly facilitate money laundering activity. Such a situation could arise if, for example, a drug dealer were to obtain a virtual asset as a payment and then exchange that asset for a stablecoin. Likewise, the bad actor could convert fiat dollars into a gift card, and use that card to purchase stablecoins directly from the issuer. In addition to implementing the Five Pillars approach discussed above, issuers must ensure that they appropriately identify the source of wealth and source of funds of the customers to whom they directly issue coins, to understand whether there is an explicable

[20] https://www.ncua.gov/newsroom/ncua-report/2017/fincen-adds-fifth-bsa-compliance-pillar
[21] https://home.treasury.gov/system/files/136/StableCoinReport_Nov1_508.pdf

means by which the funds were acquired. Secondly, They should seek to understand whether the stablecoin ecosystem that they facilitate is itself being used for bad activity. Privacy enhancing features such as coins leveraging blockchain encryption (“privacy coins”) may make a given virtual asset more likely to be used in illicit transactions. Stablecoin issuers should partner with other VASPs and financial institutions to encourage information sharing and transaction transparency where allowed by law and regulation. Only by self-policing can coin issuers hope to avoid significant regulatory intervention that may ultimately undermine the stablecoin use case.

AML for Algorithmic Stablecoins and Debt Products

DeFi lending protocol implementations and algorithmically issued stablecoins must consider AML compliance obligations related both to borrowing and lending activities and, for algorithmic stablecoins, risks related to actual use of the issued coin. Ensuring that the virtual assets being lent or borrowed are not being used to facilitate the placement of illegally derived funds into the virtual asset financial system is vital to ensuring that these DeFI protocols (and their associate VASPs) meet the recommendations outlined by FATF as implemented in their specific jurisdictions. Doing this requires the creation of compliance programs on par with those of traditional banks or money services businesses, which would represent a radical change from the current state of the industry. A peculiar challenge facing lending protocol operators is that after funds have been accepted as collateral, the delivered loan may be used without the oversight or control of the protocol or the VASP; only the posted collateral remains locked into the protocol. Protocol operators should investigate instances in which the funds used to repay a collateralized loan (whether or not such a loan is used to issue an algorithmic stablecoin) may appear suspicious or incongruent with the VASP’s knowledge of the customer.

Transaction Monitoring

Fiat world transaction monitoring is a fairly straightforward affair — specific review scenarios are created, customer activity is aggregated across various accounts and product offerings, and monitoring tools are used to generate alerts and apply risk points based on transaction activity. Such review scenarios may include suspicious values and volumes of transactions, velocity of transactions, indications of structuring, and indications of activity with prohibited counterparties — such as sanctioned persons or illegal industry participants. Though the principles remain the same within the virtual asset sector, the complexity of review scenarios and crypto-specific financial crime risks necessitate a tailored monitored and analytics program, tuned to cover DeFi protocol interactions.

Transaction Monitoring for Decentralized Exchanges

Decentralized exchanges present both obvious and nuanced use cases for transaction monitoring and analytics applications, Clearly, exchange activity between decentralized exchange platform users should be monitored to ensure that neither liquidity providers nor coin/token swappers are subject to sanctions controls, are associated with AML events, or have a nexus to terrorism or other criminal activity. The wallets of those entities or individuals engaging directly with the protocol should also be screened as industry best practice, to reduce the risk of facilitating activity with bad actors, even when a specific transaction may not itself represent the use of dirty crypto. Given that many decentralized exchanges operate with redemption coins, which are coins or tokens that represent a liquidity provider's share of virtual assets in a liquidity pool, additional transaction monitoring safeguards should be implemented to ensure that, should the redemption coin be traded to a third party, such a party is not able to extricate value from the pool when it would otherwise be subject to money laundering related controls. For instance, should a given liquidity provider have a token representing a 10% share of a pool, and then send that token to a counterparty wallet known to be associated with terrorist activity, the VASP operator of the DeFi protocol must implement controls that would prevent such a wallet from redeeming the token's liquidity pool value share.

Transaction Monitoring for Asset-backed and Algorithmic Stablecoins

Both asset backed and algorithmic stablecoin issuers must both address the scope of surveillance activity that they will seek to undertake, which may vary depending on local obligations and individual risk appetites. A given issuer may wish to conduct broad market surveillance of all coin use, while for larger issuers casting such a wide net may not be practical. At a minimum, all direct transactions with users should be monitored and transactions in support of illicit activity should be rejected and/or reported on, in the form of a Suspicious Activity Report. Given the prevalence of stablecoins with the DeFi world, as liquidity in decentralized exchange pools and issued loans from collateralized investments, particular attention should be paid to stablecoin usage on platforms that may be less likely to have fulsome compliance programs. It may be appropriate to increase customer risk scores based on interactions with such counterparties. Many stablecoin issuers may establish reliance agreements with centralized custodians or exchanges, and delegate transaction monitoring activity to such entities. Issuers should conduct an assessment of any third party service providers that they seek to engage, to ensure that all compliance requirements — including active and ongoing transaction monitoring — are appropriately addressed.

Transaction Monitoring for Algorithmic Stablecoins and Debt Products

Debt products and algorithmic stablecoins must develop transaction monitoring solutions attuned to the risks presented by both borrowers and lenders. The wallets of both the borrower and lender should be screened to ensure that no obvious connection to problematic activity exists and, if it does exist, that it is appropriately risk scored and mitigated. Furthermore, transactions related to the borrowed funds, whether they be algorithmic stablecoins or some other virtual asset, should also be monitored, to determine if the borrower is likely to be facilitating transactions with sanctioned persons, terrorist, dark markets, etc. If such bad activity is noted through the transaction monitoring process, debt protocol-associated VASPs should create mechanisms by which repayment in tainted funds are blocked or segregated and the customer is blacklisted from future lending/borrowing activity. Where possible, transactions in multiple virtual assets on the same blockchain (such as multiple ERC20 tokens) should be traced to determine if such activity is indicative of an attempt to obfuscate the movement of funds.

Closing Remarks

Supranational and national regulators globally have expressed deep concerns over financial crime compliance risks in the DeFi space. The historical regulatory recalcitrance of these protocols and their operators, and their insistence that they ought not be scoped into the definition of a VASP, is likely to cause some tumult as regulations are implemented and enforcement actions begin. DeFI sponsors/implementers/operators who are likely to be considered VASPs will be best served by getting ahead of the curve and evaluating their compliance risk model and program implementation options prior to the enactment of new regulations. As always, establishing a partnership relationship with regulators and avoiding unnecessary adversarial interaction is the best course of action.

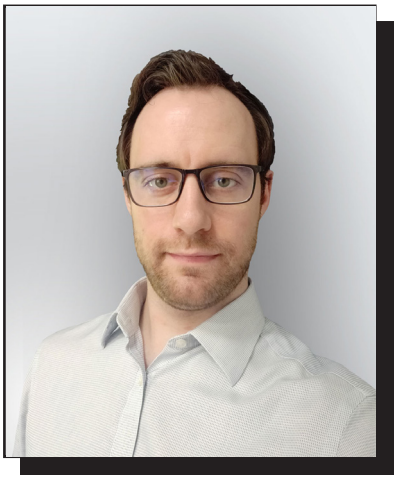
Though some may feel that mandatory compliance controls undermine the ethos of the DeFi — a name that rose to prominence due to being a homophone for “defy” — such controls are inevitable and will ultimately benefit the sector. Establishing trust and transparency while preventing isntances of child abuse, terrorism, and other odious crimes is necessary to take DeFi to the mainstream and to truly maximize the transformative potential of these technological innovations.

About the Authors

Dr. Tom Robinson

Chief Scientist & Founder

Tom is a global expert and commentator on cryptocurrency, blockchain analytics, and forensic investigations. Tom advises Elliptic's customers, regulators, and governments on cryptocurrency market developments and blockchain forensics to detect and prevent financial crime in the cryptoassets. He holds a doctorate in Physics from the University of Oxford.



Chris DePow

Senior Advisor for Financial Institution Regulation and Compliance

Chris DePow is a crypto regulatory policy expert and former bank compliance officer. Chris works with multinational financial institutions to develop crypto-specific AML policies and to integrate such policies into existing compliance frameworks. When not meeting with customers, Chris engages with regulators and law enforcement officials to help shape the future of financial crime regulation in the crypto space.

Glossary

DeFi (Decentralized Finance)

The concept of using smart contract platforms such as Ethereum to offer an alternative financial system that is open for anyone to use, and which allows financial services provided by centralized intermediaries to be replaced by decentralized applications (DApps).

DApp (Decentralized Application)

A computer application that runs on a decentralized smart contract platform such as Ethereum. In the context of DeFi, the application provides a financial service — for example lending, borrowing or exchange of cryptoassets.

Smart contract

Software code that enforces the terms of particular transactions on a smart contract platform. A DApp is typically made up of one or more smart contracts.

Smart contract platform

A decentralized system, typically based around a blockchain that allows value to be transferred according to terms specified in smart contracts, which can be created by any user. They typically incorporate a native cryptocurrency, such as Ether. Examples of smart contract platforms include Ethereum, Solana and Binance Smart Chain.

DEX (Decentralized Exchange)

A type of DApp used to exchange one cryptoasset for another. Examples include Uniswap, Sushiswap and Curve Finance.

Stablecoin

A cryptoasset with a value pegged to some other asset — for example the US dollar. Examples include Tether, USDC and Dai.

Governance token

Governance tokens are cryptocurrencies that represent voting power on a blockchain project such as a DApp. They are commonly distributed to users of a DApp, as an incentive.

Yield farming

The allocation of cryptoassets to DApps — for example committing them to DEX liquidity pools or lending DApp collateral pools — so as to maximise the returns received through the various incentive mechanisms offered by them.

About Elliptic

Elliptic is the global leader in cryptoasset risk management for crypto businesses and financial institutions worldwide. Recognized as a WEF Technology Pioneer and backed by investors including Evolution Equity Partners, SoftBank Vision Fund 2 and Wells Fargo Strategic Capital, Elliptic has assessed risk on transactions worth several trillion dollars, uncovering activities related to money laundering, terrorist fundraising, fraud, and other financial crimes. Elliptic is headquartered in London with offices in New York, Singapore, and Tokyo. To learn more, visit www.elliptic.co and follow us on LinkedIn and Twitter.

ELLIPTIC

London • Tokyo • New York • Singapore

Connect on LinkedIn

Follow us on Twitter

Contact us at hello@elliptic.co