MERKLE SCIENCE
RegWatch

Diving into DeFi

Fundamentals from the Financial Frontier

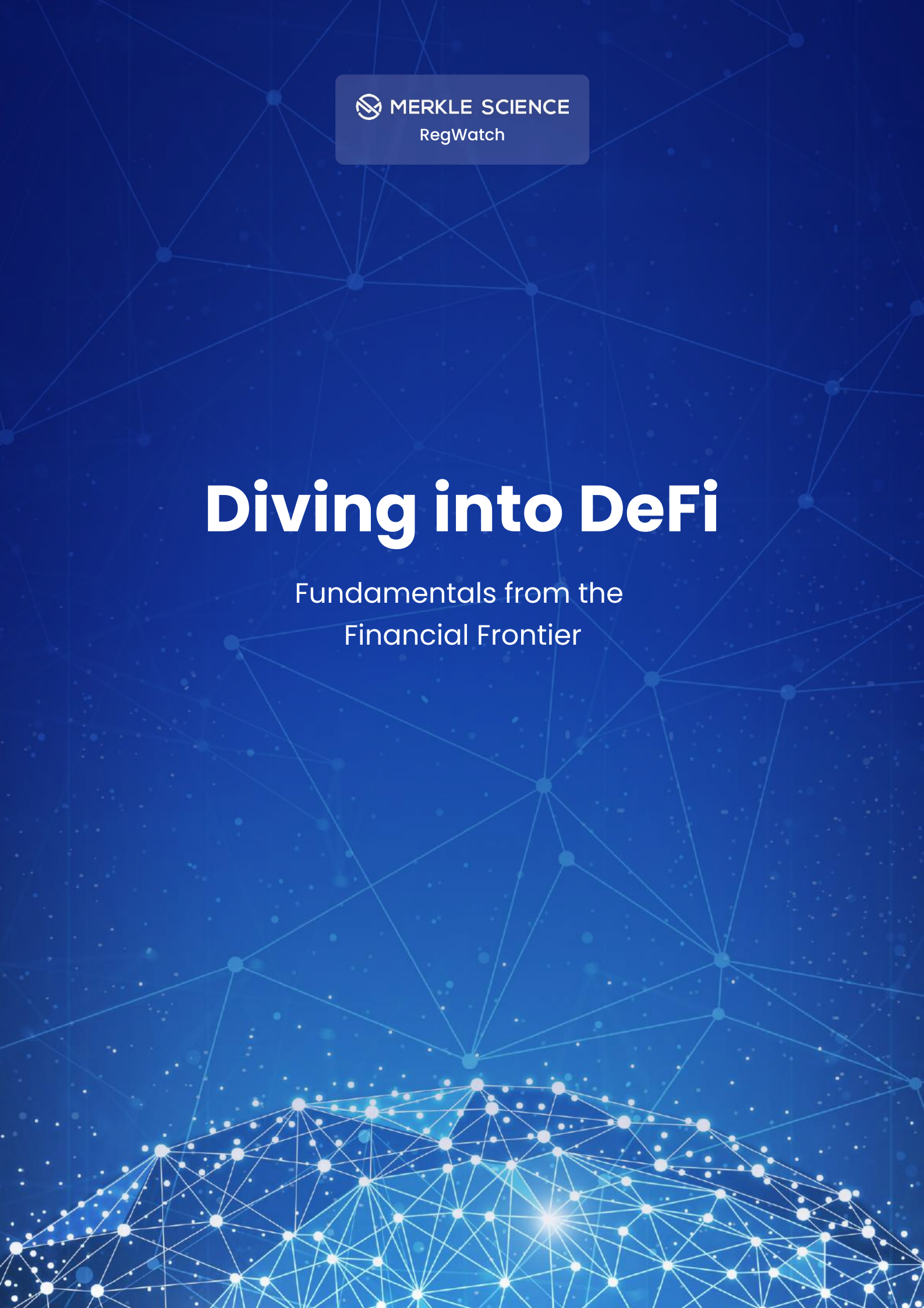


Table Of Contents

Executive Summary

For those who do not work in the cryptocurrency industry, decentralized finance is still extremely foreign. At its core, decentralized finance, or DeFi, is an extension of Satoshi Nakamoto's vision as outlined in the infamous Bitcoin whitepaper. In this whitepaper, elegantly laid out in a succinct nine pages, is the basis of a "purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution." In the 13 years since the Bitcoin whitepaper was published, an entire ecosystem has been created — and continues to evolve — that does not require centralized parties to make decisions or approve transactions.

From the surface, some products may look similar to the products and services offered within the traditional financial ecosystem — from exchanges and asset management to insurance and derivatives. However, peeking underneath the surface, the infrastructure of such products and services may look quite different in order to offset its decentralized nature. For example, automated market makers (AMMs) were created in order to solve the liquidity challenges faced by DeFi platforms. And since then, AMMs — in its myriad of formats — have become a core feature of DeFi.

In addition, completely new and innovative products have been created within the DeFi ecosystem that are completely unheard of in traditional finance. A flash loan is one such example, where a loan may be taken out without collateral with the premise that the amount borrowed will be returned before a new block on the blockchain is created. Within this time span, the borrower may use this loan for a multitude of transactions. This all happens within seconds, and it is possible all due to the fact that DeFi is programmable finance where transactions and executions happen almost instantaneously and are not hindered by third parties.

The following report is a primer of what you should know about to begin understanding the DeFi landscape, including:

- **The building blocks of the DeFi ecosystem** — what are some basic DeFi concepts?
- **The types of DeFi platforms that have emerged** — what are some of the ways in which DeFi is being utilized?
- **Emerging trends in DeFi** — what should you pay attention to?
- **Risk exposure in DeFi** — what sort of risks should individuals be aware of before engaging in DeFi?
- **DeFi vs CeFi** — what are the advantages and disadvantages of decentralized versus centralized finance?
- **Regulatory concerns** — what do we know so far about how regulators will potentially approach DeFi?

In addition, we wanted to begin taking a look at the use of DeFi platforms for illicit activity. As a jumping off point, we examined the transfer of Ether from Tornado Cash to three prominent DeFi platforms: Uniswap, Aave, and Compound. While we recognize that the use of privacy tools such as mixers are not strictly used by criminals, the prolific use of Tornado Cash in DeFi hacks warrants a closer look into fund flows from Tornado Cash into a few of the most prominent DeFi platforms.

In September 2020, the major spikes in Uniswap and Aave corresponded with the DeFi bull run as well as Aave's governance token launching in mainnet. As explained in this report, governance tokens play a significant role in the DeFi ecosystem, so a mainnet launch of a governance token would result in a spike in activity. Since January 2021, ETH transactions from Tornado Cash to each separate protocol have remained steady or decreased.

Introduction

DeFi has become a flagship use case for blockchain technology. By offering asset management, borrowing, lending, and remittance services without intermediary parties, DeFi is moving to shake up the traditional financial services industry.

What is DeFi?

Decentralized Finance (DeFi) finds its roots in the immutable blockchain network with built-in smart contracts. The convergence of blockchain technology with the realm of financial applications led to the ascent of DeFi. Throughout history, finance developed central intermediaries in order to facilitate accurate and dependable transactions. As human nature is fallible, errors and inequality still persist within a centralized financial structure. With the development of Ethereum, smart contracts were built into the blockchain — and other smart contract protocols have been created thereafter such as Binance Smart Chain, Cardano, and Polkadot and developers were able to create applications that allowed for functions to operate without any intermediaries. This included financial applications, hence decentralized finance. DeFi can be categorized as a confluence of its three pillars, namely blockchain, digital assets, and financial services.

DeFi, in theory, aspires to emerge as an alternative to the present-day financial system that replaces intermediaries with self-sufficient code embedded in the blockchain. Before diving into the evolution of DeFi and the DeFi landscape, it's important to understand some of the terms that are used in the space.

[a] Smart Contracts -The March 2021 The Draft Updated Guidance by the FATF (hereinafter referred to as The Guidance) defines smart contracts "as a computer program or a protocol that is designed to automatically execute specific actions such as Virtual Assets (VA) transfer between participants without the direct involvement of a third party when certain conditions are met."

One of the primary functions of the smart contract is to encode a set of protocols (or rules and instructions) that help complete and validate transactions. These transactions can be enforced through the application of blockchain consensus rules. Firstly, a blockchain transaction that has a designated smart contract function is submitted to a miner node on in the blockchain network who then validates this transaction and adds it to the next block, thereby changing the state of the blockchain. The miner then charges a transaction fee for adding this transaction on the block. After mining the block, the miner then transmits the new block to all other nodes on the network who then proceed to validate the block and its transactions. Subsequently the miner will then adds it to their copy of blockchain.

Ethereum is the original smart contract blockchain. It entitles the user to encode rules for the execution of DeFi transactions. It enables the creation and transformation of tokens on top of the Ethereum blockchain as payment for processing and validating transactions, also known as a gas fee. This way, smart contracts may only be executed when a predetermined set of conditions are met — only then will transactions be complete.

[b] Tokens - Tokens on smart contract blockchains are used as a mode of representation for digital assets. They may also be utilized to provide functions on the blockchain, such as the right to vote for a change on the protocol. One of the predominant functions of smart contracts is to implement tokens by adhering to the standard token interface. This allows the implementation of tokens within smart contracts and provides functionality to transfer tokens to other applications.

For instance, the ERC-20 token standard allows for the creation and deployment of an assortment of ERC-20 tokens.

[c] Liquidity Pools - DeFi applications such as decentralized exchanges (DEXs) use liquidity pools to facilitate trading. Liquidity pools in DeFi replace the traditional order book model used in Centralized Finance (CeFi), ensuring that there are sufficient assets for transactions, whether they be trading, lending, or other financial functions.

In the most basic version of the DeFi liquidity pool, two tokens are locked in a smart contract to form a trading pair. Each liquidity pool creates a new market for that particular trading pair. The first liquidity provider is required to determine the initial price of tokens in the pool.

For instance, Token A and Token B together form a trading pair and the value of 1 Token A is set in such a way that it is equal to 5000 Token B. Liquidity providers are required to contribute an equal value of both the tokens to the pool.

Accordingly, if an individual decides to deposit 5 Token A in the pool they will have to match it up with an equivalent value i.e 25,000 Token B. Subsequently when an individual wants to trade Token A for B they can directly do it against the liquidity pool based on funds deposited without the involvement of a counterparty.

To keep the liquidity providers incentivized, they are rewarded with a new type of token called LP tokens which represent their stake. Those users who want to trade in the pool by swapping token have to pay their share of the trading fee. This trading fee, however, is divided amongst all liquidity providers and their share in the fee is directly proportionate to their stake size. In order to receive their underlying liquidity back, the liquidity providers are required to burn their LP tokens. Some of the DEXs that use liquidity pools include Uniswap, SushiSwap, and Curve.

[d] Governance and Incentive - Supporters of DeFi appreciate the decentralized nature of blockchain, which, in an ideal world, moves away from the oligopolistic nature of traditional, centralized finance.

Token-based governance paves the way for further decentralization. In the abstract, DeFi would attain complete decentralized governance through the establishment of a Decentralized Autonomous Organization (DAO), the fundamental role of which would be to directly execute token votes through an automated smart contract.

A token-based incentive system would lead to further decentralization when developers give up more of their decision making power to token holders. This in turn would increase the token-holders role in decision making, which is crucial in deciding on activities such as proposed changes to protocols, defining parameters on interest rates, or collateralization ratios. Hence, the aforementioned models which are the essence of DeFi bring us closer to protocol-based democratic decision making in a transparent setting and away from a model where few potent players driven by their prejudices and monetary gains manipulate the collective benefit of the stakeholders.

DeFi Essentials

DeFi can be further broken down into functionalities of decentralized applications (dApps) that are essentially services built on the top of blockchains. Using a public blockchain like Ethereum would allow dApps to create a trustless ecosystem where transactions can be facilitated without the participation of third-party intermediaries. Additionally, all the transactions that take place on dApps are immutable — once executed, the transactions cannot be reversed as they are validated and secured on a public blockchain. Although dApps can be used to provide any kind of web services, in DeFi, the dApps are used to provide financial services such as lending or credit facilities, DEXes, derivatives, and tokenization.

Credit provision through borrowing and lending protocols is one the most important functionalities of DeFi. DApps such as DeFi lending platform facilitate peer to peer lending. Further stablecoins such as USDC and DAI are also an essential part of the DeFi ecosystem. These digital assets — pegged to a dependable fiat currency such as the US dollar — can be used by traders to log their capital gains under stable assets. Insurance protocols, which provide protection against trading risks on DeFi platforms in return for a guaranteed premium fee, and Oracles, which are connected to off-chain databases that enable smart contracts within the blockchain to receive real-world and use this off-chain to execute a transaction information, are also indispensable parts of the DeFi ecosystem. Lastly, DeFi exchanges (or DEXs) that enable users to trade with one another directly without the involvement of third parties also fall under the ambit of DeFi essentials.

[a] Decentralized Exchanges

There are two types of exchanges: centralized exchanges (CEXs) and decentralized exchanges (DEXs). Centralized exchanges require a verifiable operator to keep user funds safe, introduce buyers and sellers, regulate communication and exchange between such buyers and sellers, process, monitor and settle transactions.

In a nutshell, DEX is a peer-to-peer (P2P) marketplace that connects cryptocurrency buyers and sellers. DEXs do not require a verifiable operator; instead, transactions are processed by smart contracts against either a pool of capital or directly on a peer-to-peer basis. The purpose of DEXs is to process a non-custodial exchange of associated digital assets. The DEXs themselves do not have any ownership over the funds of the users at any point in time. They facilitate on-chain asset exchange to ensure that all the transactions are publicly verified by the network participants.

Initially, as DEXs were built upon smart contract blockchains, DEXs were limited to transactions involving only those assets which are native to their blockchain. Since then, this has been solved through wrapped tokens and novel cross chains solutions in order to overcome this limitation.

[i] Solving for Liquidity in DEXs

Different variants of DEXs include order book DEXs, batch settlements, and automated market makers (AMMs). Though the design of decentralized exchanges in terms of trade-offs around throughput, latency, security, scalability, etc. may differ, AMMs have become a popular feature used to replace the traditional order book. Through AMMs, a trader deals against on-chain liquidity pools supplied by market makers rather than the traditional order book which subjects the traders to bid/ask spread.

Relays are another popular mechanism used to solve the liquidity problem. Tools like Totle allow users to create a list of multiple tokens and then create a basket order of such tokens. Once such a basket is created these tokens

are transmitted across multiple exchanges. The user receives a new ERC-20 token instead of multiple tokens once the order for the token is settled in different exchanges.

[ii] DeFi Derivative Platforms

Still, in their nascent stages, DeFi derivative exchanges, such as dYdX and Nuo, have emerged. DeFi derivative services, unlike central exchanges, directly connect buyers to sellers without intermediaries such as swap execution facility, settlement bank or a clearinghouse. DeFi derivatives are backed by incentivised collateral pools much like other DeFi categories. In essence, they are digitized financial contracts that derive their value from the performance of associated assets.

Example: *dYdX enables the purchase of margin long and margin short notes while Nuo allows individuals to trade on leverage created by reserves loaned out by other users.*

[iii] DeFi Exchanges Case Studies

Uniswap

Uniswap is a type of decentralized exchange built on Ethereum. It takes the form of an automated liquidity protocol. Uniswap goes beyond the traditional order book architecture through the use of Constant Product Market Makers, which are a variation of Automated Market Makers (AMMs).

Uniswap, specifically, works on a constant product “rule which” helps in calculating the trading price. The formula for this is: k=x*y wherein k is the invariant which is fixed, x is the balance of Asset A and consequently Y is the balance of Asset B. The catch however is that this invariant (k)remains fixed only at a given level of liquidity. To illustrate this, let’s hypothetically consider the ETH/USDC liquidity pool. In this case, x would amount to ETH and y will represent USDC. Now, to calculate k, which is the total liquidity of the pool, it is essential to multiply x and y. In order to withdraw a certain amount of ETH, the same amount of USDC needs to be sold for k to remain constant. If user XYZ buys 1 ETH for say 500 USDC against the ETH/USDC pool, the direct consequence of this would be that the ETH portion x goes down and the USDC portion y increases, ultimately, leading to an increase in the price of ETH. Since k has to remain constant even when x portion decreases, then logically to maintain k which is the total liquidity of the pool the price of x has to go up based on how much this particular transaction alters the ratio between x and y.

As mentioned above, liquidity providers earn trading fees for providing liquidity to the pool. This process however is susceptible to the phenomenon of impermanent loss. This phenomenon can be analysed through the aforementioned ETH/USDC liquidity pool, where both ETH and USDC have equivalent values i.e the trading pair is made of 1 ETH is equivalent to 500 USDC. Say, at a given time there is a total of 5 ETH and 25,000 USDC in the pool out of which 1 ETH and 500 USDC is deposited by user XYZ, thereby giving XYZ 25% of the share in the pool. In the present case, total liquidity would be 125,000.

Should user XYZ want to convert 500 USDC to ETH, that means that the user will be putting USDC into the pool and withdrawing ETH. That would mean that the total USDC in the pool is 25,500. With k remaining constant at 125,000, that would mean that the amount of x is now 4.901. The difference, 0.099 (5 ETH - 4.901 ETH), is the amount of ETH a user can receive in exchange for tapping into the liquidity pool.

How price is calculated at the given state of the liquidity pool

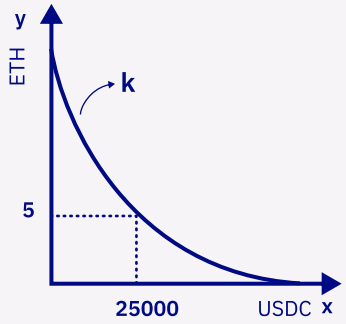
Initial Base: 1ETH = 5,000 USDC

Step 1 : ETH/USDC Pool is made up of 5 ETH (x) and 2,500 USDC (y)

k = x * y

k = 5 ETH * 25,000 USDC

k = 125,000



k = Uniswap invariant

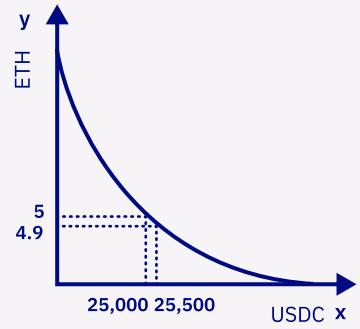
Price Cover [x*y] = k = 125,000

Step 2 : User XYZ wants to convert 500 USDC to ETH

Current USDC in the pool = 25,000 ; USDC to be added = 500

Total USDC in the pool = 25,000 + 500 = 25,500

k is the invariant and remains constant



k = 125,000 (constant)

Step 3 : New total USDC = y = 25,500 (from Step 2)

k = x * y

125,000 = x * 25,500

x = k/y ; x = 125,000/25,500 = 4.901

x = 4.901 = Total ETH

ETH (Step 1) - ETH (Step 3)

= 5 - 4.901 = 0.099ETH

User XYZ exchanges 500 USDC for 0.099 ETH

SushiSwap

SushiSwap, like Uniswap, facilitates the trading of cryptocurrencies by users against its liquidity pool. SushiSwap differentiates itself from other traditional exchanges as it does not rely on market makers. Instead, SushiSwap allows its users to provide liquidity to the platform.

Users looking to become liquidity providers can connect their Ethereum wallets to SushiSwap accounts. Like Uniswap, the users intending to provide liquidity to this platform will have to lock an equivalent amount of the two selected assets to the pool in a 1:1 ratio and calculate the value of one asset against another through the Swap function while providing liquidity. For instance, if user X wants to deposit 5 ETH to the Sushi/ETH pool he will first have to use the swap function to calculate the value of ETH against Sushi. If user X wants to provide liquidity to the trading pairs which are yet to manifest themselves in practice (trading pairs that don't exist at the point in time), then user X will just have to add the selected cryptocurrencies into the new pool created for that purpose. User X now becomes the first liquidity provider and can set the initial price/exchange ratio. However, as more users add to the pool this ratio will alter due to arbitrage and correct itself.

There are several features on SushiSwap that set it apart from Uniswap, the first of which is an innovative feature known as Sushi Bar. Here, the users stake their Sushi Token and in return earn Sushi rewards. A trading fee is charged for each transaction that takes place on the platform. The trading fee here is 0.3% which is further bifurcated into two parts: the first part, which is 0.25%, is given to the liquidity providers and the second part, which is the remaining 0.05%, is converted into pool token and is added back to the Sushi Bar. The pool tokens are subsequently liquidated for the purpose of purchasing Sushi Tokens and are distributed amongst the users staking Sushi Tokens. Unlike Uniswap, Sushi Token holders are entitled to a certain portion of the fee even after they have stopped providing liquidity.

Onsen is another feature that makes SushiSwap unique. Previously, yield farmers would constantly navigate between platforms in search of the most profitable pool. Due to the volatility of the cryptocurrency prices, the profitability of the pools was frequently changing. Therefore, the concept of 'Menu of the Week' was introduced on SushiSwap, whereby the governance participants, who are incentivized to ensure profitability and variety in terms of token offering, would vote on which liquidity pools to feature every week. Onsen is the next generation of this feature that showcases more pairs on the platform for longer periods of time. Liquidity pools on Onsen last for 60 days and may feature as high as 58 pairs.

Another feature is BentoBox, which essentially works as a decentralized app store where users can deposit assets to enable multiple dApps built within BentoBox. dApps that are built within BentoBox can save users on network wallet fees and can algorithmically generate yields for depositors. Kashi was the first dApps built on BentoBox for lending, borrowing, and 'one-click leverage' trading transactions..

Balancer

Similar to Uniswap, Balancer uses an AMM that automatically maintains supply and demand through ratios. What differentiates Balancer, however, is the use of three kinds of pools: a) shared, b) private, and c) smart pools.

- Shared pools are public pools whereby anyone who wants to participate as a liquidity provider may do so. Once created, the parameters of a shared pool — the types of tokens, the ratio of the tokens, and the fees — are fixed.
- Private pools, unlike shared pools, have variable parameters that may be changed anytime by a pool's owner. In addition, the owner of a private pool is the only individual who may contribute liquidity to the pool.
- Smart pools combine features from both shared pools and private pools. Shared pools allow for open access for liquidity providers, but the pool's parameters remain flexible. Smart pools allow for conditional investing strategies that can be encoded into a Balancer smart pool akin to an active investment portfolio.

Balancer users can create the liquidity pools themselves, allowing them to choose upto eight compositions of ERC-20 tokens and set their own trading fee structure which may range from 0.0001% to 10%.

The Balancer token (BAL) can be used for controlling and incentivizing the platform. Akin to the Compound token

(COMP), the Balancer token also does not have any economic value; it is merely a governance token. The users can use BAL on the Balancer voting platforms to cast votes for tasks such as validating/invalidating improvements to protocols.

[b] Lending & Borrowing

Decentralized lending platforms allow for P2P lending and borrowing of crypto assets without centralized intermediaries. Unlike the centralized platforms, users of decentralized loan platforms do not have to go through KYC processes. Lenders in the DeFi platform enlist their tokens on a specific money market and receive interest on such tokens facilitated by the lending protocol.

Much like the traditional financial system, debt markets in DeFi facilitate lending and borrowing of associated on-chain assets. However, DeFi uses protocols for loanable funds (PLFs), which uses smart contract code to replace an intermediary to facilitate the loanable funds. Lenders look for primarily two things when choosing a DeFi lending platform: first, a platform that provides a high-interest rate; and second, where the interest can be settled with a currency such as ETH, USDT, or US dollars.

[i] Calculation of Interest Returns

The amount of interest earned on each lending platform depends on each platform's methodology used to set its interest rate. In general, the interest rate mechanisms within each platform are used to equilibrate the supply and demand of funds on the platform.

The deposited funds are pooled in smart contracts to ensure that funds of crypto assets are available for the provision of loans when the need arises. The size of the debt market can be calculated through an amalgamation of total borrowed and total supplied amount of tokens. The liquidity of the debt market can therefore be viewed in terms of deposits available i.e available non borrowed tokens.

The DeFi lending platform's underlying model shapes the cost of borrowing by determining the interest rate to be paid by the borrower. In any particular market, the rate to borrow an asset should be higher than the rate owed to the lender. The interest rate on any given platform may change drastically, depending on the platform's supply annual percentage yield (APY). This means that borrowers' interest amount may change drastically — over the course of borrowing period of a transaction — in line with the change in lending and borrowing demand of the specific token taken by the borrower.

[ii] Restrictions on Borrowing

Primarily, there are two considerations governing the cap placed on the amount that an individual can borrow.

First, the collateral factor of the tokens supplied by the borrower. The collateral factor refers to the quality of the borrower's collateral in relation to the total amount to be borrowed. Essentially, the maximum amount that the borrowers can take is limited by the collateral factor of the asset they have supplied — the higher the quality of the asset, the greater the borrowing limit. For instance, if borrower A supplies 300 DAI and in turn, possesses a collateral factor of 75% on the chosen DeFi lending platform, then the borrower can take a loan of up to 75% DAI worth of other assets such as ETH or the platform's native token.

Second, if a borrower is looking to borrow a large volume of a specific token, the amount he may borrow may be restricted by the total fund pool — in other words, how liquid the pool is — of that token available in the given market.

[iii] Repayment of Loans

To ensure that the loan amount is repaid to the lender, DeFi platforms have adopted two primary approaches (a) Flash Loans and (b) Collateralized Debt Positions:

- ***Flash Loans*** - A flash loan is a loan that is made and returned within the timeframe it takes to create a new block on the blockchain. It is a loan that doesn't require the borrower to put down any collateral. The borrower will quickly flip a profit on the amount and return the initial loan before a new block is formed.

  To protect the interest of lenders, there are two mechanisms put in place. Firstly, the immediate repayment of the loan. Under this approach, users request the funds, receive, utilize and finally repay them with the requisite interest all within the same blockchain transactions. In case the borrower fails to repay the loan amount inclusive of interest, the whole transaction gets negated and the original loan is

reverted back to the lender.

- ***Collateralized Debt Positions*** – Collateralized Debt Positions (CDPs) are a type of financial product created by MakerDAO. It is when the complete loan amount can be secured by using collateral assets. Users can get loans quickly and in case the market tumbles, the collateralized asset can be liquidated swiftly to ensure solvency. The collateral itself is locked within the smart contract and once the full debt amount is repaid the collateral is released.

  Oftentimes, as DeFi does not use credit scores nor does it require any formal identification, DeFi lending applications will require over-collateralization in order to protect the lender. A collateralization ratio indicates how much a loan must be collateralized; a collateralization ratio over 1 (or 100%) means that the loan must be over-collateralized.

[iv] DeFi Lending Case Studies

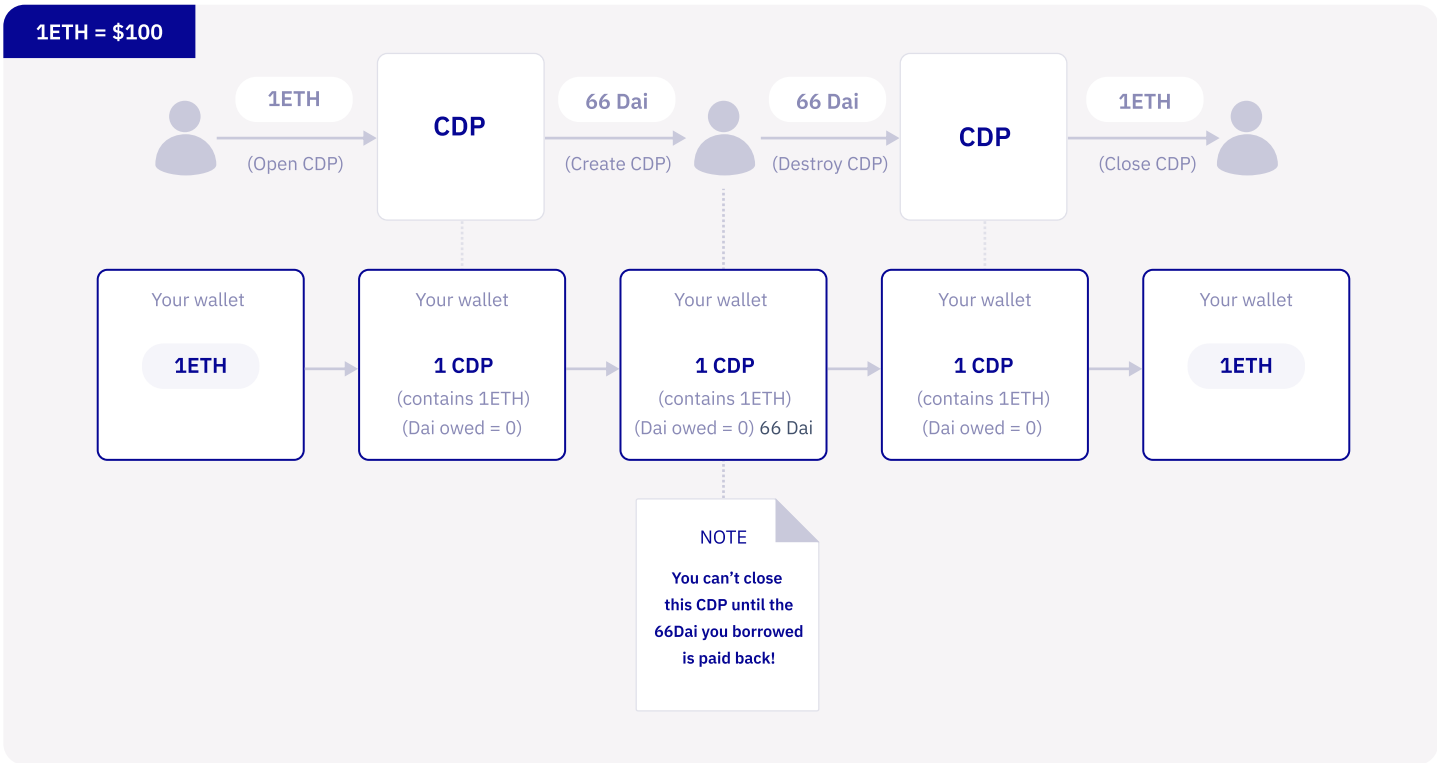
MakerDAO

MakerDAO, a decentralized autonomous organization, is considered to be the paragon of the DeFi ecosystem and specializes in creating DeFi products and services, one of which is the aforementioned Collateralized Debt Position. MakerDAO is a two-token system (MKR and DAI), one of which is a USD-pegged stablecoin (DAI). The DAI plays a key role in CDPs, as detailed below. The MKR token is the second type of token on MakerDAO and is the governance token, giving its holders the right to participate in the democratic decision-making mechanism. Holders of MKR, for instance, have the right to vote on decisions including but not limited to authorizing protocol updates such as validating new collateral types for vault, tweaking the parameters such as collateralization ratios, and approving upgrades to increase functionality. The platform employs incentive techniques to ensure good governance.

How a CDP works on MakerDAO

To own a CDP on MakerDAO, the borrower must deposit collateral, or margin as per traditional finance, in the form of ETH or whatever asset the platform will accept as collateral. Once deposited, DAI is generated (pegged 1:1 to USD). In order to figure out the maximum amount of DAI that may be generated by the collateral deposit, one must divide the total value of the collateral by the CDP's minimum collateralization ratio.

Example: *CDP's minimal collateralization ratio is 150% aka 1.50*
Sample price of ETH value: ***$100***
Amount of ETH deposited: ***1 ETH***
The maximum amount of DAI that may be generated from the deposit:
$100/1.50 = 66.7 DAI



An Overview Of How The CDP System Works (Source)

Should the price of ETH rise to $200, then an additional 66 DAI (132 DAI in total) may be generated, increasing the debt amount. In the case of a bear market, borrowers need to pay their debts in order to maintain the 150% collateralization ratio. Should the collateralization fall below the target ratio, the borrower may be liquidated.

During this time, the borrower can utilize the borrowed amount in any way that it deems fit. For example, he can exchange the DAI generated for cash or can use it as leverage to accumulate more collateral assets. The borrower must then repay the debt along with the accrued interest to satisfy the CDP.

Margin Calls and Liquidations

Unlike its traditional financial counterpart, margin calls on CDPs lack a grace period and an opportunity to post additional collateral (or margin). This may lead to immediate liquidation. Therefore, it would be wise to set a buffer amount before minting.

However, to avoid a margin call, the user can deposit more collateral into the vault till his position once again falls under the collateralized ratio. However, if this does not happen, the Maker Protocol has a system that stabilizes the value of DAI through the use of Auctions and Keepers. Auctions handle the liquidations of CDPs. Keepers are (usually automated) independent actors and in such scenarios of CDP liquidation, will sell some of the collateral, liquidate the user's position and close the debt.

Liquity

Liquity protocol is a decentralized borrowing protocol that offers interest-free collateralized borrowing and lending, using ETH as collateral. Similar to MakerDAO, Liquity has a USD-pegged stablecoin called the LUSD and all loans are paid out in LUSD. The minimum collateralized ratio on Liquity is 110% or 1.10. Users pay a one-off borrowing fee on Liquity.

Aside from LUSD, Liquity also has a Liquity token (LQTY). But unlike MakerDAO's MKR, LQTY is not a governance token. Instead, LQTY is more likened to a LP token mentioned in DEX liquidity pools, whereby LQTY tokens represent stakes of LUSD in their stability pool and stakers are rewarded a portion of the borrowing and redemption.

To borrow on Liquity, you must open a Trove, which is linked to an Ethereum address and where your loan is maintained. A minimum debt of 2,000 LUSD — and therefore its corresponding amount of ETH deposited into the Trove based on price and the collateralized ratio of 110% — is required to participate on the platform. Troves maintain two balances: one is an asset (ETH) acting as collateral and the other is a debt denominated in LUSD. It is important to note that LUSD is paid at the time of borrowing while ETH is paid during redemption. Users can change the amount of each by adding collateral or repaying debt. As they make these balance changes, users' Trove collateral ratio changes accordingly. Every time LUSD is withdrawn from the Trove, a one-off borrowing fee is charged.

Liquity protocol is more capital efficient than other borrowing systems as less collateral is needed for the same loan amount. The protocol charges one-time borrowing and redemption fees that algorithmically adjust based on the last redemption time. As more redemptions are happening (which means LUSD is likely trading at less than 1 USD), the borrowing fee would continue to increase, discouraging borrowing.

As mentioned, every time LUSD is withdrawn from Trove, a one-off borrowing fee is charged on the drawn amount and added to your debt. The borrowing fee is variable and determined algorithmically, with a minimum value of 0.5% under normal operation. The fee is 0% during Recovery Mode, which is when the Total Collateral Ratio (whereby the sum of the collateral of all Troves is expressed in USD, divided by the debt of all Troves expressed in LUSD) falls below 150%. Loans issued by the protocol do not have a repayment schedule. Users may leave their Troves open and repay their debts any time, as long as a collateral ratio of at least 110% is maintained. The collateral ratio of the user's Trove may fluctuate over time as the price of Ether changes

Compound

Compound is a lending market that offers several different ERC-20 assets — such as ETH, BAT, or DAI — for borrowing and lending. All the tokens in a single market are pooled together so every lender earns the same variable rate and every borrower pays the same variable rate. For this reason, all loans are overcollateralized in a collateral asset different from the one being borrowed. If a borrower's loan amount falls below the market's

collateralization ratio, their position is liquidated to pay back their debt. The debt can be liquidated by a keeper, similar to the process used in MakerDAO vaults and the keeper receives a bonus incentive for each unit of debt they closeout

When borrowing, a collateral factor of zero means an asset cannot be used as collateral. The amount of collateral required for a loan is calculated by dividing 100 by the collateral factor. Volatile assets generally have lower collateral factors, which results in a greater risk of under collateralization (and therefore liquidation) when there are sudden price movements. An account may use multiple collateral types at once, in which case the collateralization ratio is calculated by dividing 100 by the weighted average of the collateral types. For example, suppose an investor deposits 100 DAI with a collateral factor of 90. This transaction alone corresponds to a required collateralization ratio of 111% (100/90 = 111%). Assuming 1 DAI = $1, the investor can borrow up to $90 worth of any other asset from Compound. Should she borrow the maximum, and the price of the borrowed asset increases at all, the position is automatically subject to liquidation as the loan will be under-collateralized. Suppose she also deposits two ETH with a collateral factor of 60 and ETH is priced at $200. The total supply balance is now $500 ($100 in DAI and 2*$200 in ETH), with 80% being ETH and 20% being DAI. The required collateralization ratio is 100/(0.8*60 + 0.2*90) = 151%.

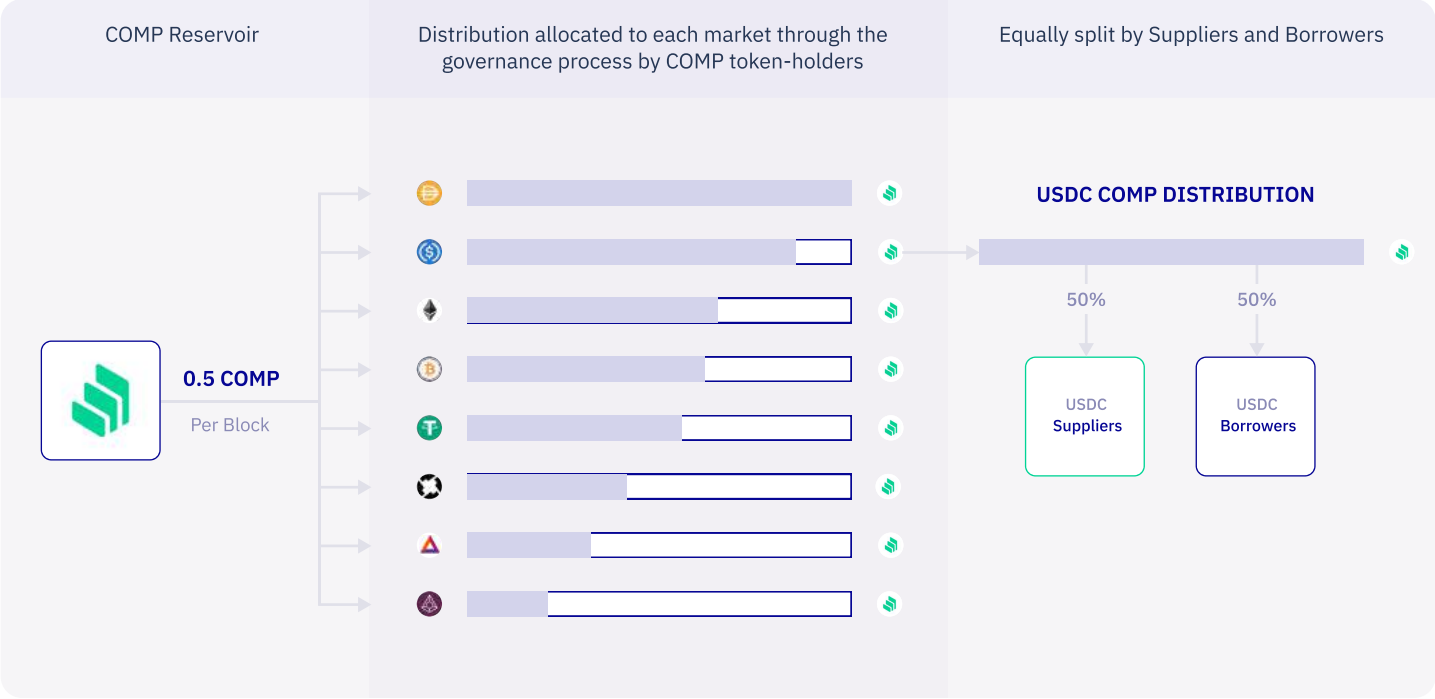
Governance in Compound

COMP is the governance token of the Compound protocol and a predetermined amount is distributed to all lenders and borrowers on the Compound protocol every day. COMP distributions happen every time an Ethereum block is mined (every 15 seconds) in an amount proportional to the interest accrued by each asset. Governance of Compound through the COMP token aims to remove a significant, centralized, single point of failure. With every COMP token representing one vote, anyone who owns at least 1% of the total COMP supply can submit and vote on proposals to change the protocol. The proposals are executable code that is subject to a three-day voting period. If a governance change to the protocol is passed by the community, it will take effect two days later giving anyone a chance to close any open positions before the changes go into effect. In this way, Compound is an entirely self-governed blockchain.

[c] Yield Aggregators

Yield aggregators allow users and depositors of DeFi protocols to earn yields through a concept known as yield farming. Yield aggregators leverage the different DeFi protocols and strategies in order to maximize profits, usually requiring users to lend, provide liquidity, or stake funds.

Yield farming began when Compound launched its governance token COMP, which was distributed to its



COMP Distribution To Suppliers And Borrowers

users in an automated manner. This was novel in the sense that both borrowers and lenders on Compound were able to earn COMP every week. As more users started using Compound and more deposits in the protocol rose, it became more difficult to farm COMP tokens and the value of the COMP governance token also increased in parallel.

In the case of Compound, users may deposit a token, borrow against it, swap for the original deposit token, and re-deposit it. This cyclical nature of the Compound platform allows users to deposit and borrow multiple times in order to maximize its farming rate using the COMP token.
Yield farming is not limited to Compound. Other protocols such as Balancer, Curve, and SushiSwap also have governance distributions that allow for yield farming. And with multiple protocols distributing governance tokens in such a way, yield aggregators were created in order to optimize for yields across multiple protocols in order to find the highest yield.

[i] Yield Aggregator Case Study

Yearn.Finance
Yearn.Finance automates yield-maximizing profit switching opportunities for liquidity providers and yield farmers. Yearn's governance token is YFI. Yearn's creator, Andre Cronje, infamously did not set any YFI aside for himself; instead, he gave them all to those who deposited in certain key liquidity pools that had a significant impact on the project. There are only 30,000 YFI and all have been distributed, which means that in order to get YFI, users must buy them off the market. YFI holders have to stake their YFI in order to participate in governance. Once a vote is cast, the token is frozen for three days and the YFI holder will earn a small fee for voting, likened to a dividend.

Yearn.Finance's core products include:

- **Vaults:** yVaults essentially act like robo advisors for users who deposit crypto assets. Once the crypto assets are deposited, they are then invested in a number of investment strategies that seek out the highest yield available in DeFi.

  By depositing into the vaults, users receive yVault Tokens , which act as deposit receipts and represent a user's share of the yVault that they are participating in. Should the yVault generate a profit, the share price of the yVault tokens will increase. Once a user withdraws their liquidity from the vault, the yVault Token will be burned.

Earn: Earn is a lending aggregator and Yearn.Finance's first product. Funds deposited in Earn are shifted between dYdX, Aave, and Compound automatically as interest rates change between the protocols. Users can deposit to these lending aggregator smart contracts via Yield.Finance's Earn page.

Example: *a user can deposit DAI into the Earn yDAI pool. Yearn will programmatically deposit DAI into one of three lending protocols (Aave, dYdX, Compound). Yearn will withdraw from one protocol and deposit to another automatically as interest rates change between protocols. As a result, the user will receive the optimal interest rate on his or her DAI deposit at all times.*

[d] Insurance Pools

Insurance policies for DeFi cover losses from theft to smart contract issues. Like in traditional finance, DeFi coverage platforms are based on pooling, transfer, and share of risk. Insurance pools manage risk by trading the payment of a guaranteed small premium for the possibility of collecting a large payout in the event of a covered scenario. In DeFi insurance, decentralized transactional and governance systems are used to manage and structure the insurance life cycle for certain types of risks such as smart contract hacks. Though technically insurance contracts are derivatives – they pay out based on some external event – insurance plays a distinctive risk-hedging function in markets by spreading risks across a common capital pool.

When a user requests a payout, they send a claim to the designated assessors governing the DeFi coverage protocol. These assessors could be members of a DAO, multisig, or a centralized resolver. The assessors then follow the steps required to validate the claim. If approved, the smart contract will issue payment to the claimant, or an approved interested party on behalf of the claimant.

[i] Insurance Pool Case Study

Nexus Mutual

Nexus Mutual is an Ethereum-based decentralized insurance platform that is made up of a risk-sharing pool governed by members with NXM tokens as membership rights. Nexus Mutual offers insurance policies that are managed and financed by the members of Nexus Mutual community. Nexus Mutual allows members to buy insurance on Ethereum smart contracts (its first product called Smart Contract Cover) on its platform, which protects smart contracts used on multiple decentralized finance (DeFi) platforms from smart contract vulnerabilities and discards the need for a middle man and middleman fees during transactions.

Nexus Mutual is organized as a decentralized autonomous organisation (DAO) with members owning 100% of the company. On the Nexus Mutual network, the NXM token is used to maintain membership, provide rewards, and hold governance voting rights.

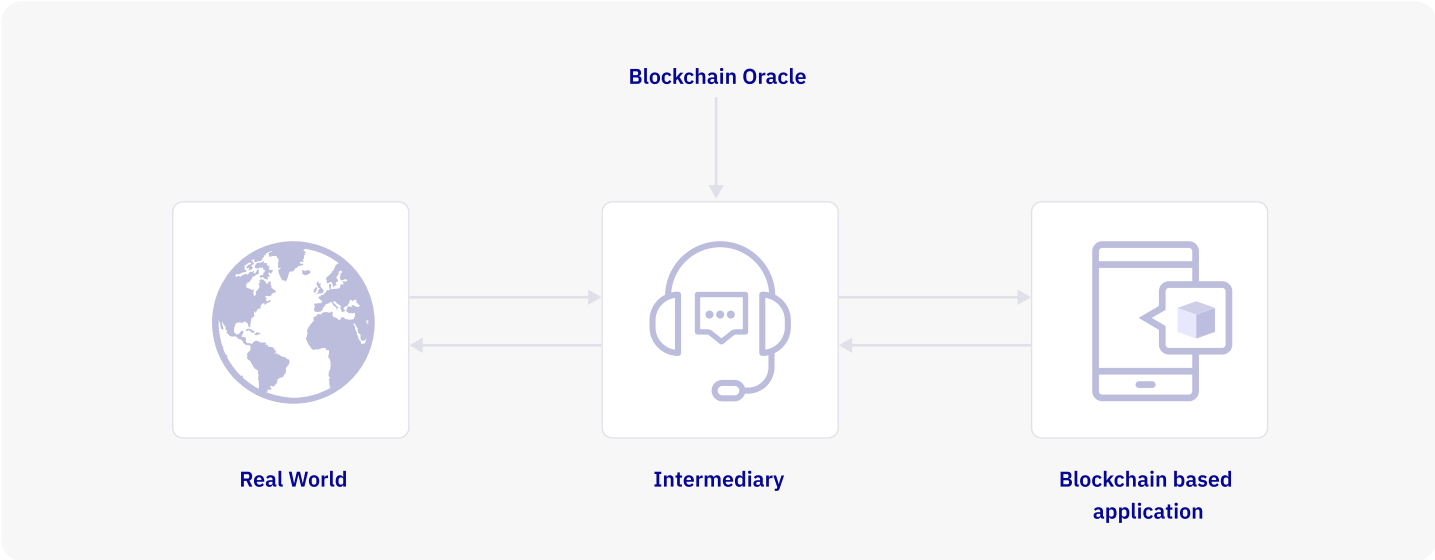
[e] Oracles

Smart contracts are often limited by the data within their own blockchain ecosystem. Oracles are third-party services looking to solve this problem and allow blockchains to receive external data.

Oracles are data sources acting as bridges between DeFi applications and external information. Most DeFi platforms either have their own oracles or attach themselves to an existing oracle from a well-reputed platform. Oracles act as a data source that can be fed into a smart contract, which enables them to access real-time data that isn't on the blockchain such as the real-time price of assets. Even though oracles themselves aren't data sources, they are layers that verify on-chain data related to real-world events and then submit the cumulative data to smart contracts.

Oracles come in two forms: centralized and decentralized. The issue when it comes to centralized oracles because there is only one node in charge, is that there is a single point of failure. Consequently, the smart contract becomes less secure and more prone to being corrupted and attacked by bad data supplied into it. Decentralized oracles, on the other hand, rely on multiple external sources to increase the credibility of the data provided to the smart contracts. Decentralized oracles work on the Schelling points game theory in which all participants provide data without colluding with one another, and the Schelling game determines whether the consensus data point or amendments proposed to the software are valid and acceptable, after filtering for any inaccuracies.

According to a study conducted by the Duke University and National Bureau of Economic Research, there are three types of oracle solutions introduced, developed, and used to date. First is the aforementioned Schelling-point oracle, where owners of a fixed-supply token vote on the outcome of an event or report the price of an asset in this oracle. Augur and UMA are examples of this type of oracle. While Schelling-point oracles maintain the decentralization of protocols that rely on them, they have long resolution times. The second oracle solution is the API oracle. These oracles are centralized entities that reply to data or price requests asynchronously — Provable, Oraclize, and Chainlink are some examples. All systems that rely on API-based oracles must trust the data provider to answer all requests correctly. Last but



not least is the tailored, application-specific oracle service. MakerDAO and Compound both employ this form of oracle. Its design varies depending on the protocol needs for which it was created. To send all on-chain price data to the Compound oracle, for example, Compound relies on a single data provider that the Compound team controls all on-chain price data to compound oracle.

[i] Oracle Case Study

Chainlink

Smart contract platforms, such as Ethereum, lack the ability to connect smart contracts to off-chain resources such as the web. Chainlink intends to address this problem by functioning as a decentralized oracle network that connects on-chain smart contracts to the off-chain world. It does so by providing smart contract APIs that allow users to request off-chain resources like market data, bank payments, retail payments, back-end systems, event data, and web content. Chainlink consists of a network of multiple decentralized, and independent oracles and aggregators that collect and process off-chain data and deliver it (processed) to smart contracts on request. AmpleForth and Synthetix are examples of platforms that are integrated with Chainlink.

In September 2020, Synthetix, a software that allows users to mint and trade new crypto assets that mimic both real-world assets and crypto assets, announced that all Synths now use Chainlink oracles for price determination, including price feeds for all cryptocurrency and index Synths. As a result, traders on Synthetix.Exchange are trading on the most up-to-date market prices.

Trends In DeFi

DeFi has dominated the conversation in the crypto industry for the greater part of 2020 and through 2021, capturing the attention of the broader financial ecosystem. Since hitting its peak in May 2021, total value locked (TVL) in DeFi platforms has decreased in correlation with the wider crypto market, the amount of investment and utilization in DeFi is still significantly higher than they were a year ago. In the meantime, new products and platforms continue to emerge and gain momentum as emerging startups and firms look to capitalize on DeFi's robust demand. Within DeFi, there are several areas that Merkle Science is keeping an eye on.

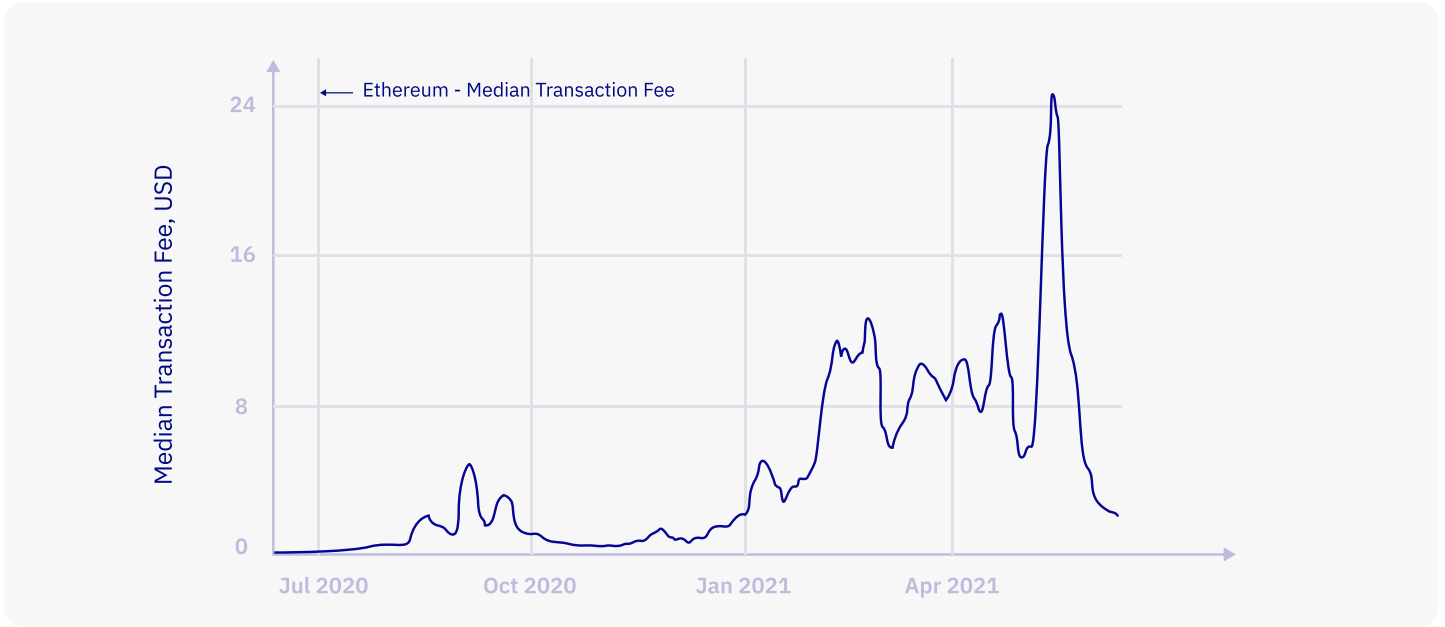
[a] Cross-Chain Technology Hopes To Solve Scalability Issues

Scalability has been one of the three central challenges in blockchain since its inception. With the growth of DeFi — and more dApps being built and utilized as a result — it has become more urgent than ever to find tangible solutions in this area.

Networks like Polkadot, which allow for the cross-blockchain transfer of token data and other assets, not only allow DeFi platforms to scale in a much simpler and efficient manner than on Ethereum, but also increase the efficiency of transactions by distributing them across multiple parallel blockchain platforms. Equilibrium is one such DeFi project. Originally built as a MakerDAO analogue on the EOS blockchain, Equilibrium announced its plans to develop a new interoperable protocol on Polkadot in parallel to the one on EOS. Central to this transition is interoperability across parallel blockchains including Ethereum, which will also allow for Equilibrium to expand its suite of products wherein users can lend, stake, trade assets, and create smart contracts across the network.

[b] Growing DeFi Beyond Ethereum

One of the challenges hindering the rise of DeFi is the increasing transaction costs due to the increase in the Ethereum gas fee. While Ethereum still dominates as the



7-Day Moving Average Of Ethereum Transaction Fees (Source)

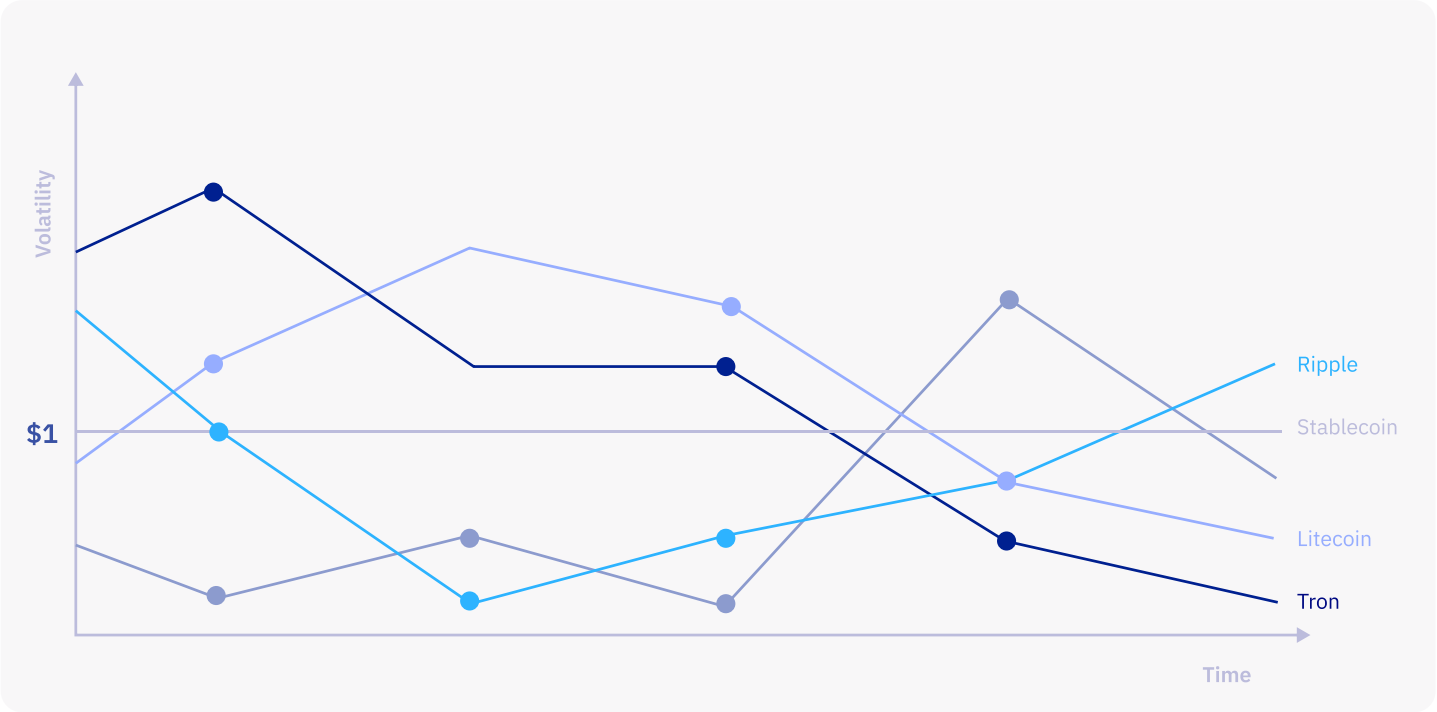
leading DeFi platform, there has been an expansion of DeFi, non-fungible tokens (NFTs), and gaming dApps onto other chains such as Polygon and Binance Smart Chain since the beginning of 2021, enforcing the narrative of the multichain paradigm.

[c] The Role of Stablecoins Continues to Evolve & Expand

Stablecoins play an outsized role in the world of DeFi as cryptocurrencies such as Bitcoin fluctuate too much — and therefore subject to drastic inflation or deflation — to be a practical medium of exchange.

While stablecoins have been used extensively with trading and transferring across centralized exchanges, in DeFi, stablecoins have become a cornerstone of the ecosystem. Rather than being dependent on fiat currencies, crypto natives are leveraging stablecoins when exiting risk positions. In Glassnode's overview of stablecoins in DeFi, there are a number of demand drivers behind their continued growth, including:

- Flight to stability from volatility and risk exposure without using native currency



The Price Of Stablecoin Does Not Change Over Time, While It Does For Other Cryptocurrencies (Source)

Total Value Locked In Stablecoins Between July 2020 And March 2021 (Source)

- Moving assets across centralized exchanges without holding risk
- Collateral for borrow and leverage
- Use in decentralized lending, exchanging, derivatives, etc. - using stables removes the risk of exposure to volatile tokens, but is usually associated with lower returns because of lower risk
- Payments, salaries, forex, 3rd world access to non-hyperinflationary currencies, and other niche consumer use-cases

Two diverse streams of secure tokens will emerge in the future. Collaborations between exchanges, such as Terra, will contribute towards one stream. The primary goal of these tokens would be to provide traders with a secure alternative to banking services and a safeguard against their loss. Digitally native tokens with built-in security will cut out fees from middlemen such as banks and foreign exchanges. Groundhog is already working towards the creation of subscription layers to administer and support such payment systems.

[d] The Gamification of Crypto

2021 has witnessed (and continues to witness) the rise of several sub-sectors within DeFi — one of which is gaming and the gamification of crypto, meaning that Non Fungible Tokens (NFTs) will play a more crucial role in the DeFi ecosystem.

New users may venture into the DeFi ecosystem due to the development of in-browser wallets, examples of the same include Opera and Brave. These wallets are set to dole out the usage of NFTsin consumer applications. Consumer applications such as gaming will invite in-game asset tradings facilitated by browser-based wallets.

DeFi will further assist in the monetization of blockchain gaming, this will be done through the development and implementation of those DeFi protocols that pave the way for in-game transferability of assets. BitSport, Ubisoft, Axie Infinity, F1 Delta Time and Cryptokitties are a step forward in this direction.

[e] Self-Regulation & Governance Increases in Importance

Currently, digital asset regulations have been adapted from traditional finance regulations for the most part. However, DeFi is forcing regulators to reevaluate approaches and frameworks, especially when it comes to flagging for and preventing illicit activity. DeFi will usher in new governance structures combining aspects of on-chain governance, decentralized ownership, and flexible regulatory regimes.

Due to its programmable nature, DeFi has a propensity toward the fast-paced creation of new financial instruments and services, paving way for new risks caused by unanticipated interactions. Conversations between the DeFi ecosystem and regulators have ramped up their efforts to preserve DeFi's open nature while protecting investors. This may come in the form of dApps that may help solve this problem, giving users control over the types of personal information being shared in order to comply with regulations.

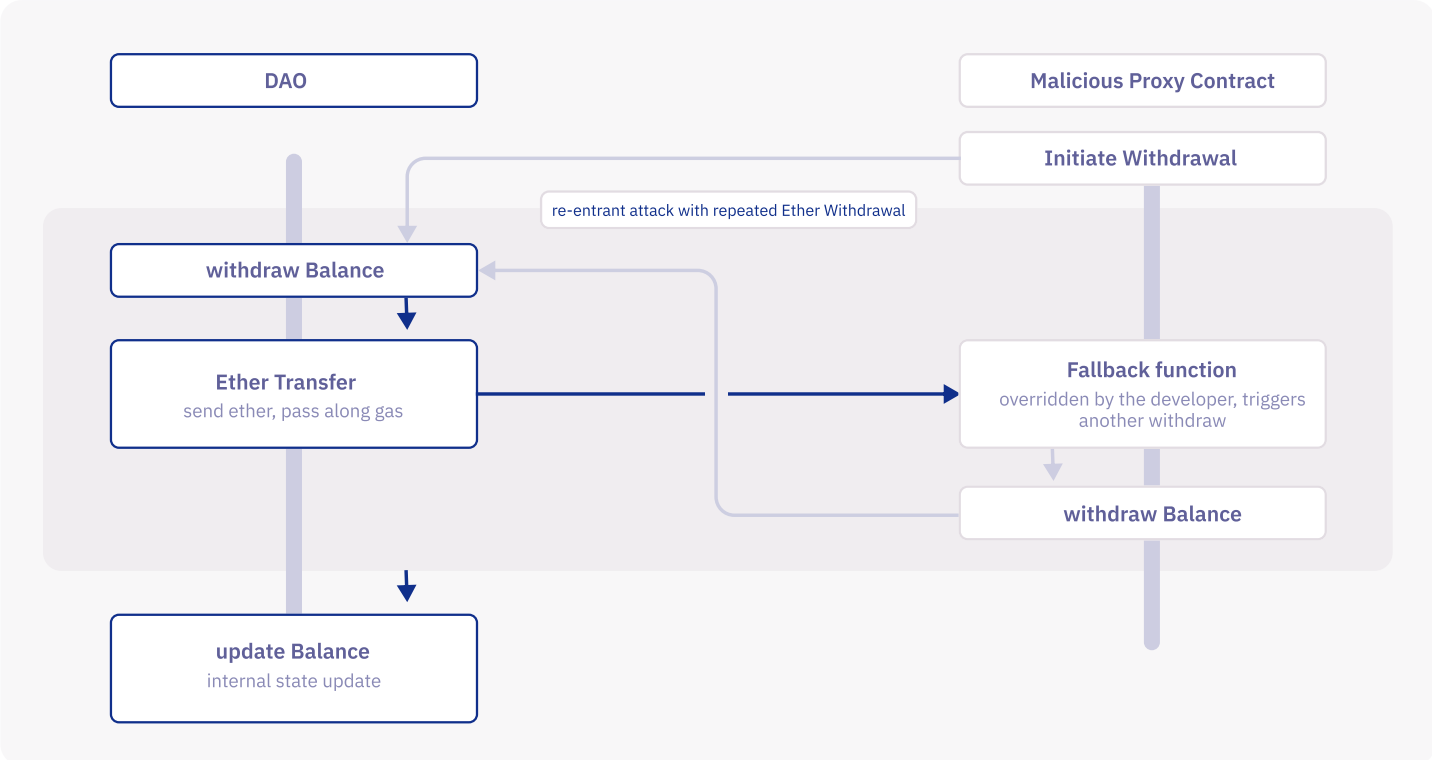
Risks

DeFi enables developers to construct new types of financial products and services, thereby broadening the scope of financial technology. While DeFi can remove some counterparty risks by eliminating intermediaries and make room for the trustless exchange of financial assets, it also — like with any nouveau technologies — introduces new hazards. Crypto businesses must efficiently tackle these risks in order to provide customers with a reliable and fault-tolerant system capable of handling these new financial applications at scale. The following highlights the top areas of concern individuals and businesses should be aware of when engaging with the DeFi ecosystem.

[i] Smart Contract Risk

Crypto-based platforms, especially exchanges, have been regularly exploited over the last decade. While many of these attacks were the result of inadequate security practices, they nevertheless highlight an essential point: software is particularly vulnerable to attacks and developer errors. Public blockchains, as previously said, are open platforms. Following the deployment of code on a blockchain, anyone can access and interact with it. As this code is responsible for keeping and moving financial assets on DeFi platforms, it poses a new and distinct type of risk. Smart contract risk is the name given to this new attack vector.

Logic errors in a smart contract take place when a developer writes code that makes smart contracts susceptible to attacks, such a software bug. An example of this are reentrancy attacks, which is when an execution can be interrupted in the middle, re-entered, and multiple runs can be completed without any errors in the



Mechanism of a reentrancy attack (Source)

execution of the code. A famous example of this was the DAO Hack that happened in 2016. The DAO, which stands for "decentralized autonomous organization," refers to an entity that operates based on transparent rules enforced and maintained through smart contracts. A logic error in the smart contract resulted in a reentrancy attack that would allow an attacker to 'loop' the result of the function, transferring ETH to the wallet of the user without updating the balance. When the smart contract fails to update the user's balance before sending funds, an attacker can use the "withdraw function" of a smart contract to continuously drain the funds stored in smart contracts.

Smart contracts are also susceptible to oracle exploits, which take place when an attacker manipulates market conditions to profit at the expense of the smart contract, for instance, when a smart contract facilitates the exchange of two tokens. It calculates the exchange price by comparing it to the exchange rate of another similar contract on the chain and offering it with a little adjustment. Here, the other exchange is acting as a pricing oracle for this contract. In this scenario, when the oracle exchange has much less liquidity than the primary exchange, the opportunity for an economic exploit occurs through price manipulation. An attacker can make large purchases on the oracle exchange to manipulate the market exchange rate and can then make considerably larger purchases on the primary exchange to profit from the price shift. When writing smart contract code and creating procedures, extra caution must be taken to prevent exploitation through enormous market volatility in a single transaction.

Spartan Protocol, a DeFi protocol on Binance Smart Chain, faced an attack due to a flawed liquidity share calculation. Spartan Protocol termed it as an economic exploit and tweeted that the attacker used $61 million in BNB to overcome the liquidity pool through the use of an 'unknown economic path' to remove roughly $3 million from the pool. Basically, the asset balance of the liquidity pool was inflated and then the same amount of pool tokens were burned to claim a large number of underlying assets. The total loss is calculated to be more than $30 million.

A third type of exploit is a flash loan attack, which takes advantage of a flash loan, which is a loan that is made and returned within the timeframe it takes to create a new block on the blockchain. It is a loan that doesn't require the borrower to put down any collateral. The borrower will quickly flip a profit on the amount and return the initial loan before a new block is formed. In February 2020, bZx Fulcrum, a loan market similar to Compound, was the target of a series of high-profile flash loan attacks. The attacker took out a flash loan and used some of the money to buy a leveraged short position, then used the rest to manipulate the price of the oracle exchange on which the short position was based. After that, the attacker profitably closed the short, unwound the market trade, and repaid the flash loan. The net profit was about $1 million.

[ii] Governance Risk

DeFi applications such as MakerDAO are dependent on human-controlled governance process, for example adjusting parameters of the protocol, making it susceptible to human fallibility.

Usually, changes within DeFi protocols take place through democratic mechanisms. In order to participate in these governance mechanisms, users have to first acquire governance tokens that have protocol governance rights attached to them such as MKR tokens issued by MakerDAO. The users can then use these tokens to partake in the decision making process. To ensure that no single user attains majority — so as to maintain decentralization — the number of governance tokens supplied are usually fixed. However, governance risk is triggered if one of the users acquires a majority of liquid governance tokens and manipulates his or her position to gain control of the protocol and possibly steal funds.

One instance of this would be the True Seigniorage Dollar attack. True Seigniorage Dollar (TSD) is a decentralized, algorithmic stablecoin driven by oracle data. It uses a supply elasticity method around a Time Weighted Average Price (TWAP) oracle for price stability. The attacker gradually gained enough stake (33%) to control the voting process, thus hijacking TSD's DAO governance. Since the developers of the platform only had 9% stake, the attacker proposed a new implementation in the code using his 33% stake. While passing the new implementation, the attacker inserted a malicious token to mint 11.8 Billion TSD tokens. The attacker then immediately sold the aforementioned TSD tokens in PancakeSwap, thereby bringing the price of the project down to zero.

[iii] Oracle Risk

Without external input, blockchains are totally self-contained with no information other than the transactions that are happening on and added to the native blockchain, making them extremely limited and somewhat ineffective. Oracles were created in order to bring off-chain data securely onto the blockchain so that DeFi protocols may ensure that routine activities like liquidations and prediction markets work properly, for example.

Oracle risks occur when the data on these oracles is inaccurate or can be manipulated. DeFi platforms become susceptible to attacks when the operators of oracle have the power to manipulate the on-chain price of the asset. One such example was the Compound oracle exploit; the price of the DAI stablecoin increased by 30% from its original value on Coinbase, which acted as a price oracle for Compound. With the increase in the price of DAI, a majority of loans which were handed out by Compound were now under collateralized, meaning the value of loans exceeded the collateralization ratio threshold. In order to overcome the problems ensued from under collateralization, about $89 million assets locked in Compound were liquidated. The reason behind the spike in prices remains unclear, but it was likely an oracle attack directed towards Compound.

[iv] DEX Risk

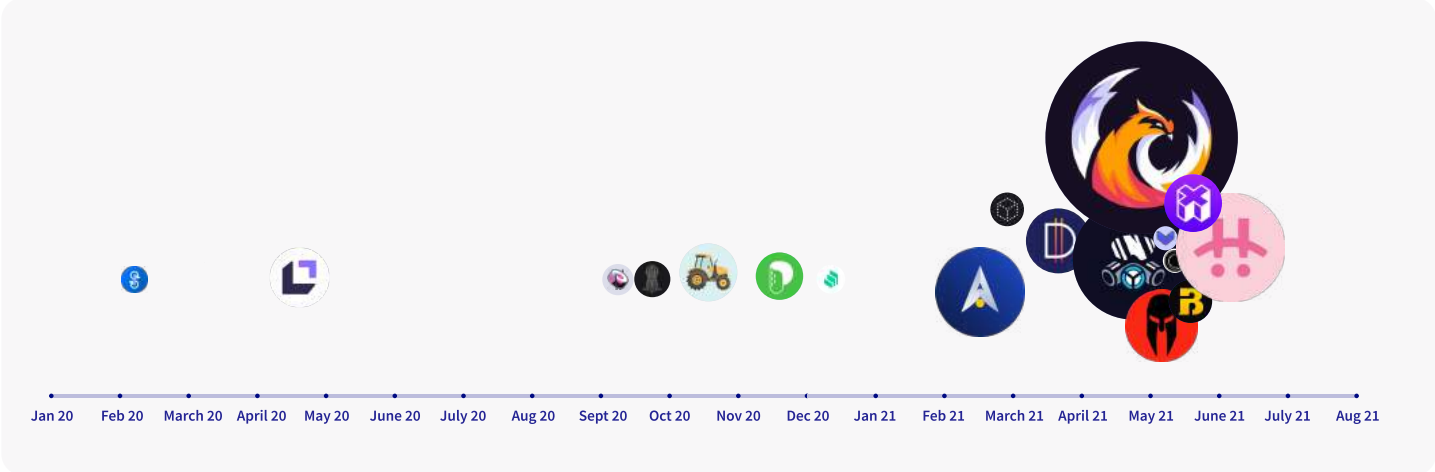
One of the biggest risks faced by DEXs is impermanent loss, which refers to the difference in value between funds held in a liquidity pool of anAMM compared to holding the same funds in a crypto wallet Users may provide liquidity to a pool in the DEX and become liquidity providers (LPs).

Since AMMs are disconnected from the external markets, the change in the price of the token in the external market does not affect the price of the token in the liquidity pool — this presents an opportunity for arbitrage. Arbitrage traders will then buy that token, the price of which has increased at a discounted rate. This will go on till the state of equilibrium is achieved. Post- arbitrage liquidity providers will end up with more of one token in comparison to another. Impermanent loss occurs when the value of assets due to arbitrage decreases as compared to what it would be if the assets were for instance merely deposited in an exchange. Therefore impermanent loss is the temporary loss that occurs when liquidity providers maintain liquidity in the pool. The loss only becomes permanent if the liquidity provider decides to withdraw their assets for good. Further, DEXs like Uniswap also give the liquidity providers a share of fees in order to stabilize the loss they may incur with impermanent loss.

The loss only becomes permanent if the liquidity provider decides to withdraw their assets for good. While some AMMs, such as Cap, are looking to reduce impermanent loss by utilising an oracle to establish exchange prices and dynamically changing a pricing curve to prevent arbitrageurs from exploiting LPs, impermanent loss continues to be a major issue with the majority of AMMs now in use.

[v] Crypto Crime in DeFi

The graph above highlights DeFi scams below the value of $10 million that have happened in 2020 and 2021 so far. As DeFi gained popularity in the last two years, DeFi scams have not only increased in frequency but also in size. Below are some of the most notable DeFi hacks and



Notable DeFi hacks above $10 million in 2020 and 2021

scams that have occurred in the last couple of years.

Rug pulls are exit scams that happen when cryptocurrency promoters disappear with investors' money during or after an initial coin offering (ICO). **DeFi rug pulls** are the new iteration of this type of scam whereby crypto developers abandon a project and run away with investors' funds by draining the funds from the liquidity pool into their own private wallets. Rug pulls exploit the vulnerabilities present in smart contracts until the value of the token drops to zero. Some examples of DeFi rug pulls include:

- The **PAID Network scam**, which happened on 5 March 2021, is pegged to be one of the biggest scams wherein the hackers minted about $160 million worth of currency by exploiting PAID contract's token minting feature. The hackers after exploiting the feature transferred the amount into their own wallet and exchanged the newly minted tokens for ETH on Uniswap.
- The **Meerkat Finance** scam was brought to light on 4 March 2021. Meerkat Finance was a yield farming project launched on Binance Smart Chain that fell victim to a rug pull. The scam drained about 13 million BUSD and about 73,000 BNB, which in total are now worth $31 million. The on-chain data shows that the hacker(s) drained the funds by altering Meerkat Finance's smart contract containing the project's vault business logic using the original Meerkat deployer's account.

Flash loan attacks were previously mentioned under "Smart Contract Risk." Flash loans are a new type of uncollateralized loans enforced by smart contracts, which enable the required amount without any capital. Flash loan attacks are smart contract exploits wherein an attacker takes out a flash loan from a DeFi protocol to manipulate the market and exploit the software vulnerabilities within the code. Some examples include:

- Binance Smart Chain-based **Bogged.Finance** lost $3 million due to a flash loan attack. According to the team of Bogged.Finance, a flash loan attack targeted the protocol which permits users to place 'limit orders' on any token on Binance Smart Chain.
- Not long ago, **PancakeBunny**, a DeFi revenue aggregator on Binance Smart Chain, also fell victim to flash loan attack. The hacker stole $45 million (114,000 WBNB) from the BSC exchange. PancakeSwap was used by the hacker to borrow a huge supply of Binance's BNB token through a flash loan. The borrowed funds were then used to flood the PancakeSwap USDT-WBNB pool, triggering a large amount of Bunny tokens (BUNNY) to be minted, thereby crashing the price of BUNNY.
- Similarly, on 16 May 2021, bEarn.Fi a cross-chain farming protocol lost close to $11 million. According to the report published by bEarn.Fi, the attackers first took a flash loan on Cream Finance and then made 30 repeated deposits and withdrawals on bEarn.Fi's bVaults for. Afterwards, the attackers repaid the flash loan to Cream Finance and drained around $11 million worth of stablecoins from the bVault.

[vi] Tornado Cash Case Study

Tornado Cash is the most popular coin-mixing service on the Ethereum blockchain. It is a privacy tool for obfuscating Ethereum transactions. First launched in August 2019, Tornado Cash utilizes zero-knowledge proof (ZKP) — through mathematical evidence, there is proof that a transaction occurred without revealing the transaction's payment information. Unlike other ZKP-based Ethereum systems — Aztec and Nightfall (released by Big Four accounting firm, EY) — Tornado Cash is often compared to coin mixers on Bitcoin because of its popularity amongst retail users to make tracing funds more difficult.

What is a coin mixer?

A coin mixer helps obfuscate crypto assets by breaking the link between the original asset address and a new one. This makes tracing funds from a coin mixer to the source address a difficult task. Coin mixers are often used by malicious actors who have stolen, hacked or scammed to obfuscate their flow of funds. Though not all activities carried out by mixers can be definitively termed as illicit, a significant amount of funds from mixers can be illicit. In blockchain transaction monitoring, funds flowing to and from coin mixers are generally labeled high risk.

How does Tornado Cash work?

Tornado Cash offers a set of smart contracts that enable the user to obfuscate their funds by cutting the link between the original address and the receiver address. This is usually done by allowing users to deposit ETH in pools according to the following denominations:

- .1 ETH

- 1 ETH
- 10 ETH
- 100 ETH

Users then wait an indeterminate amount of time to allow more users to deposit after them. As the number of users accumulate in the pool, the 'anonymity set' increases. The larger 'anonymity set' within the pool, the harder it is to track the ETH that is withdrawn from the pool.

The funds are then withdrawn into a separate cryptographic address; Tornado Cash will hand the user an off-chain cryptographic receipt that the user can use at any point in time to pull out the ETH from the address.

Flow of funds analysis from Tornado Cash

While its efficacy as a privacy solution and how it may be regulated in the future are yet to be seen, the following analyzes the funds flowing from Tornado Cash to some of the most popular DeFi protocols in an attempt to get a taste of the illicit activity happening within the DeFi ecosystem. In particular, the following analyzes fund flows from Tornado Cash to **Uniswap**, **Aave**, and **Compound**.

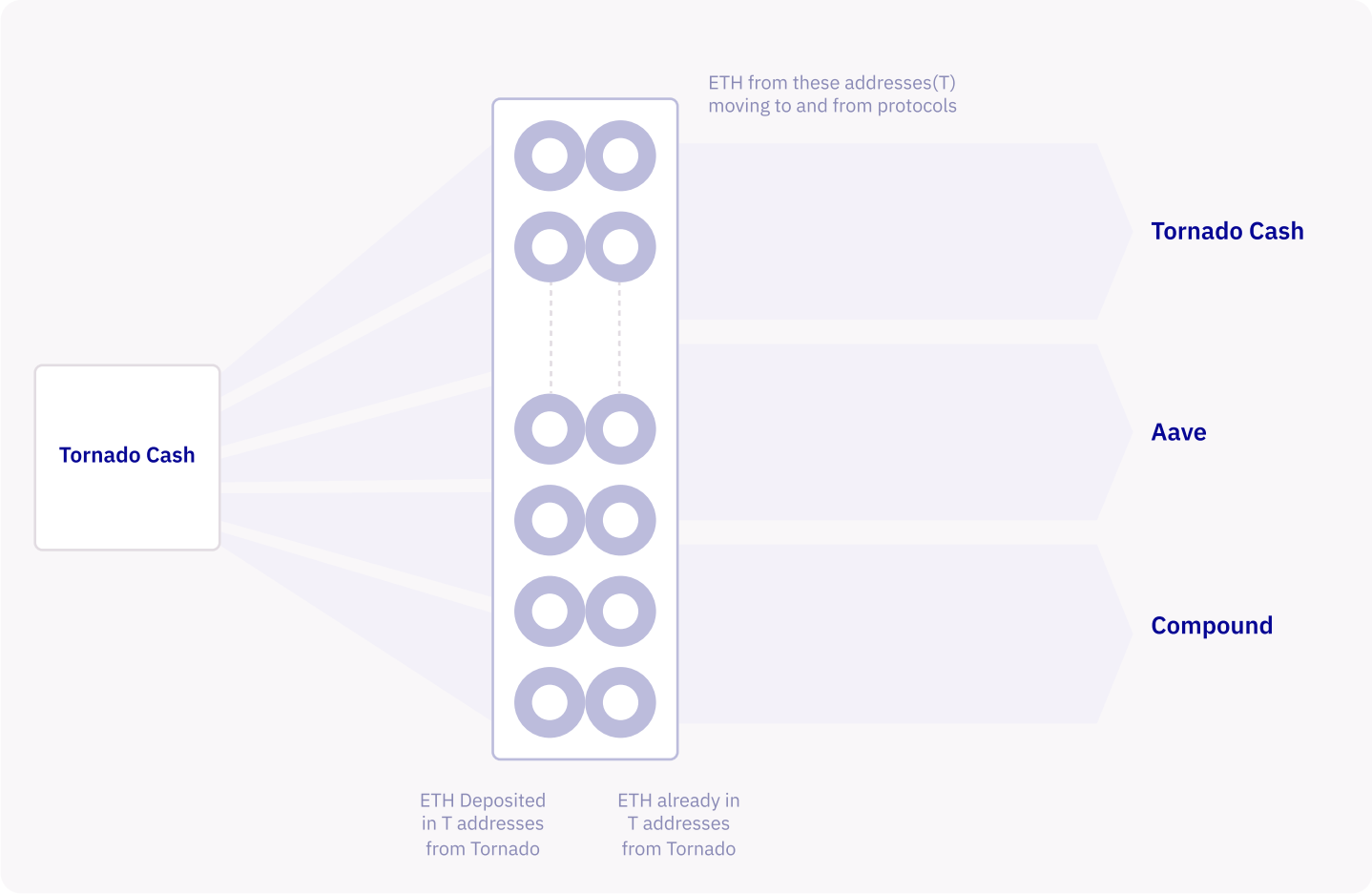
Please note that while Tornado Cash allows other crypto assets like USDT to be mixed as well, the following focuses on ETH as majority of the funds mixed using the service are ETH.

Methodology

The following methodology was used to to identify the flow of ETH for all four protocols listed above:

We refer to the following smart contract addresses as Tornado Cash for the purposes of our study. (Note that they correspond to the denominations users are allowed to deposit ETH, as listed above.)

Tornado.Cash: .1 ETH pool:
0x12D66f87A04A9E220743712cE6d9bB1B5616B8Fc
Tornado.Cash: 1 ETH pool:
0x47CE0C6eD5B0Ce3d3A51fdb1C52DC66a7c3c2936
Tornado.Cash: 10 ETH pool:
0x910Cbd523D972eb0a6f4cAe4618aD62622b39DbF
Tornado.Cash: 100 ETH pool:
0xA160cdAB225685dA1d56aa342Ad8841c3b53f291



Transferring ETH From T To Uniswap, Aave, And Compound

To identify the flow of funds, we tracked all addresses to ever receive funds from the Tornado Cash smart contracts. The set of these addresses are referred to as **T** hereafter.

Thereafter, we then studied the movement of these funds from **T** to three of the most popular protocols on the Ethereum blockchain. Using these protocols we can observe the broadest spectrum of the flow of funds.

We use the following smart contract addresses for the protocols studied:

Uniswap

Uniswap v2: 0x7a250d5630b4cf539739df2c5dacb4c659f2488d

Uniswap v3: 0xE592427A0AEce92De3Edee1F18E0157C05861564

Aave

Aave v1: 0x398eC7346DcD622eDc5ae82352F02bE94C62d119

Aave v2: 0xcc9a0B7c43DC2a5F023Bb9b738E45B0Ef6B06E04

Compound

0x4Ddc2D193948926D02f9B1fE9e1daa0718270ED5

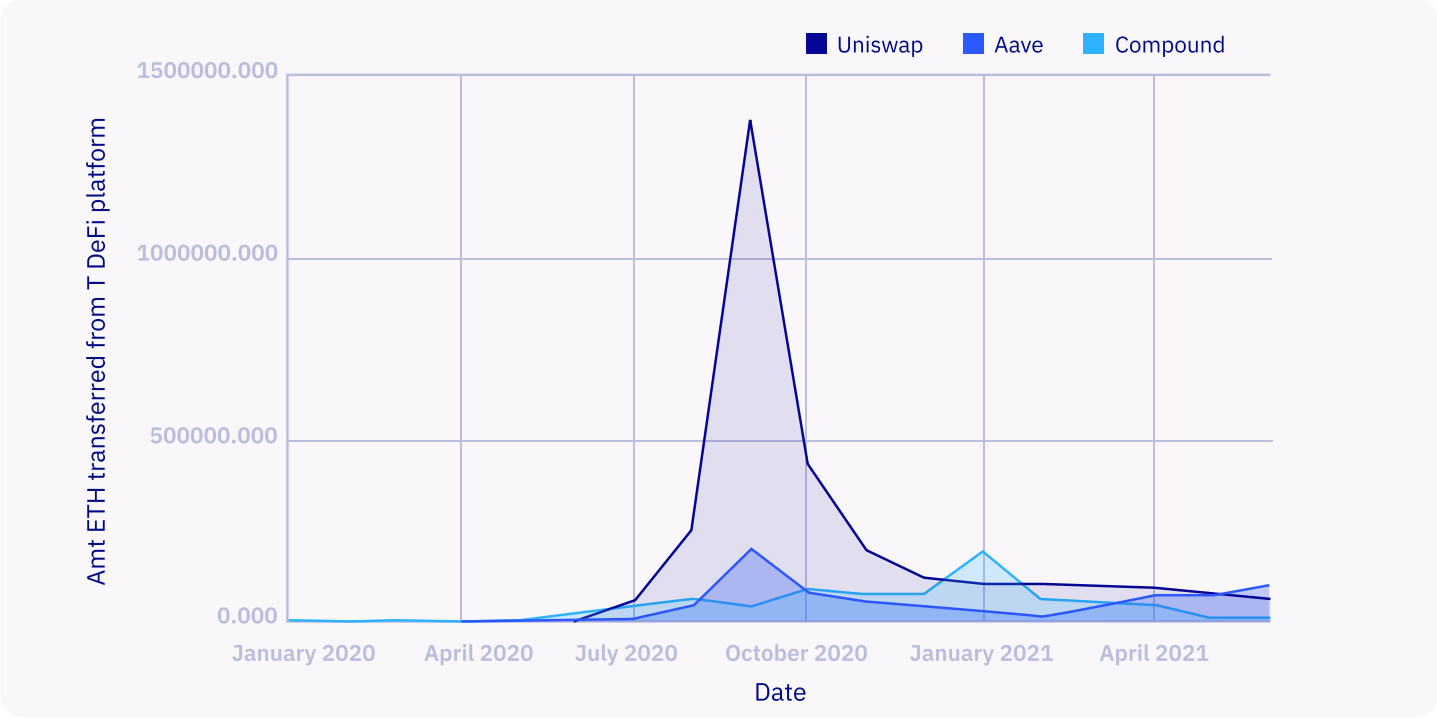
FINDINGS

Transactions received by T

A total of 20,446 addresses (**T**) were identified as receiving ETH from Tornado cash between the dates of 16 December 2019 (when version 2 of Tornado Cash was released) and 4 June 2021. These addresses interacted with Tornado Cash directly, in the first hop, without any intermediary entities. The same addresses (**T**) received 1,288,362.80 ETH in total.

Transactions sent by T to Uniswap, Aave & Compound

Protocol	Amt of ETH moving from T to protocol (ETH)	# Transactions moving ETH from T to protocol	# Addresses from T to protocol
Uniswap	2,887,770	434,409	7,353
Aave	698,684	14,509	671
Compound	840,414	5,036	507



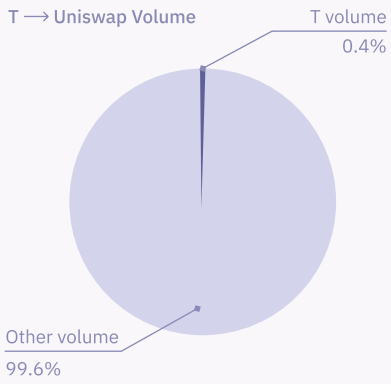
Amount Of ETH Transferred From T To Uniswap, Aave, And Compound By Month From January 2020 To July 2021

Uniswap

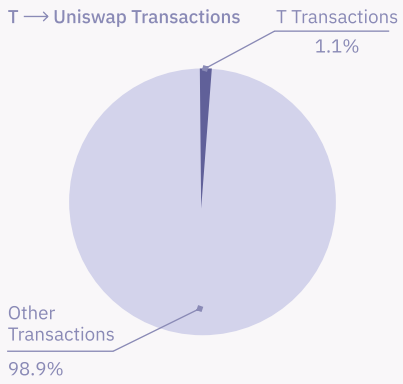
Uniswap is a decentralized exchange based on the Automated Market Maker mechanism.

Interaction of **'T'** addresses with Uniswap

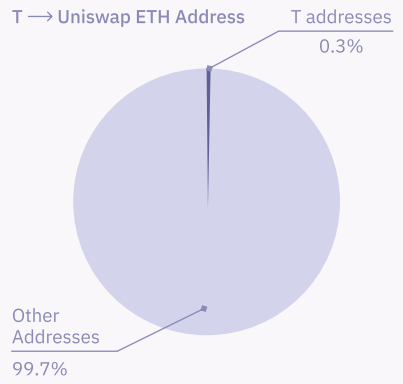
- Amount of ETH moving from '**T**' to Uniswap: 2,887,770 ETH
- Number of transactions moving ETH from '**T**' to Uniswap: 434,409 transactions
- Number of addresses moving ETH from '**T**' to Uniswap: 7,353 addresses



Amount of ETH moving from T to Uniswap as a percentage of total amount of ETH moving into Uniswap over the same period



Number of transactions moving ETH from T to Uniswap as a percentage of total number of transactions moving ETH into Uniswap over the same period



Number of addresses moving ETH from T to Uniswap as a percentage of total addresses moving ETH to Uniswap over the same period

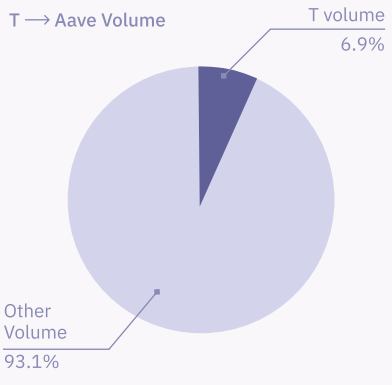
---

Aave

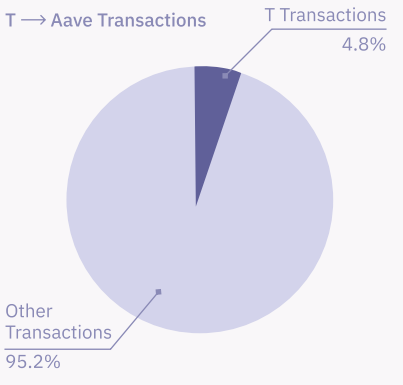
Aave is a decentralized protocol on Ethereum blockchain that enables users to lend and borrow a range of crypto assets. Aave can be used to earn passive income for lenders who have given out crypto to borrowers.

Interaction of **'T'** addresses with Aave

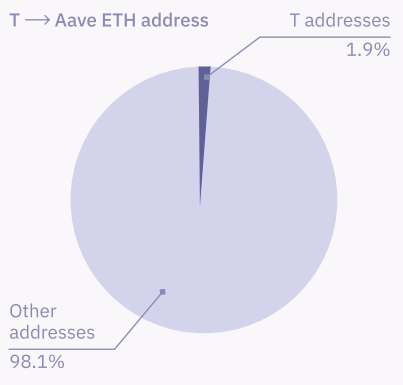
- Amount of ETH moving from '**T**' to Aave: 698,684 ETH
- Number of transactions moving ETH from '**T**' to Aave: 14,509 transactions
- Number of addresses moving ETH from '**T**' to Aave: 671 addresses



Amount of ETH moving from T to Aave as a percentage of total amount of ETH moving into Aave over the same period



Number of transactions moving ETH from T to Aave as a percentage of total number of transactions moving ETH into Aave over the same period



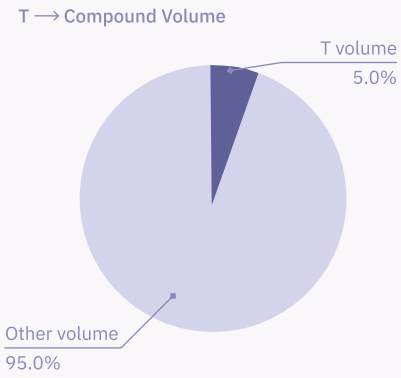
Number of addresses moving ETH from T to Aave as a percentage of total addresses moving ETH to Aave over the same period

Compound

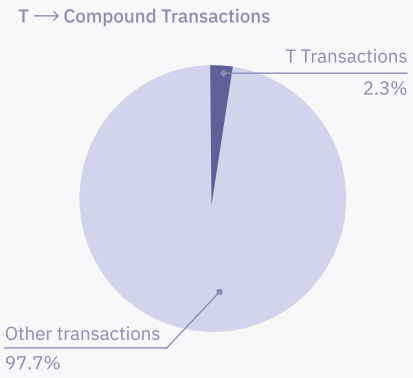
Compound is another decentralized algorithmic money market (AMM) which allows its users to lend and borrow crypto on its platform, letting lenders earn passive income from the crypto being lent out.

Interaction of **'T'** addresses with Compound

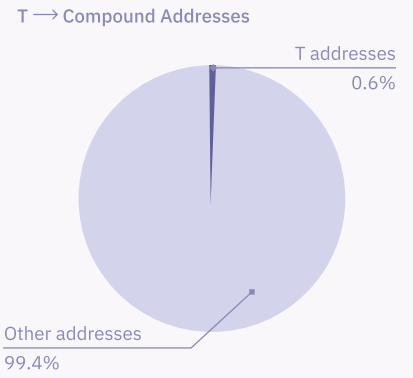
- Amount of ETH moving from '**T**' to Compound: 840,414 ETH
- Number of transactions moving ETH from '**T**' to Compound: 5,036 transactions
- Number of addresses moving ETH from '**T**' to Compound: 507 address



Amount of ETH moving from T to Compound as a percentage of total amount of ETH moving into Compound over the same period



Number of transactions moving ETH from T to Compound as a percentage of total number of transactions moving ETH into Compound over the same period



Number of addresses moving ETH from T to Compound as a percentage of total addresses moving ETH to Compound over the same period

DeFi Vs. CeFi: A Comparative Approach

[a] The Pros

Compared to its centralized counterpart, DeFi brings financial infrastructure and applications to the masses — creating a more accessible way to utilize financial systems and tools through a permissionless ecosystem that does not require centralized third-party intermediaries. Due to the lack of centralized intermediaries, DeFi automates many functions, ensuring lower costs, a higher degree of privacy and security, and more democratic decision making. The increase in accessibility also benefits developing nations with emerging economies. Compared to CeFi (centralized finance), it provides greater opportunities when it comes to credit, access to trading platforms, and investments. For many, the limited access to financial systems means that individuals' means to grow wealth — much less generational wealth — has been stifled.

DeFi promotes rent-seeking behaviour and discourages oligopolistic behaviour in financial institutions. Traditionally, the barriers to entry for the financial sector are high. Due to limited capital and resources, it is often difficult for small and medium-sized businesses to compete against larger financial institutions, resulting in acquisitions by large conglomerates and decreased competition. DeFi's permissionless nature also means that barriers to access for users are lower, allowing for free flow of interaction between individuals and entities. For example, an individual who requires a loan may submit an application without the need to wait for approval or rejection by an authority. It is simply completed through code on the blockchain and a traditional credit score may be replaced by over-collateralization or through other means.

Another point to note is that decision making on distributed ledgers — upon which DeFi is built — is not reliant on a single operator, but is instead completed through a network of nodes. For protocols that have gained a critical mass, security is assumed based on the belief that a sufficient number of nodes in a network would be incentivized to behave honestly to reach a consensus and validate the recorded transactions. This consensus model results in immutability and censorship resistance. The transparent and publicly verifiable structure of DeFi ensures that the custodian of an asset is always validated on a public blockchain and unlike centralized exchanges custody of assets involve only open-sourced smart contracts and wallets.

As transactions between parties are verified and processed through code and cryptography, there is no need for validations from third parties, eliminating bottlenecks and human errors that are rife in traditional financial systems. However, once a transaction is made over the blockchain, it is not easily reversible. For greater user protection, additional measures such as escrow mechanisms may also be put in place.

While sceptics may cite consumer protection as the primary concern that therefore requires conventional legal mechanisms (ie. insolvency laws or debt litigation), evangelists of DeFi may argue that the system is self-sustaining as it primarily acts as non-custodial platforms that control collateral through a coded set of rules. Governance and effective regulatory regimes with specific legal implications can be built into the system, making the applications self-sustaining and more secure.

In the example of DeFi lending, the system allows lenders to generate passive income by providing and maintaining liquidity to the system. And in the case of an unhealthy loan, it allows for faster liquidation — thus killing two birds with one stone. Further, it negates the impediments created by the traditional collateral system, which is usually impractical to enforce due to the sheer amount of

expenses and documentation involved.

[b] The Cons

As DeFi is still in its nascent stages, there are still areas where DeFi falls short in its goal of true financial democratization. As the industry matures, solutions will be built in order to overcome these challenges.

In its current form, the lack of a credit score system — or something similar to it — requires borrowers to over-collateralize in order to access DeFi loans. As a result, only crypto holders can gain access and benefit from the DeFi ecosystem.

As previously mentioned, the issues of speed and scalability continue to persist. The current public blockchains underlying DeFi may be unequipped to process large amounts of data at the speed in which transactions occur by today's standards. This shortcoming is especially problematic to institutional players who require speed and certainty of execution. During peak usage, networks may be clogged even further, resulting in a backlog of pending transactions, ultimately resulting in information gaps, pricing delays, and overall market insufficiency. Furthermore, technical instability issues may cause eventual liquidity risk.

Transaction costs is another issue that needs to be addressed. Since network fees and on-chain transactions go hand in hand, an increase in the latter could lead to a situation where network fees become disproportionately high. In this situation, transactions that do not demand an extremely high network fee will most likely not be processed — causing an imbalance in the system. According to DappRadar's Q3 2020 Decentralized Finance Ecosystem Report, Ethereum holds 96% of total transaction volume in the DeFi ecosystem, highlighting the overdependence on Ethereum and consequently on the Ethereum 2.0 update to resolve some of the major technical issues of DeFi. Further, newer chains have emerged since Q3 2020, like Binance Smart Chain, Polygon, and Matic, which may be able to reduce the dependence on ethereum, however most of the DeFi protocols still run on Ethereum.

Users of the DeFi ecosystem need to be aware of smart contract risks. Essentially, the custodial risks in CeFi are exchanged for smart contract risks in DeFi. Examples of smart contract risks include the exploitation of bugs in the code or the manipulation of price oracles. In all fairness, these are all developmental flaws that can be monitored and corrected to reduce the odds of their occurrence. DeFi protocols and dApps may implement bug bounty programs or encourage more rigorous security audits so that the system is less susceptible to hacks, massive losses, and illicit transfer of funds. DeFi may also take a leaf from the CeFi playbook and implement tactics such as third-party audits and insurance schemes, enforcing compliance with regulations, administering risk management procedures, laying down capital buffers, and consumer protection measures.

Unlike CeFi, DeFi does not have effective regulations in place to protect users in the present time and as a result, the victims of DeFi hacks have no resources in the current regulatory regime. Further, anyone sitting in any country may access DeFi protocols without the need to go through KYC — unintentionally providing bad actors access to financial services for illicit activity. The lack of KYC also means that users often need to over-collateralize to access services such as loans. Proof of on-chain identity will eventually lead to dApps or protocols that will provide something similar to credit scores.

Regulating The Financial Frontier: Notes From The FATF & Notable Jurisdictions

When it comes to digital asset regulation, so far, jurisdictions around the world have been able to lean on and build upon previously established financial regulations. DeFi, with its unique code-based structure and fast-paced developments, is forcing regulatory bodies to re-evaluate some of their existing frameworks so that they may implement guidance and regulations against money laundering, terrorism financing, and other illicit activity in more effective manners. While these frameworks are still in the process of being crystallized, existing guidance and regulations may provide some clues on how policymakers may approach the DeFi ecosystem.

The dramatic rise of DeFi in the last couple of years has resulted in one of the most notable changes in the latest FATF draft updated guidance for Virtual Assets and VASPs. More often than not, the crypto industry is keen to follow the FATF's guidance as it provides clarity and certainty for all stakeholders involved. However, in the present case, the latest draft guidance — published in March 2021 — has been a source of significant controversy.

While the updated guidance was expected post-June plenary, the FATF announced that there has been a delay and the updated guidance for VAs and VASPs is expected to arrive in November 2021. While the crypto industry awaits the latest update, the following section highlights some of the most notable and intensely debated points in the latest guidance.

[a] FATF Guidance Related to DeFi

The FATF is the international regulatory body responsible for developing best practices and setting international standards on combating AML/CFT activities. The FATF adopts a broad scope of governance and also ensures the implementation of these international standards by imposing a series of recommendations on national governments. However, it gives complete discretion to independent jurisdictions when it comes to implementation — for example, jurisdictions may choose to put in legislation in the form of a new Act or they may choose to amend the regulations already in place. Usually, a grandfathering period is also put in place to ensure its smooth and timely execution.

In its 2019 guidelines, FATF coined the term Virtual Asset Service Providers (VASPs) and provided guidance on the scope of their activities and limitations in order to ensure stakeholder protection. On 19 March 2021, the FATF published a draft Updated Guidance (The Guidance) recommending a risk-based approach applicable to those entities that are engaging in activities related to Virtual Assets. The guidance expands the scope of VASPs, placing DeFi platforms under the VASP umbrella. Consequently, many newly-designated VASPs will not be able to implement the AML/CFT obligations set out in the guidelines.

The crypto industry collectively responded to the FATF's draft guidance, highlighting the following:

- The ways in which DeFi platforms are structured make it improbable for platforms to readily identify intermediaries who would be responsible for AML/KYC compliance.
- Due to the nature of DeFi, only a handful of protocols are programmed to provide automated KYC/AML checks.
- The implementation challenges faced by centralized VASPs, such as Travel Rule, will also apply to DeFi. In fact, it may be even more challenging for the DeFi ecosystem as the guidance was not created with the DeFi ecosystem in mind.

In the draft Guidance, the FATF expanded its VASP scope to include service providers that were previously not on their radar, including non-custodialsoftware wallets, multisig services, software-based decentralized exchanges, and other forms of non-custodial services. The said Guidance focuses on six areas: 1) clarification of virtual assets and VASP definitions, 2) stablecoins, 3) the risks and potential risk mitigants for peer-to-peer (P2P) transactions, 4) licensing and registration of VASPs, 5) implementation of the Travel Rule, and 6) principles of information-sharing and cooperation among VASP supervisors.

Aside from upcoming guidance on VAs and VASPs, the FATF released the Second 12- Month Review of Revised FATF Standards on VAs and VASPs, taking a look at the progress that has been made so far by jurisdictions in implementing the Standards. Within the review, the FATF further stated that the definition of VASPs which was set out in the FATF's 2019 guidance could apply to dApps. The FATF further elaborated that the draft revised Guidance largely adopts and expands upon the same language used in the 2019 guidance. Based on the feedback received in the public consultation, the FATF acknowledged that it needs to give more extensive and clearer guidance on how decentralized projects fall under the definition of VASPs

[i] Summary of DeFi-Related Points & Their Implications

- The draft updated guidance discourages the interaction of regulated custodial intermediaries with the DeFi ecosystem. It lays down that VASPs "should consider whether any VAs or products they plan to launch or transact with, will enable P2P transactions... Similarly, VASPs and other obliged entities should consider the extent to which their customers may engage in, or are involved, in P2P activity."

  Implication: *This bifurcation will lead to the creation of two parallel financial systems that will not coincide in any manner: one system would be completely regulated with robust user protection laws and the other would be permissionless lacking minimum surveillance, thereby opening up their users to a number of risks including, but not limited to, AML/CFT risks and leaving the users of the latter without any legal recourse.*

- The 2019 guidelines, though narrow in their scope, only focused on those entities who had custodial relationships with VAs on behalf of the customers such as centralized digital exchanges that hold on to the private keys of their customers and move the VAs from one VASP to another. The draft Guidance abandons this approach and expands the application of financial surveillance requirement beyond custodial financial intermediaries and expands it to include the newly designated VASPs

  Implication: *The aftermath of this would require the implementation of AML/CFT guidelines on the newly designated VASPs. This approach is contradictory to the position adopted by FATF member countries and followed by industry participants. In the U.S., this would directly go against the CVC wallet requirements and exemptions given to money transmitters laid down by FinCEN. Additionally, in order to comply with the Guidance, non-custodial decentralized financial protocols will have to change their infrastructure to become centralized in order to permit access.*

  Secondly, if the same regulations which are applied to custodial financial intermediaries are applied to VASPs as set out in the draft updated guidance, then in such a case the newly designated VASPs would be unable to implement such AML/CFT obligations due to their inherent decentralized nature. Due to the decentralized nature of DeFi, no DeFi platform has the same level of control over a protocol that a CeFi custodial financial intermediary does. For instance, DeFi platforms do not have control over assets as users of the DeFi ecosystem retain complete control over their assets, meaning DeFi platforms would not be to comply with guidelines such as the ones pertaining to the asset freeze.

- The Guidance seeks to bring within its scope those individuals or entities that benefit from the provision of financial service "regardless of whether the profits are direct gains or indirect." This is done to expand the perimeter of those regulations which solely cover custodial financial intermediaries.

  Implication: *The guidance draft does not differentiate between those directly involved in the provision of DeFi services and those who play a limited or more indirect role in their provision. This essentially means that any person who controls a blockchain address or interacts with DeFi protocol in any manner — including merely conducting sanctions checks — would be required to*

partake in AML/KYC in compliance.

Such stringent regulations aimed at encompassing all the VASPs partaking in VA arrangements at any stage will prove to be counterproductive as it would amount to effectuating a de facto ban on even licit participants who may not have the technological infrastructure to comply with these guidelines.

- Under the draft guidance, multiple non-affiliated persons or entities — such as the developers who built the DeFi platforms — may fall within the ambit of VASPs. On the surface, the draft guidance excludes software developers from its definition of VASPs "...when solely developing or selling the application or platform." However, when read in conjunction with the other parts of the guidance, software developers do not stand absolved for instance FATF implores the regulators to not only identify entities "who generated and drove the creation and launch of a product or service" but also to ascertain whether such entities would fall under the definition of VASPs.

  Implication: *Individuals who build the codebase for a DeFi protocol would fall under the definition of VASPs and be held responsible for compliance — irrespective of whether he or she was directly or indirectly hoping to realize economic gains from the said codebase. These individuals or entities would have to be compliant with the full range of obligations that a centralized VASP would have without having access to the resources that centralized agencies would have.*

  This begets the question that whether launching a self-propelling infrastructure offering VASPs services is equivalent to offering them. Following the same line of thought, entities that are commissioning others to build a DeFi infrastructure would have the same level of obligations as those actually building them. According to the FATF, the lifecycle or circulation of a service such as a DeFi platform should be viewed in its entirety — meaning that decentralization of an individual aspect of an operation cannot be viewed in isolation and would qualify as VASP thereby not realising it from its obligations.

  The ramification of this would be that any software developer who publishes a code that may be autonomous and open-sourced may still be considered a VASP if he or she has contributed towards the financial service offering, even when that developer has no ongoing control over the program and does not directly or indirectly profit from its use. Such developers would not be able to implement AML/CFT controls as they no longer have the protocol under their control and when the protocol in question could already have been copied and multiplied.

- The FATF guidelines have set out a precondition that for an entity to be considered VASP they should conduct listed activities on behalf of a legal or natural person. In essence, this guidance removes governance token holders from their purview. However, the FATF has also laid down regulations that may indicate otherwise. For example, "where customers can access a financial service, it stands to reason that some party has provided that financial service" and "each natural or legal person constituting the governance body could also be a VASP depending on the extent of the influence it may have."

  Implication: *Under this guidance, it is reasonable to assume that governance token holders would fall under the category of VASPs and would be obligated to comply with AML/CFT regulations. But given that no individual entity can make changes to the blockchain protocol on their own, they may not be able to implement AML/CFT controls.*

  This will likely result in two scenarios: firstly, good actor governance token holders, understanding that they might not be able to unilaterally implement the obligations required for VASPs, will not partake in DeFi activities, which would lead to the second scenario. With the good actor governance token holders out of the way, governance of DeFi would lie either with the illicit actors resistant to follow the law or protocol governance would totally be eliminated.

- To comply with AML/CFT obligations laid down in the Guidance, large stores of personal data about actual persons or businesses conducting transactions will have to be stored somewhere.

  Implication: *Such requirements would, in turn, open up the possibility of a data breach if compliance is being conducted through the use of a rapidly assembled automation platform and if those platforms had*

not been robustly tested.

- The draft updated Guidance requires VASPs to record and monitor information of non-FI counterparties (ie. self-hosted wallets) who transact on their own behalf with a user on the VASP even though the VASP may have no relationship with the individual (as they would now fall under the VASP definition.) Non-FI counterparties would also include web developers or software coders of DeFi platforms and will now be required to ensure compliance with the Travel Rule. These individuals — who may no longer be a part of the DeFi platform once it has been launched — may not have access or means to ensure such compliance. Counterparty data has to be collected and recorded for all the transactions — not just those which fall beyond Recommendation 16's USD 1000 threshold. In addition, the guidance specifically states that jurisdictions should mandate VASPs to carefully scrutinize transactions between them and self-hosted wallets to ensure that they do not fall under suspicious activity criteria and meet sanctions compliance.

  Implication: *There are several issues for VASPs dealing with non-FI parties. Firstly, the FATF has not set out any mechanisms for VASPs to obtain such information from non-FI entities. Secondly, even if the VASPs were able to adhere to the customer's counterparty identification requirement, VASPs are not able to conclusively prove that no other person has the private key to the wallet and the ability to transfer the associated digital assets — even if one identified counterparty has access to a crypto wallet's private key, it does not mean it has complete and exclusive control over the digital assets also. Last but not least, there are also privacy issues to take into account, further negatively impacting financial intermediaries.*

- Software programs that are decentralized or take the form of dApps and operate on a P2P network of computers running a blockchain protocol are recognised by the FATF. Though the FATF acquiesces to the fact that VASP activities such as exchange or transfer of virtual assets may also take place through decentralized exchanges, the position regarding the status of dApps as VASP remains unclear as FATF maintains that it does not aspire to regulate technology and its recommendations are meant to be technology-neutral.

  Implication*: While the FATF indicated that they do not plan on regulating technology, it did not take DeFi into account when making this statement. Under its expansive definition of VASPs under the draft guidance, dApps would fall under the definition of VASPs as they would inevitably have a central party involved in creating, launching, setting parameters, holding an administrative key, or collecting the fee. Sufficiently regulating such entities would amount to the regulation of dApps without directly bringing them under the purview of VASPs.*

  However, smart contracts do not require the involvement of entities other than the participants for the execution of financial transactions. In this situation, it is unclear which VASPs, if any, would be required to implement compliance obligations.

[b] EU Regulations: A Focus on Stablecoins

On 24 September 2020, the European Commission (the Commission) published a much-anticipated proposal on the establishment of an EU-level regime for crypto-assets; the Markets in Crypto-Assets Regulation (MiCA). MiCA aims to bring stablecoins within the ambit of the MiCA regime on crypto assets. Additionally, it further sets its sights on revamping the e-money regime by expanding its scope

In this regime put forth by MiCA, stablecoins are likely to fall under either one of the definitions depending on their inherent characteristics:

- One class of stablecoins would fall under the definition of asset referenced tokens — "a type of crypto assets whose main purpose is to be used as a means of exchange and that purports to maintain a stable value by referring to the value of several fiat currencies, one or several commodities or one or several crypto assets, or a combination of such assets."
- Another class would fall under the e-money token definition: "electronic money token or e-money token means a type of crypto asset whose main purpose is to be used as a means of exchange and that purports to maintain a stable value by being denominated in (units of) a fiat currency".
- Those stablecoins which do not fall under the aforementioned definitions can alternatively be classified as algorithmic stablecoins: "So-called algorithmic 'stablecoins' that aim at maintaining a stable value, via protocols, that provide for the increase

or decrease of the supply of such crypto assets in response to changes in demand should not be considered as asset-referenced tokens, as long as they do not aim at stabilising their value by referencing one or several other assets."

The issuers of these assets are required to have a legal entity separate from that of its owners so that when there is a breach of these regulations, the investors can file for damages against the issuers. Similar to those obligations imposed on entities issuing a prospectus for public offer securities, issuers of asset referenced token holders will now have to (a) publish a white paper and (b) attain authorization from their home state regulators.

The white paper must be registered with the home state regulators where the (a) crypto assets will be solicited or marketed to the customers or (b) listed in a crypto asset trading platform within the EU. Further, the issuer of such assets is required to publish the white paper on its website. The white paper, per MiCA, should essentially include a comprehensive description of the asset and the project, rights and obligations of the parties, details pertaining to the associated technology, and descriptions of the risks involved.

Both e-money token holders and asset referenced token holders who hold a significant amount of the aforementioned assets will be directly governed by European Banking Act and not their home/national regulators. The threshold for a significant amount is yet to be determined by the commission. This threshold will be decided via the size tests to be set by the commission.

Qualified investors — as defined by the European Parliament and the Council of the European Union — of e-money tokens and asset referenced tokens are exempt from such requirements. Adding to this, the above-mentioned asset holders will have to comply with comprehensive guidelines laid down by EBA concerning capital, interoperability and liquidity management. Any breach in these standards will trigger liability on the issuers for damages to be given to the investors.

A stablecoin that is operated or marketed toward customers within the EU region will have to be compliant with MiCA and EBA. Unlike issuers of general crypto assets, it is mandatory for issuers for e-money and asset referenced tokens to be (a) established in the EU and (b) should be authorized under MiCA or EMD (aka the E-Money Directive, which regulates electronic payment systems in the EU). Furthermore, issuers of stable coins that are outside the EU will need to establish a significant local presence in order to facilitate solicitation or target customers in the EU.

While one would expect that stablecoins, by definition, may fall under the EMD, the European Commission observed that they are better suited to be regulated under MiCA. Usually, crypto assets that can be defined as e-money under the EMD would not fall within the scope of MiCA. EMD defines e-money as "electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds to make to make for payment transactions (...) and which is accepted by a natural or legal person other than the electronic money issuer." Stablecoins which fall under the definition of e-money may also fulfil the requirements set by EMD. While the European Commission recognized this overlap it also stated that the EMD "might not mitigate adequately the most significant risks to consumer protection, for example, those raised by wallet providers." Hence, stablecoins fall under MiCA.

Lastly, crypto asset service providers — be it a trading platform, investment firm, or credit institution — all have to obtain authorization under MiCA.

[c] Singapore Regulations: If DeFi Tokens Were Capital Market Products

The Monetary Authority of Singapore (MAS) has broadened its scope of digital payment tokens to include any digital representations of money, whether or not generated on the blockchain. Should a DeFi token be pegged to be a capital markets product — in the same category as securities or derivatives contracts — then the DeFi exchange operating such a platform in Singapore may fall under the category of those engaging in the Securities and Futures Act's (SFA) controlled activities.

Unless otherwise exempted, an individual who conducts business in a regulated activity or holds himself out as conducting business in a regulated activity must hold a capital markets services license for that regulated activity under the SFA. If the token falls under the definition of Capital Markets Product, then such a token will have to be issued through the prospectus unless the project falls under SFA exemptions.

Further entities engaging in the issuance of such a token will need to apply to the MAS for issuance of the requisite license. In this case, the applicant DeFi platform will have to prepare and submit a detailed business plan, a compliance manual, as well as an AML/CFT enterprise risk assessment.

Further, P2P lending — which is a facet of DeFi — may also fall under the oversight of the MAS. But P2P lending may also come under the purview of the Moneylenders Act. Therefore any DeFi platform engaging in the activity of money lending will have to acquire a license for the same.

Section 3 of the Act defines a moneylender as “any person who lends a sum of money in consideration of a larger sum being repaid shall be presumed until the contrary is proved to be a moneylender.” This could potentially bring DeFi lending and borrowing platforms under the purview of the Moneylenders Act — even those individuals on DeFi platforms who issue loans to multiple participants on the platform, this might require the definition of excluded moneylender to be amended as under the present act.

New York | London | Bangalore | Singapore