DeFi: Reborn

A Spartan Labs X CoinMarketCap State of the DeFi Industry Report

September 2022

This report was authored by Gabriel Foo, Derek Lim, and Edmund Chua
of Spartan Labs Research in collaboration with CoinMarketCap.

Table of Content

CoinMarketCap

CoinMarketCap Research is CoinMarketCap's newly-formed research arm. It aims to leverage our data analysis and bring unique insights into the crypto market. We look to collaborate with other industry-leading voices and create a platform for people to learn and share their passion for crypto.

SPARTAN LABS

As The Spartan Group's Web3 strategic research arm, Spartan Labs Research is a specialized unit that advises and aids projects with tokenomics design/review to empower them with the most optimal and effective token models at launch and beyond. It also produces research reports and articles that are aimed at helping web3 users gain insightful perspectives with regard to the developments and issues within the space.

Is DeFi Dead?

The creation of Decentralized Finance (DeFi) has taken the crypto industry by storm.

The story was borne from a hypothetical thought experiment by Reddit user u/vbuterin (now widely known as Vitalik Buterin, co-founder of Ethereum) all the way back in 2016. He proposed an idea to run on-chain decentralized exchanges in the style of on-chain automated market makers, similar to that of prediction markets. This subsequently led to the creation of a decentralized financial system built on top of blockchain technology.

The DeFi industry has since grown by leaps and bounds to become a flourishing multi-billion dollar ecosystem full of opportunities. At its peak in December 2021, DeFi had garnered a whopping $247.96 billion in total value locked (TVL) across multiple blockchain ecosystems and applications. However, and in the wake of all the macroeconomic uncertainties, geopolitical tensions, increase in DeFi hacks and exploitations, general market downturn and increasingly bearish outlook due to recent events (collapse of Terra, 3AC, Celsius), the DeFi space has taken a large hit, with TVL falling to a low of $67.46 billion in June 2022.

This begets the question: Is DeFi dead?

Now, this is a tricky question to answer. Too hasty to say no, we come across as web3 bros/maxis living in denial; too hasty to say yes, we will be underestimating how dynamic and robust this space really is, how much it has gone through just to exist, and how much more it can still grow and evolve.

The best answer then, lies in the middle. Whilst DeFi is certainly not dead by any means, going down the same beaten path that led to this market cap collapse and TVL drain won't do this space any favors at all.

To be reborn, DeFi must build from the ashes of previous cycles. The way forward should always be informed by the lessons of the past, so that is where we will first comprehensively look to.

DeFi: A History

From the bleak cold of crypto winter, Uniswap, Maker Protocol and Compound stood out among the first few explorers to seek out uncharted lands. These projects were created with a similar vision in mind, to create a decentralized and trustless financial system built to be censorship-resistant and economically inclusive, while uncompromising on its capabilities and efficiency.

With this trio of decentralized applications, the idea of trustless digital asset exchanges, stablecoins and crypto loans became a reality. According to DeFiLlama, by June 2019 these protocols cumulatively had amassed a staggering figure of close to $500 million, a feat to behold at the time.

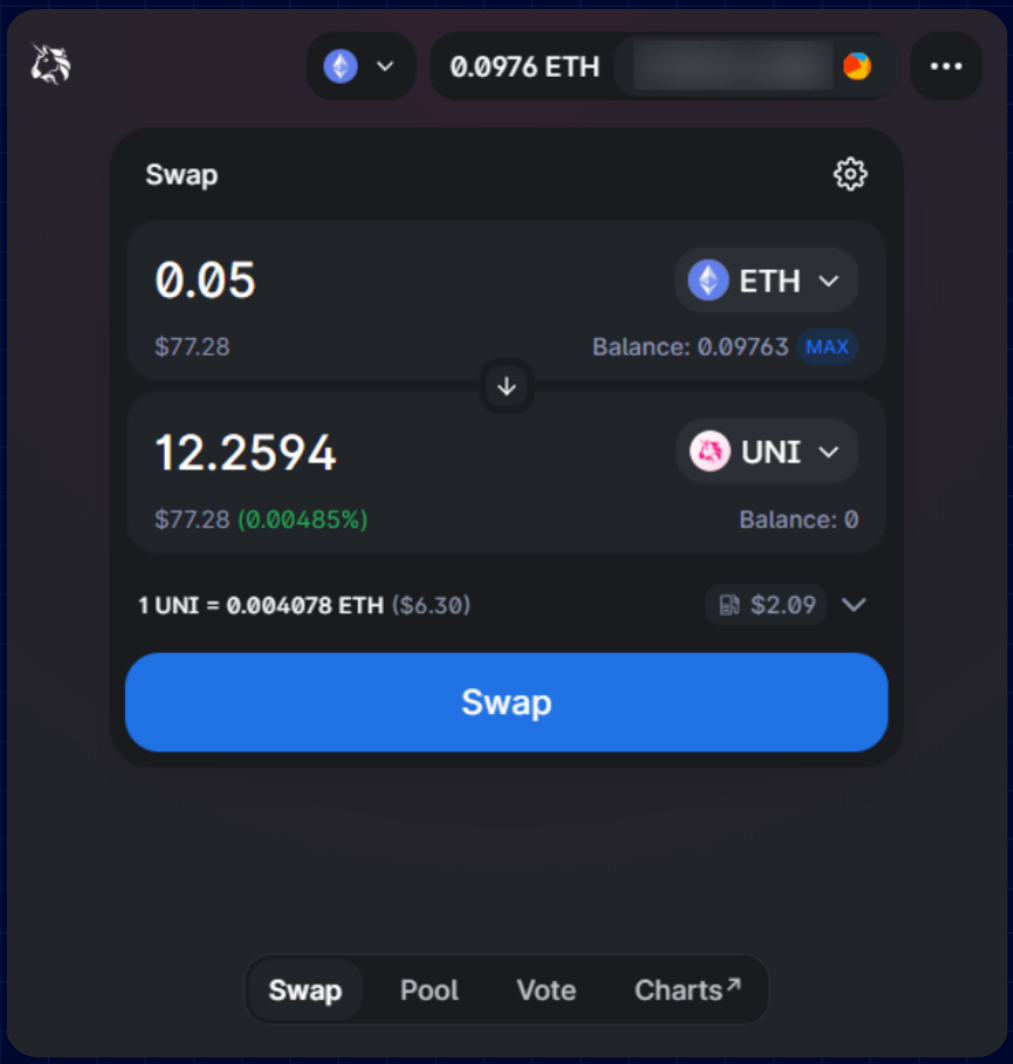
With that said, the idea of decentralized finance was not really a thing back then, it was simply a handful of smart contracts living on the Ethereum blockchain.

The term 'DeFi' was sort of a buzzword that was frequently thrown around as a glimpse into a hopeful future of a decentralized financial system. The monumental shift towards building DeFi really started with Uniswap in November of 2018.

The Birth of DeFi: Uniswap, the On-Chain Automated Market Maker

Building on top of Vitalik Buterin's thought experiment on decentralized exchanges, Uniswap launched as one of the first on-chain automated market maker protocols on Ethereum. Although Bancor first came up with the concept of liquidity pools, Uniswap popularized it for the masses with its famous 'x * y = k' constant product pool formula.

Uniswap V1's mission was simple, to provide an interface for users to seamlessly exchange ERC20 tokens on Ethereum. With its main focus on decentralization, censorship resistance and security, it effectively enabled Uniswap to create a safe and secure way for users to trustlessly trade their digital assets without a centralized custodian.



Source: Uniswap

Designed as a public good to push the industry forward, the Uniswap protocol's code is fully open source and there is no special treatment given to early investors, adopters or developers, no governance tokens or platform fees.

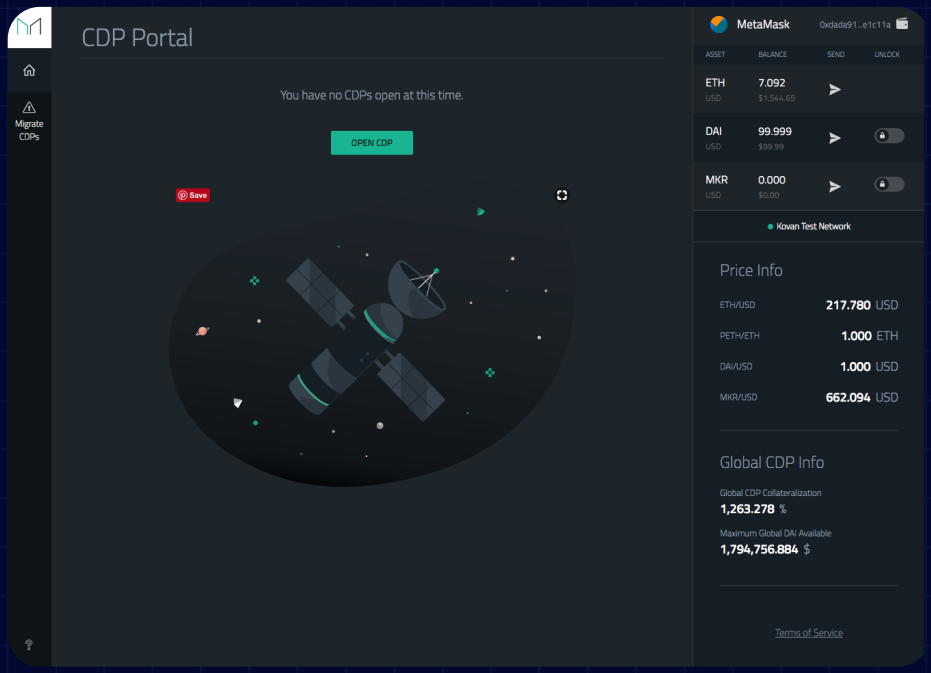
The choice to fully open source the Uniswap protocol's code has evidently shaped the decentralized exchanges of today, across a multitude of blockchain networks.

Enter Maker Protocol and DAI, the First Decentralized Stablecoin

The Maker Protocol platform enabled anyone to generate DAI, the first decentralized collateralized stablecoin collateralized against crypto assets such as ETH and BTC.

As the market value of cryptocurrencies typically experienced significant volatility, the need for stablecoins was clear. However at the time, the only market offerings were centralized stablecoins backed by the assets of centralized parties, which were exposed to custodial and regulatory risks.

In a decentralized economy, the product market fit for DAI was clear as it upheld the founding ethos of the crypto industry, censorship-resistance and decentralization.



Source: Maker Protocol

The protocol and its stablecoin has since gone through multiple iterations since its inception.

On 12 March 2020, a day referred to as Black Thursday, the price of ETH experienced a dramatic drop and fell more than 30% within 24 hours. This market volatility coupled together with Ethereum's rising gas fees put significant stress on the protocol, as many DAI vault owners had their vaults undercollateralized and liquidated.

At the same time, there were not enough liquidators bidding on liquidatable collateral as arbitrageurs paused operations amidst network congestion. This quickly led to stability issues as DAI depegged from its dollar peg and the price of MKR fell drastically by more than 50% in the same day.

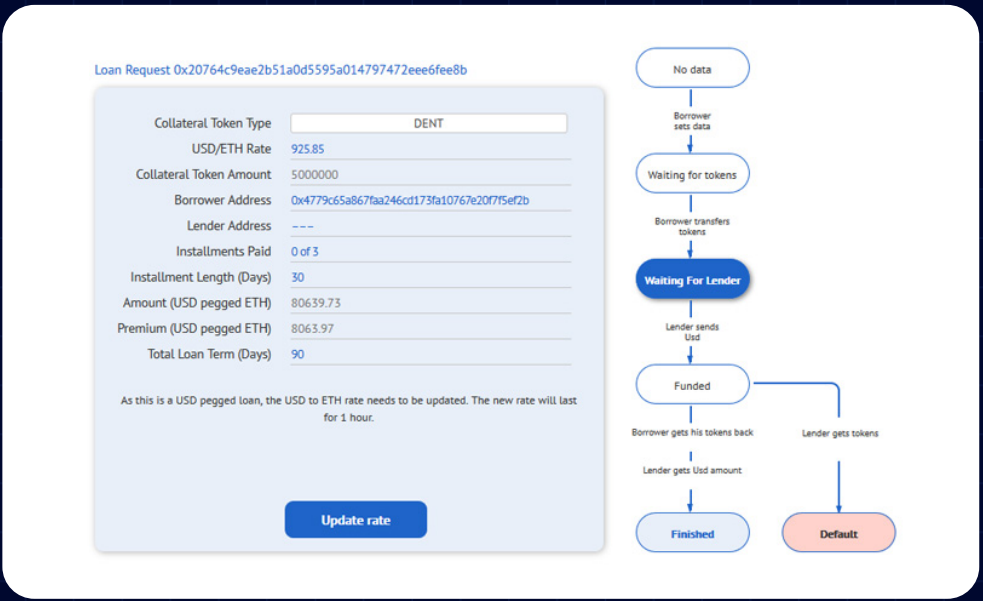
To save DAI, the MakerDAO community proposed adding USDC, a centralized stablecoin backed by Coinbase's Circle, as a collateral to mint DAI to provide more stability to the protocol and its DAI stablecoin.

While a controversial decision at the time, collateralizing USDC proved to be a good move to stop the bleeding and effectively saved the Maker Protocol.

Aave (ETHLend) & Compound: Pushing The Boundaries Of DeFi Lending

Launched in 2017, ETHLend was the first decentralized lending marketplace on Ethereum. As the first of its kind, the platform matched individual lenders and borrowers who wanted to partake in collateralized loan positions in a safe and secure manner.

To ensure its security and trustlessness, the platform utilized smart contracts on Ethereum to store user funds and their collaterals to facilitate peer-to-peer loan agreements. The platform opened a whole host of DeFi capabilities as traders were able to leverage or short crypto assets, while businesses and consumers could draw cash flow and liquidity without selling their underlying collateral.



Source: ETHLend

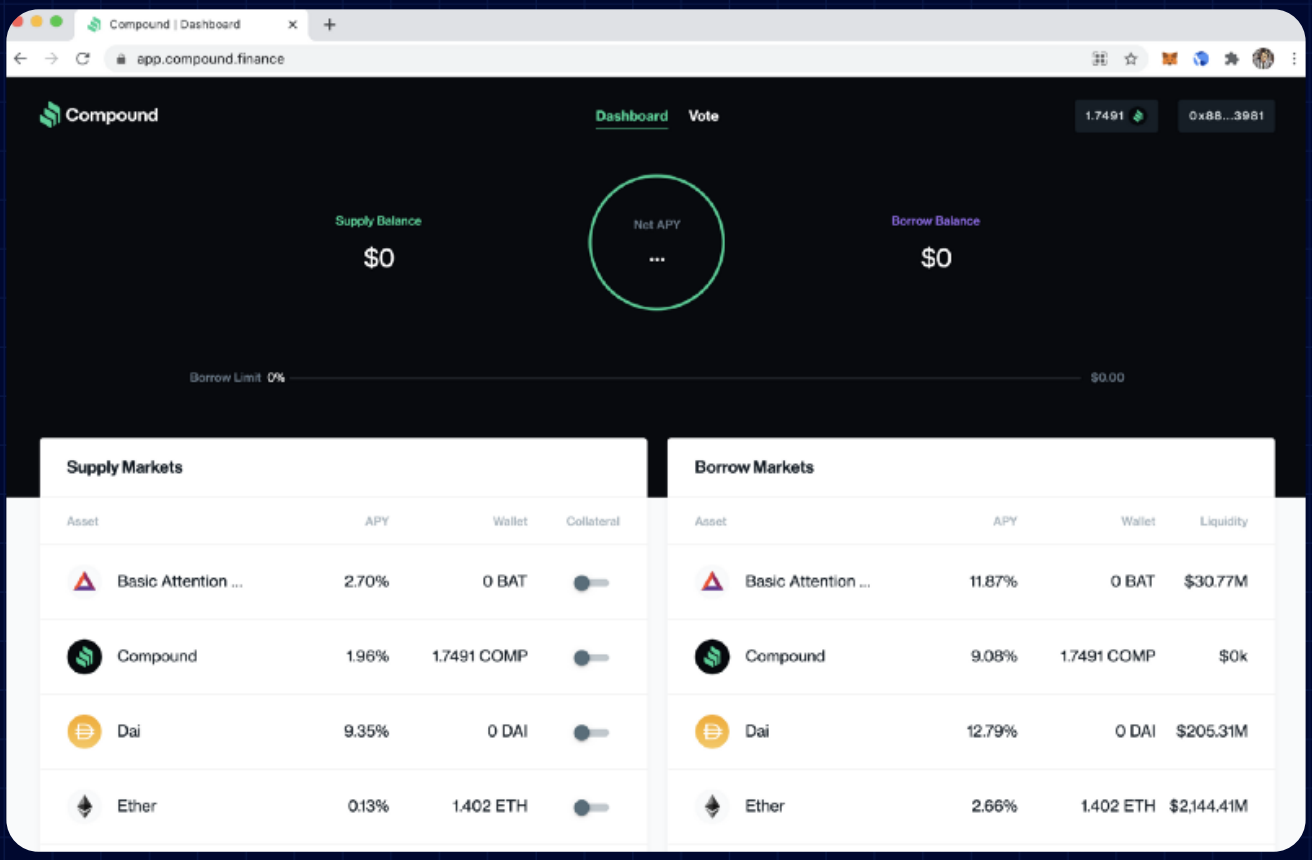
With that said, ETHLend had its limitations as its whole lending and borrowing process came with a lot of friction in terms of user experience. As a peer-to-peer protocol, lenders are required to post, manage and supervise loan offers and active loans. The whole process was often slow and tedious as loans had to be manually funded. Further, platform participants also lived around the world in different timezones, complicating the matter to a larger extent. If DeFi was the future of finance, this was definitely not it.

This was when Compound entered the picture.

In September of 2018, Compound launched its algorithmic and autonomous money market protocol on Ethereum, allowing anyone to frictionlessly earn interest on or borrow crypto assets in a trustless manner without having to interact with a counterparty. What made Compound stand out was its introduction of its peer-to-contract design and dynamic borrowing interest rates.

Instead of interacting with another user, lenders and borrowers only interacted with a lending pool, a smart contract reserve containing user-pooled assets. Each lending and borrowing market automatically calculates a supply and borrow rate which floats in real-time as market conditions adjust.

This allows Compound to effectively provide lenders and borrowers with efficient interest rates that react to market conditions.



Source: Compound Finance

Unlike a traditional credit intermediary where a borrower needs to negotiate a loan maturity along with a borrowing rate, Compound reimagined this service in a trustless and automated manner to make lending accessible to all, as well as allowing lenders to generate yield on their crypto assets.

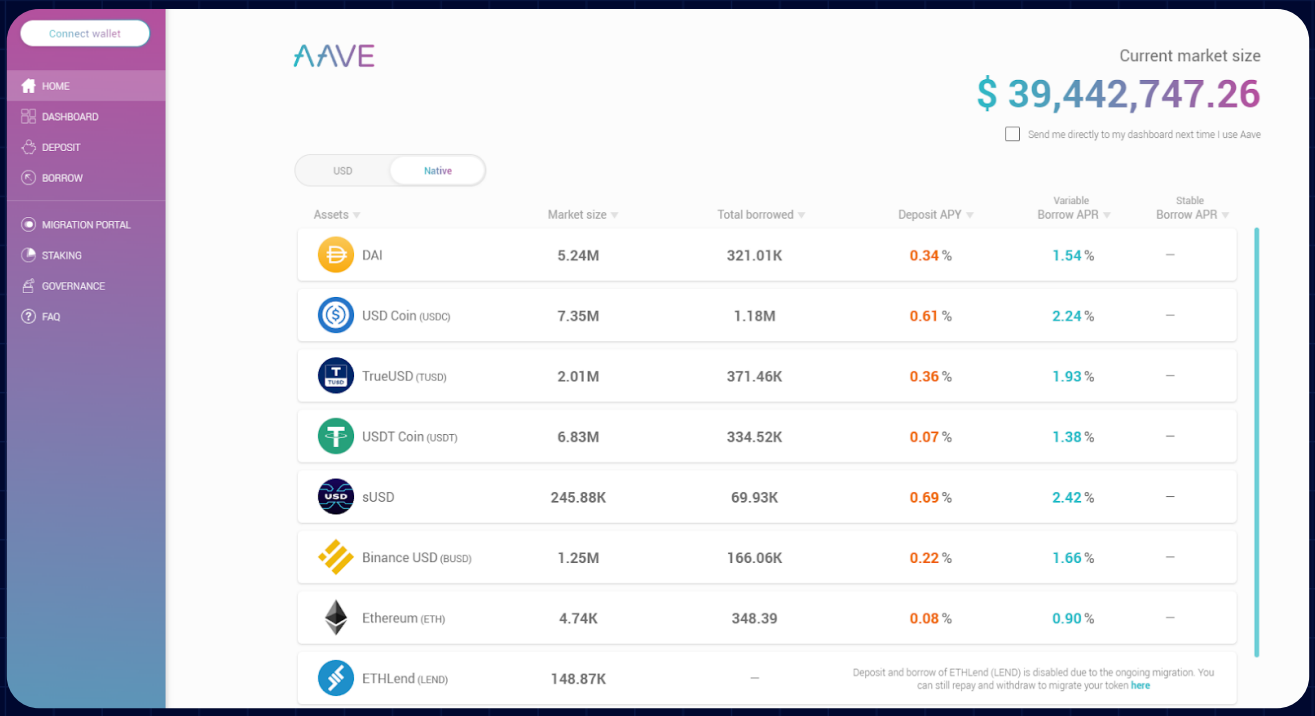
This pool-based model allowed loan positions to be opened in perpetuity as the borrower pays a borrow rate while the lender receives interest on their supplied assets. This dynamic is balanced by the loan-to-value (LTV) mechanism, a metric to measure a loan position's liquidation threshold.

As the protocol is fully open-sourced, Compound played an important role in pioneering the algorithmic on-chain money market protocol design in the decentralized economy.

Taking its learnings from Compound and shifting away from the decentralized peer-to-peer lending design, ETHLend eventually rebranded its platform to what is now famously known as Aave Protocol.

Like Compound, Aave's infrastructure is built on its pool-based vaults. However, Aave took DeFi lending a step further by introducing innovative features like flash loans, interest rate swaps, and liquidity provider tokenization.

The protocol has since gone through two upgrades and is now Aave V3.



Source: Aave V1

Whilst they may not have been aware of it at the time, Uniswap, MakerDAO, Aave and Compound were laying the foundations for the entire DeFi industry to come, and paving the way for many other household names that we know of today.

In fact, 2020 and 2021 were the years that shaped the nascent industry by leaps and bounds as many said names started pushing the boundaries of DeFi, growing it beyond what was first conceived just a few years back.

The Birth of Yield Farming

The COMP Governance Token

On February 27, 2020, Robert Leshner, founder of Compound announced the new COMP token as a way to introduce a new, community-led governance system that will replace Compound 's centralized administration.

This change effectively allowed COMP token holders to suggest, debate and implement changes to Compound without relying on, or requiring the project's team. The COMP token allowed token holders to delegate their voting rights to any ERC-20 address of their choice; essentially allowing others to vote on their behalf.

Source: Compound Finance

The COMP token, the first 'governance token' enabled anyone to have a stake in Compound and have an active say in the protocol's future plans. By design, the COMP token is distributed directly into the hands of its most important stakeholders, such as the users of the protocol.

This distribution empowers and incentivizes the protocol's community to collectively steward the protocol into the future through good governance. Unknowingly, this new design caused a monumental shift that would change the industry forever.

While initially meant for community governance, the distribution of COMP tokens marked a whole new paradigm shift as traders were able to speculate on the future worth of the Compound protocol.

In reality, users started using Compound for the sole purpose of farming its token, thus yield farming was born.

Shortly after its token generation event in June 2020, the COMP token spiked to a high of $336.22, a 399.51% increase from just 4 days prior. This price move launched the COMP token into the top 20 cryptocurrencies as measured by market cap.

Source: CoinMarketCap

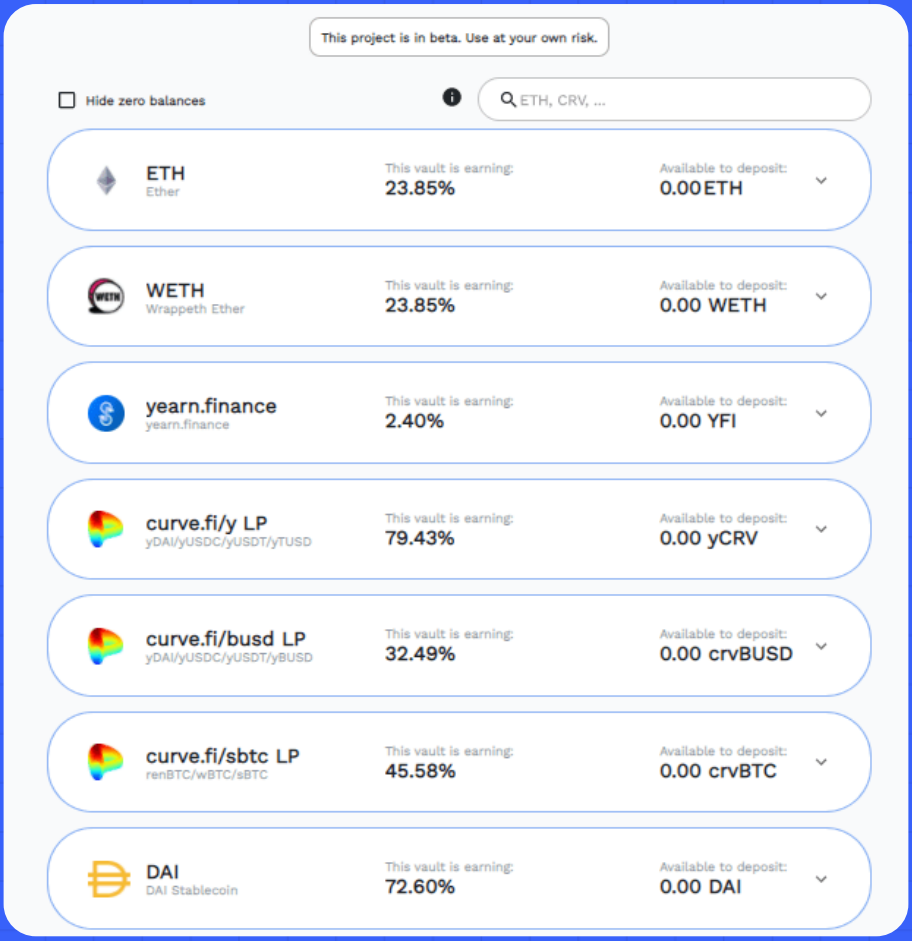
From a technological standpoint, this shift from centralized administration to community governance sparked various new innovations — from decentralized governance, to new ways to attract liquidity to the protocol. While already popular at the time, the Compound protocol's most active users greatly benefited from extremely high APYs in the form of COMP tokens.

This method would prove to be extremely successful as it attracted a lot of new users to the protocol. The protocol's pools were so popular that APYs would rapidly change by several percentage points every single minute. It came to a point where users who were actively hunting for the juiciest yields sought to automate the process of swapping their assets to the highest APY pools.

Andre Cronje's Yearn Finance

Enter Yearn Finance, the first yield farming aggregator in DeFi launched on July 17, 2020 by Fantom developer Andre Cronje. In order to optimize one's returns from yield farming opportunities, Yearn Finance acted as a shared vault where anyone can deposit their crypto assets into.

Vaults are capital pools which would automatically deploy capital into the best strategies to generate the highest yields for its depositors. In addition to generating the highest yield, these vaults benefit its users by socializing gas costs, automating the yield generation and rebalancing process, as well as automatically shifting capital as new opportunities arise.



Source: Yearn Finance

At the time, there were a few ways one could generate yield on their crypto assets. The most common ways include earning trading fees from providing liquidity to an asset pair on Uniswap or Curve Finance, or simply earning lending interest from supplying your assets to a lending platform like Compound or Aave.

This all changed when the incentivized liquidity wars began, Compound was the first one to start the mad rush with its COMP token. One by one, every DeFi protocol would introduce their own governance token and offer token emissions to the users of their protocols.

This made yield farming significantly more complex as yields became more lucrative. For example, users would supply DAI to Compound, deposit cDAI (the token representing the right to claim DAI from Compound) into Balancer, in order to earn COMP on the DAI, and BAL on the cDAI.

On top of that, this strategy would yield lending interest on the DAI and trading fees from the Balancer pool. Yearn Finance would simplify this process and turn it into a one-step solution for the passive investor.

Following in the footsteps of Compound, Yearn Finance launched its own YFI governance token. However, taking it a step further, Andre Cronje declared that the fair value of YFI is $0 as there was no token sale, all YFI tokens will be earned by the users of the platform.

Despite that, some argued that a token's value should be worth more or equal to the protocol's TVL.

Source: CoinMarketCap

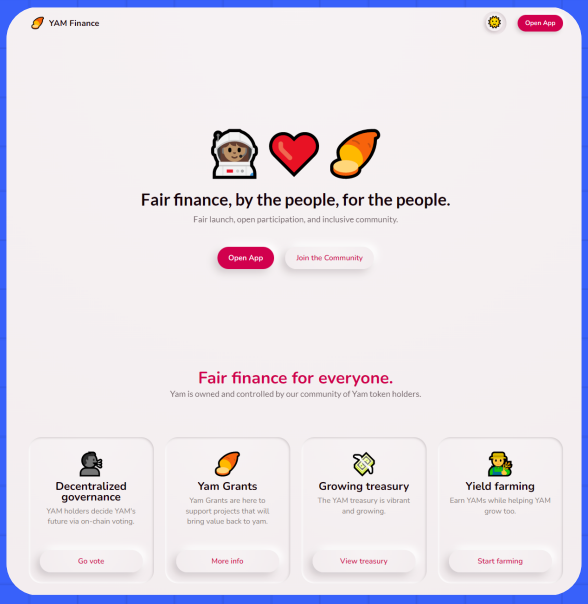
If applying the concept of comparing market cap to TVL, YFI was severely undervalued given the services it provided at the time. Coupled with its highly lucrative yields, the protocol garnered a significant increase in TVL leading to an astronomical increase in price.

From a starting point of $0, Yearn's governance token YFI charged to a high of over $43,000 just 2 months later from its launch, definitely a sight to behold.

YAM and the Food Farms

Yield farming created a mad rush of liquidity chasing the highest yields in the most degenerate fashion. However, no one could predict what was about to happen next.

What started as a convergence between cryptocurrencies and accessible financial products quickly devolved into a subculture of meme coin food-themed yield farms.



Source: Yam Finance

Launched as a monetary experiment, Yam Finance explored various DeFi concepts such as elastic supply tokens, protocol treasury governance, fair token distribution mechanisms and fully on-chain governance from its inception. Named after the starchy tuberous root, YAM, the protocol's governance token was evenly distributed across eight staking pools (COMP, LEND, LINK, MKR, SNX, wETH, YFI and ETH/AMPL LP) to reach the overall DeFi community.

In less than 48 hours, the yield farming protocol garnered over $600 million in TVL with its highly lucrative yields and subsequently kickstarted the DeFi food farm frenzy. One by one, sprouting out of thin air, you'd see 'delicious' names like Pickle Finance, Cream Finance, Beefy.Finance, Kimchi, BurgerSwap, Tendies and the list goes on.

One would think that this was a sign of bull market peak euphoria but degens being degens, they aped in anyway. Unfortunately, a critical bug was found in YAM's token which led to over-minting and the eventual demise of the token's price, causing over $500 million of wealth destruction.

Likewise, many other food farms and forks of Yam Finance suffered a similar fate

SushiSwap: The Uniswap Spinoff

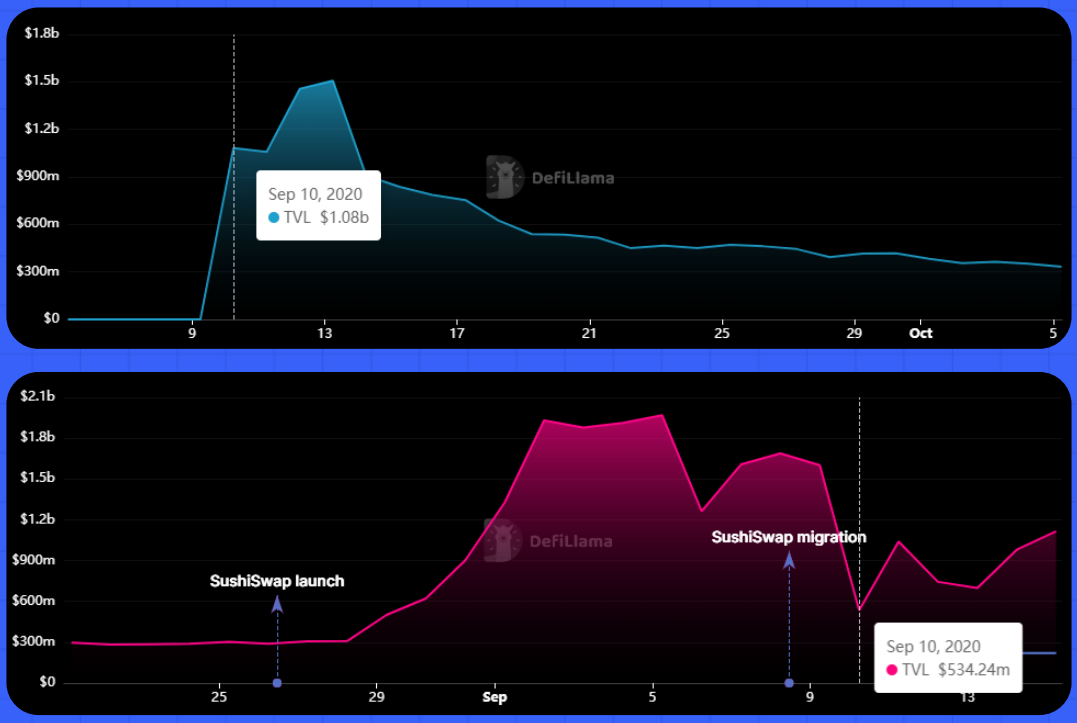
Through the banquet table of Yam forks, food rugs and questionable delectables, there stood one protocol that made waves within the DeFi community. SushiSwap, a simple spinoff of Uniswap launched back in August 2020 allowed users to stake their Uniswap LP tokens on the SushiSwap platform to earn SUSHI governance tokens.

However, SushiSwap's creator Chef Nomi took it a step further and revealed plans to redeem those Uniswap LP tokens for new LP tokens that would be transferred over to SushiSwap. Widely known as the 'vampire attack', this novel technique allowed SushiSwap to draw significant amounts of liquidity from Uniswap to bootstrap its own liquidity pools.

Source: SushiSwap

As Uniswap did not have a governance token at the time, SushiSwap's approach proved to be highly effective. Uniswap liquidity providers chased after the highest yielding opportunities on their LP tokens as they could earn SUSHI tokens.

On the day of the LP token migration to SushiSwap, the protocol rapidly garnered massive amounts of TVL from Uniswap's liquidity pools to the tune of over $1 billion. On the other hand, Uniswap experienced a mass exodus of TVL of equivalent proportions, the protocol's TVL quickly fell to $534.24 million from a high of over $1.6 billion.



Source: DeFiLlama (TVL, 1st Image = SushiSwap, 2nd Image = Uniswap)

While closing in on the designated liquidity migration date in September 2020, SUSHI's price tanked significantly by over 70% in a day as its creator, Chef Nomi, drained the SushiSwap protocol's development fund, swapping it for 37,400 ETH worth about $14 million at the time.

Chef Nomi faced heavy pressure and backlash as Nomi's actions were publicly seen as a betrayal of the SushiSwap community. Caving into the community's demands, Chef Nomi handed over SushiSwap's smart contract private keys to FTX's CEO Sam Bankman-Fried who proceeded to postpone the liquidity migration to September 9, 2020.

Not long after the event successfully migrated over $800 million of liquidity from Uniswap, Chef Nomi voluntarily returned the ETH to the community out of guilt and subsequently made a public apology for his actions. A week later, FTX's Bankman-Fried returned the SushiSwap protocol to its community following the implementation of a multisig to prevent a sole bad actor from having full control of the protocol.

Despite the drama, SushiSwap's aggressive liquidity mining incentives and launch approach inspired many future projects as the fight for TVL became increasingly difficult in an ever-growing DeFi ecosystem.

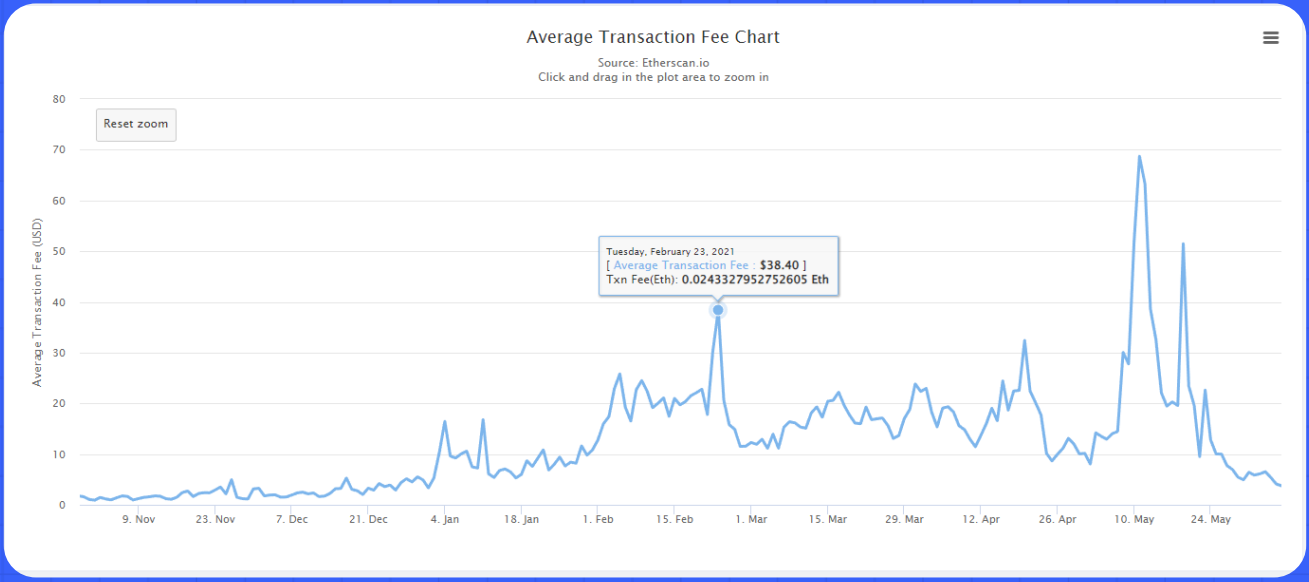
Ethereum Scalability & The L1 Arms Race

The Consequential Blockchain Scaling Problem

Towards the end of 2020's DeFi summer and moving into 2021, Ethereum's DeFi ecosystem was flourishing, with countless number of decentralized applications deploying on mainnet.

ETH's price buoyed to new highs, going from as low as $150 in May 2021 to a peak of $4100 just one year later. As users explored Ethereum's DeFi ecosystem, on-chain activity continued to accelerate and Ethereum's gas fees started to become increasingly more prohibitive, sometimes costing more than $30 in ETH for a simple swap transaction on Uniswap.

Adding to that, the non-fungible token (NFT) market was starting to heat up and gain traction, as OpenSea and CryptoPunks stole the limelight in terms of sales volume and price action. On a daily basis, OpenSea would consistently rank among the top ETH gas guzzlers on Etherscan.

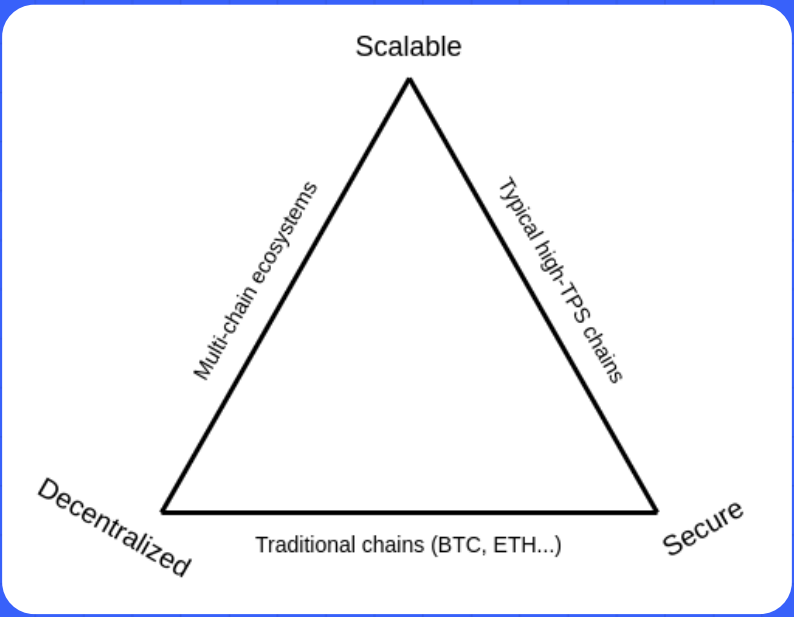


Source: Etherscan (Average Transaction Fees on Ethereum)

According to Vitalik Buterin, creator of Ethereum, every blockchain should strive to achieve three key properties: decentralization, security and scalability. However, sticking to simple techniques, one can only achieve two of the three, hence what he calls the 'Blockchain Scalability Trilemma'.

At the time, it was clear that Ethereum needed to scale. However, Layer 2 scaling solutions like optimistic rollups and zero-knowledge rollups were not ready yet, and were still very much in the developmental phase.

At some point, and after it became relatively inaccessible and expensive to the average retail user, capital started to migrate away from Ethereum to greener pastures like Binance Smart Chain, Polygon, Solana, Avalanche, Fantom and Terra, kicking off the alternative Layer 1 blockchain narrative into full turbo.



Source: Vitalik Buterin

The Layer 1 Blockchain Arms Race

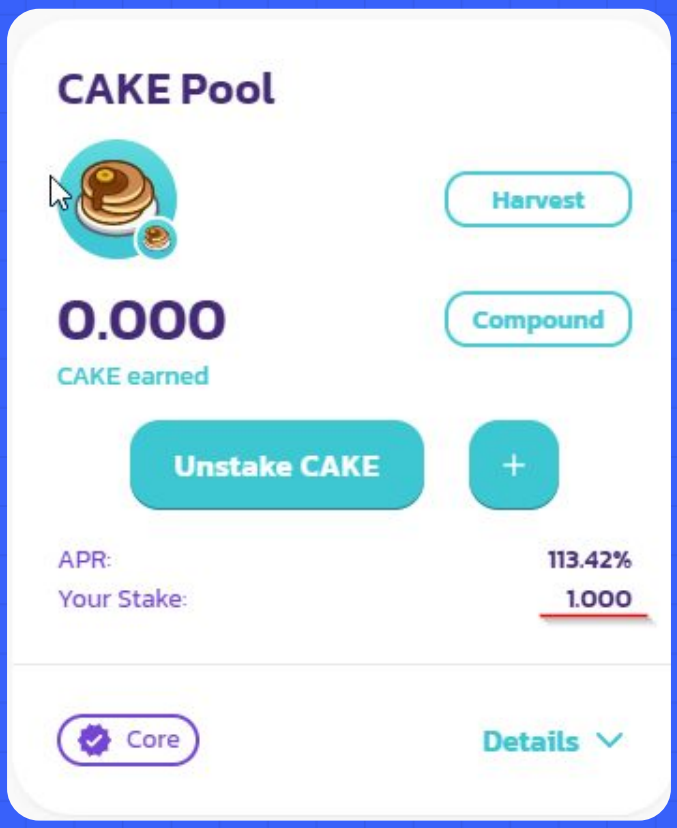
One by one, each Layer 1 blockchain ecosystem's foundation announced their own liquidity mining incentives and builder grant programs to attract both developers and users alike.

Binance kicked off the frenzy when it announced its $100 million support fund for DeFi projects on Binance Smart Chain (BSC). Although its effect was not immediate in terms of price action, in February 2021 on-chain activity on the BSC chain started gaining traction as the price of BNB shot up from $40 to a peak of $686 in just 4 months.

Source: CoinMarketCap

Developers coming over to this new ecosystem quickly realized that they did not need to reinvent the wheel. As Ethereum already had a number of successful applications that found their product market fit, developers would fork and rebrand them on BSC to quickly gain TVL and market share in the new ecosystem in hopes of getting a slice of the $100 million incentive pie.

Oddly enough, the most successful application (in terms of market share) happens to be a Uniswap fork as well as a delicious food farm, the famous PancakeSwap. While not entirely a copy-and-paste, PancakeSwap solidified itself as a core decentralized exchange on BSC, with added features like staking-as-a-service, yield farming, a launchpad as well as prediction markets.

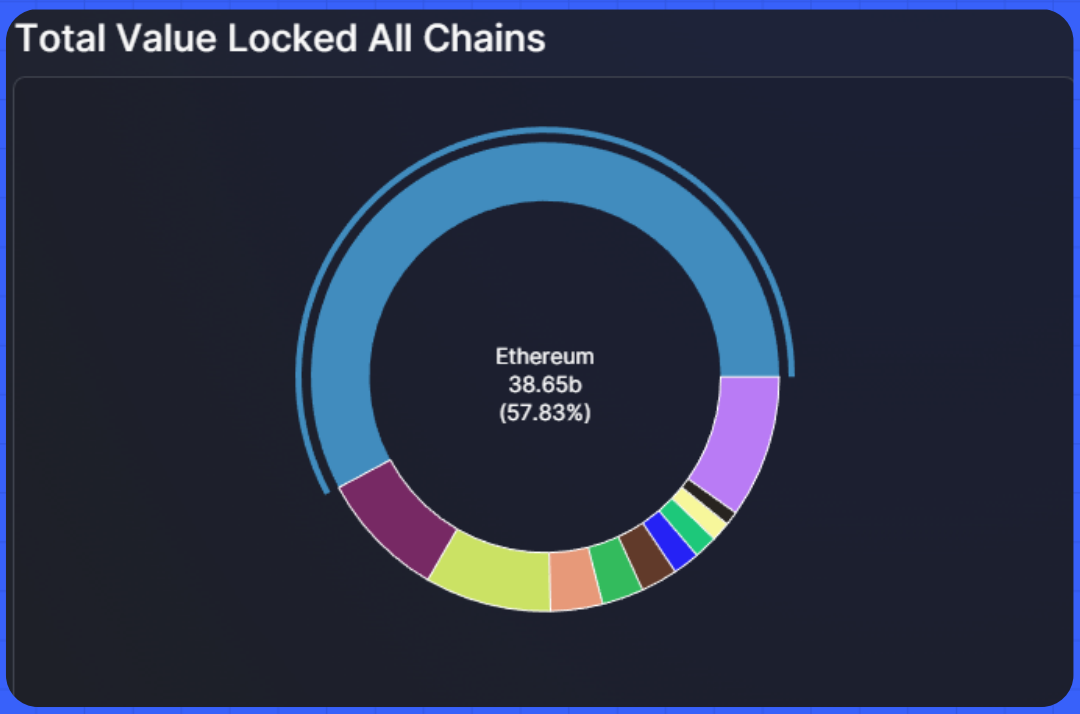


Source: PancakeSwap

The narrative that Ethereum was unable to scale was strong enough that every one of the major Layer 1 ecosystems had its own heyday as liquidity mining incentives were thrown around in typical bull market fashion.

Similar to what happened on BSC, developers would replicate the same strategy by pushing out DeFi applications in the fastest time possible to acquire the most market share and TVL to be eligible for ecosystem grants. Although non-Ethereum virtual machine (EVM) chains like Solana and Terra were not able to fork Ethereum applications due to differences in codebases, many new protocols built upon the design architectures of existing DeFi solutions.

As most younger ecosystems were missing key DeFi primitives such as decentralized exchanges, lending markets, yield aggregators, stablecoins and cross-chain bridges, there was an abundance of opportunities for the taking.



Source: DeFiLlama

This trend continued throughout 2021 into 2022 as DeFi degens hopped from one ecosystem to the next to take advantage of liquidity mining rewards. Crypto Twitter frequently referred to this as the 'L1 Rotation' and even coined the term 'SoLunAvax' with reference to the Solana, Terra and Avalanche Layer 1 rotational play.

As the TVL market share of Ethereum's DeFi was slowly being eaten away by newer ecosystems which offered cheaper fees, faster transaction finality and an overall more user-friendly experience, many applications from the first generation of DeFi like Uniswap, Aave and Curve Finance were forced to expand their reach into newer blockchain ecosystems.

Ultimately, this narrative shift further validated the thesis of a multichain future. Sovereign Layer 1 blockchains were more interconnected than ever through the creation and expansion of cross-chain applications and asset bridges.

However, with reference to Vitalik Buterin's concept of the Scalability Trilemma previously mentioned, these newer Layer 1 blockchains were not without their own issues and growing pains, as varying degrees of decentralization and security were sacrificed for speed and scalability.

With that said, the birth of multiple DeFi ecosystems meant that a significant amount of load was taken off from Ethereum's mainnet, inevitably reducing network congestion.

Interoperability: A Multichain Future

Following the rise of younger blockchains, it became apparent that these ecosystems started to become more isolated from one another. While already a nascent industry, DeFi protocols operating in newer blockchain ecosystems experienced considerable difficulty in garnering liquidity as well as user adoption. Interoperability is a key part of the future of blockchain technology as well as an essential piece of infrastructure for DeFi.

As the number of projects and use cases grows, so does the need for interoperability between blockchains. Interoperability will enable a multichain ecosystem where different chains can communicate with each other, allowing them to collaborate and share data in real time, both from an economic and technological standpoint.

A number of companies and teams are already working toward this goal by creating solutions that allow one blockchain to communicate with another, whether directly or indirectly through a third party. From a high level, interoperable solutions can be broken down into two distinct categories: (a) Patch Solutions retroactively built on Non-Interoperable Ecosystems, and (b) Natively Interoperable Solutions.

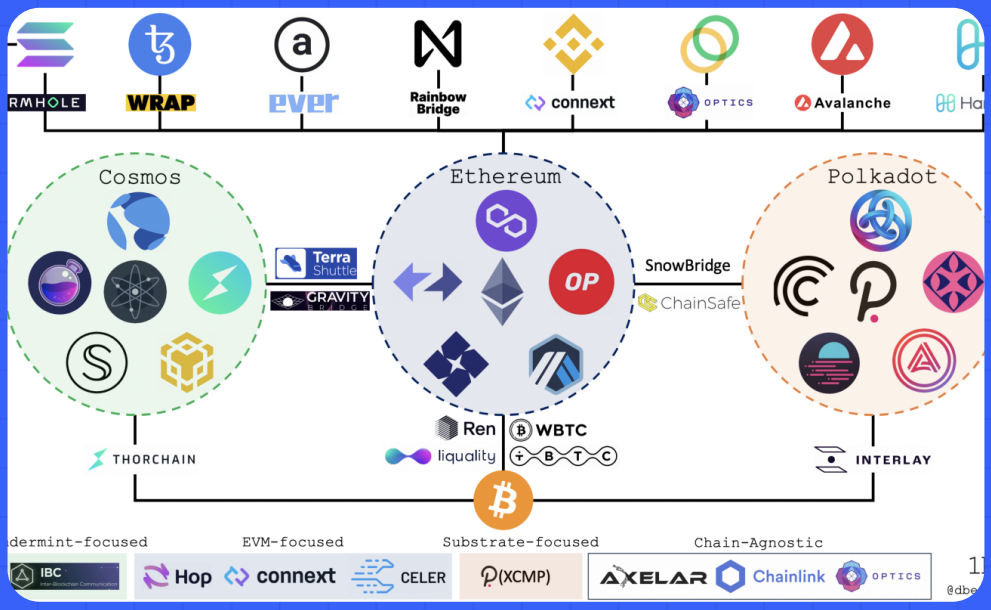
To elaborate further, patch solutions retroactively built on non-interoperable ecosystems refer to interoperable solutions built on top of existing chains which are not built for interoperability. These can be further distilled down into solutions like Centralized Exchanges and Cross-Chain Asset Bridges.

Source: Binance

Centralized exchanges are the most commonly used type of crypto exchange as they can be thought of as the "traditional" way to trade cryptocurrencies. In a centralized exchange, users deposit their funds into an account controlled by the exchange itself. The exchange then keeps track of all trades in central order books and holds the money in escrow until it's time for an on-chain transaction to take place.

While this allows for a fast and easy trading user experience between different cryptocurrencies regardless of blockchain network, this form of off-chain interoperability adds multiple layers of complexity as these platforms are subject to stringent regulation. For centralized exchanges to serve its clients, the exchange must comply with each country's own laws and jurisdiction, most times requiring customers to verify their personal identity through a Know-Your-Customer (KYC) process before allowing users to withdraw their assets on-chain and regain custody of their funds.

Inadvertently, this exposes users to counterparty and credit risk as the exchange can withhold users' funds at any given time in the event of liquidity issues or even insolvency.



Source: Dmitriy Berenzon, September 8, 2021

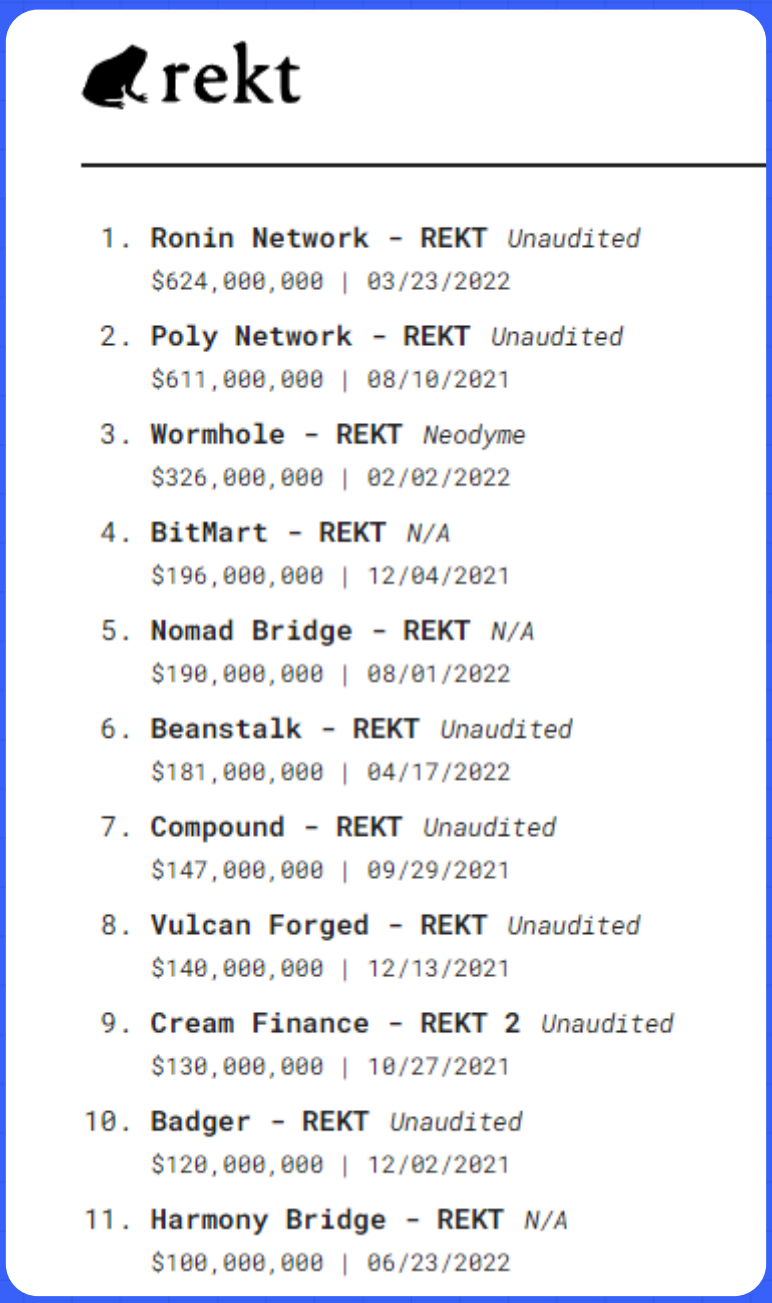
In terms of on-chain interoperability, the image above depicts how blockchains are connected to one another as of September 2021. In line with the core tenets of decentralization, cross-chain asset bridges like Wrapped BTC, Multichain (previously AnySwap) and Portal (previously Wormhole Bridge) opt for a more permissionless approach. These solutions are built according to similar design architectures which enables users to transfer their crypto assets from one chain to another in a trustless manner.

Cross-chain asset bridges typically operate on a 'lock-and-mint' mechanism whereby assets on a source chain are locked in the bridge's smart contract vault, and redeemable 'wrapped' versions of the native assets are minted on a destination chain.

The rationale for this design is because native assets from one chain cannot natively exist on other sovereign blockchains, thus these newly minted wrapped assets which are pegged in value on the destination chain can inversely be burned and redeemed for the equivalent native assets on the source chain.

Whilst still the most used form of interoperability with over $12 billion in TVL, cross-chain asset bridges have been the prime target of many hacks and exploits due to the sheer amount of funds locked within them.

In the past two years alone, over $1.85 billion in pooled funds have been siphoned away by hackers from a handful of high profile incidents such as the Ronin Network and Wormhole bridge hacks, both losing $624 million and $326 million respectively.



Source: Rekt News - Leaderboard

While most cross-chain bridges normally function in a similar fashion, there are some variations in each design, with some structurally more centralized than others and subject to additional flaws like the risk of censorship and poor liquidity. Despite these discrepancies, blockchain security experts at Halborn found that most blockchain bridge hacks target a few specific attack vectors which are typically designed to cause tokens to be released on one blockchain without a corresponding deposit on the other. In recent history, exploits have been carried out in a few main ways:

1. False Deposit Events:

   Cross-chain bridges frequently keep an eye out for deposit events on one blockchain in order to start a transfer to the other. An attacker can take money out of the bridge at the other end if they can create a deposit event without making a valid deposit or by making a deposit with a token that has no value.

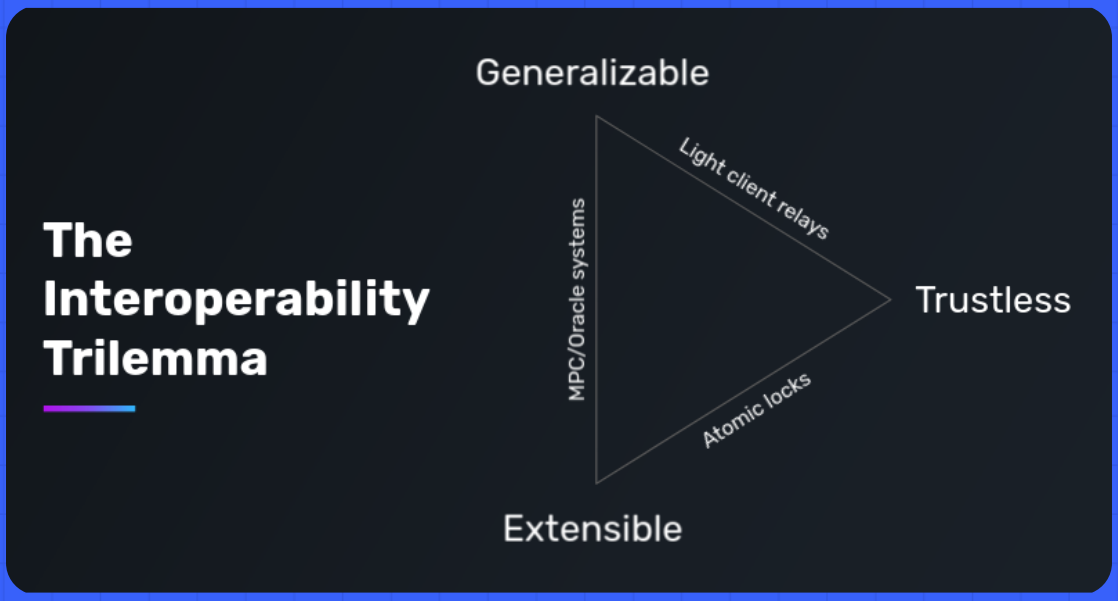
2. Fake Deposits:

   Each deposit is validated by the cross-chain bridge before said transfer is approved. This validation procedure can be tricked if an attacker can make a false deposit that verifies as a real one. This was the case with the Wormhole incident, where $326 million was stolen by the hacker who took advantage of a weakness in the validation of digital signatures.

3. Validator Takeover:

   Depending on how the bridge is set up, a set of validators on some cross-chain bridges cast votes to approve or disapprove a specific transfer. The attacker can authorize fictitious and harmful transfers if they have control over the majority of these validators. In the Ronin Network exploit, the attacker acquired control of 5 of the bridge's 9 validators enabling the withdrawal of funds from the bridge's smart contract.

Despite the amount of code audits and security measures undertaken by bridge operators, the nature of cross-chain bridges creates a complex environment which exposes itself to a multitude of risks. With the number of vulnerabilities faced by centralized exchanges and cross-chain asset bridges mentioned above, it is clear that natively interoperable solutions are required in building a multichain future.



Source: Connext - Arjun Bhuptani

While many teams have recently stepped up to the challenge and have pursued more innovative methods, building interoperability solutions is no easy feat. Similar to Vitalik Buterin's Scalability Trilemma; there exists an Interoperability Trilemma. As described by Connext's founder, Arjun Bhuptani, interoperability protocols can only have two of the following properties, usually compromising on one or more properties in pursuit of the others:

1. Trustlessness refers to having equivalent security to the underlying blockchain.

2. Extensibility refers to the ability to be easily integrated on any blockchain.

3. Generalizability refers to the capability of handling more complex cross-chain data.

As of the time of writing, many new native interoperable solutions have opted to use more sophisticated methods in an attempt to achieve all three properties above. Projects like THORChain have opted to build its own decentralized liquidity network that acts as a full chain decentralized exchange (DEX) which results in depeg risks being offloaded to individual liquidity pool providers; interoperability hubs like Cosmos and Polkadot pioneered the idea of homogeneous "network of networks" as they act as the base layer 0 of an interoperable network of multiple Layer 1 blockchains.

Despite the more complex designs, these protocols have had varying degrees of success in terms of user adoption and garnering more market share.

However, the most recent interoperability designs seem to be the most promising with their elegant and scalable approaches. Going far beyond wrapped assets and centralized systems, cross-chain communication protocols like LayerZero, Axelar Network and Router Protocol cuts out a lot of moving parts and attack vectors in comparison to traditional bridge designs through the idea of relaying both generic and complex data using a mixture of nodes, relayers and oracles to establish fast, cost-efficient and
decentralized inter-blockchain communication while not compromising on security.

While not as widely adopted as its predecessors, these newer solutions built with interoperability in mind seem to be a promising advancement towards building a multichain future and solving the interoperability trilemma.

Troubled Waters, and a Way Forward

From this point on, however, and as we entered into 2022, things started to go awry for the broader crypto market at large as several unfortunate events unfolded.

First, there was the (not so little) problem of rising inflation from all the printing that went on because of the COVID situation that came to plague the past 2 to 3 years. Geopolitically, there was also a lot of tension and fears due to the Russia-Ukraine War that broke out in February of this year. All these culminated in great macroeconomic instability, as the U.S. Federal Reserve eventually turned to interest rate hikes in their fight against inflation, triggering market fears of a looming recession.

Flowing from this, and very unsurprisingly, the global markets all suffered large downturns; the S&P 500 drew down by quite a substantial level, the broader crypto market similarly plummeted, whilst the DeFi market also took quite a huge hit.

The bad news didn't stop here. Murphy's Law dictates that anything that can go wrong will go wrong, and at the worst possible time. This adage couldn't have been more relevant for the crypto market.

As market participants were just coming to terms with the aforementioned macroeconomic catalysts, the proverbial final nail in the coffin was drilled into the crypto market from the inside. One of the space's most beloved darlings at the time, UST, suffered an unfortunate depeg. This led to an Anchor bank run, before Terra ultimately and inevitably collapsed from hyperinflation, rounding up a massive $60 billion blow-up with aplomb. Terra's caving-in had severe repercussions for the space at large.

From here, 3AC, one of the largest players within the industry at the point of time, found themselves blowing up. Huge CeFi lenders like Celsius, BlockFi, Babel and Voyager also crumbled from the contagion of Terra's and 3AC's falls. As CeFi lenders were forced to repay DeFi lending protocols like MakerDAO and Aave in order to unlock their collateral, stETH started trading at a discount from ETH due to all the forced selling, exacerbating the market situation further.

As the total crypto market cap collapsed, we also saw DeFi's total market cap take a whopping 75% plunge in Q2 of 2022 as TVL started to rapidly exit the ecosystem. Whilst total DeFi market cap has since been restored to some extent, the road to full recovery is still a long and arduous one.

Where do we exactly go from here?

Terra's high profile collapse, though extremely unfortunate, was helpful in unearthing the fragility of the algorithmic stablecoin model, as well as the need for more sustainable tokenomics within the larger DeFi ecosystem. This pointed a way forward for DeFi.

The act of printing stablecoins out of thin air worked wonders while it lasted but alas — it was anything but sustainable.

Afterall, and as a very solemn reminder of the above, Terra crumbled in a mere matter of days the moment UST lost its peg, and subsequently death spiraled from $1 to $0.12 between the 9th and 14th of May of 2022.

It was clear that something had to radically change. The DeFi ecosystem should not be propped up on ultra-mercenary capital that leaves the moment anything untoward happens. That is simply not wise if we want a DeFi ecosystem that is vibrant, robust, and most importantly — sustainable through the cycles. If sustainability isn't there, the DeFi ecosystem will never be substantive in any meaningful way too.

DeFi: Reborn

Here at Spartan Labs Research, we see a clear way forward for DeFi, at least in the near-to-mid-term.

Caveat: a rebirth does not equate to a boom; the two are necessarily mutually exclusive. Hence, neither Spartan Labs nor CoinMarketCap are claiming that DeFi will experience a boom in the months to come. Instead, these are simply, in our opinion, several steps that the ecosystem should take to move forward from the lessons learned in the past.

For the DeFi ecosystem to bounce back stronger from the relative lows that it is currently mired in, and for it to truly learn from the lessons of the past, there are three main pivots and progressions that must take place.

First, **all given DeFi protocols should necessarily prioritize their own sustainable cash flow-generation capacities to a much larger extent.** In the past year or two, most DeFi projects were (in large part due to all the extreme euphoria generated by the bull cycle) very much overtly focused on the user-acquisition/TVL bootstrapping aspect of their roadmaps and operations. However, and in the wake of the bull cycle, we are starting to realize now that this might not be the best strategy for the long-term sustainability and overall longevity of DeFi protocols in general. This is something that we will elucidate further in the next section.

Next, **the tokenomics models that have come to dominate the DeFi space must also evolve to adapt to the changing/changed times.** Instead of liminal mercenary capital, protocols must learn (through their tokenomics strategies) to attract the appropriate user-base that are aligned with their respective long-term goals and visions.

Finally, we also believe that **the rise of synthetic assets will power the DeFi space forward and sustain it to a large extent in the many years to come.** After all, the derivatives space is one that is still very much largely untapped when it comes to DeFi and web3. With the rise of synthetic assets, perhaps the potential of this DeFi sub-vertical can be maximized to the point that it should really have been.

A Shift Towards Sustainable Cash Flow-Generating Protocols

Witnessing the full meltdowns of LUNA and UST, both of which (at that point) ranked within the top 10 list of coins by market cap, within a matter of days severely shook the confidence of the general market. The fear, uncertainty and doubt lingering within the market (even till today) triggered a massive shift in narrative with regard to what a desirable DeFi protocol should be like. Investors no longer blindly craved ponzi-like yields and functionalities that promised absurdly high rewards if they worked.

Instead, investors started to cast their eyes on true stability and sustainability to ensure that their token investments would be able to withstand the volatile market conditions that have come to define the crypto/DeFi market, while still providing decent returns that could outpace traditional markets.

As such, whilst DeFi in 2021 and the earlier part of 2022 was largely defined by insanely high APRs (think Olympus DAO, Wonderland) and the rise and subsequent fall of liquidity mining incentives, both of which were specifically geared for large-scale user-acquisition, many are now realizing that the real key (for both users and builders) is found in strategies of user-retention, something that both aforementioned models lacked.

For builders, it should now no longer be merely about getting truckloads of users onto your platforms and protocols. Whilst important, it should not be the only thing being prioritized by projects. What happens **after** the users are acquired is extremely vital too, as that basically is what and why the users are brought in for in the first place. The key question has now become: how do projects and protocols retain the users that they have on-boarded by the masses? How do they create a form of stickiness, and a moat, around said users?

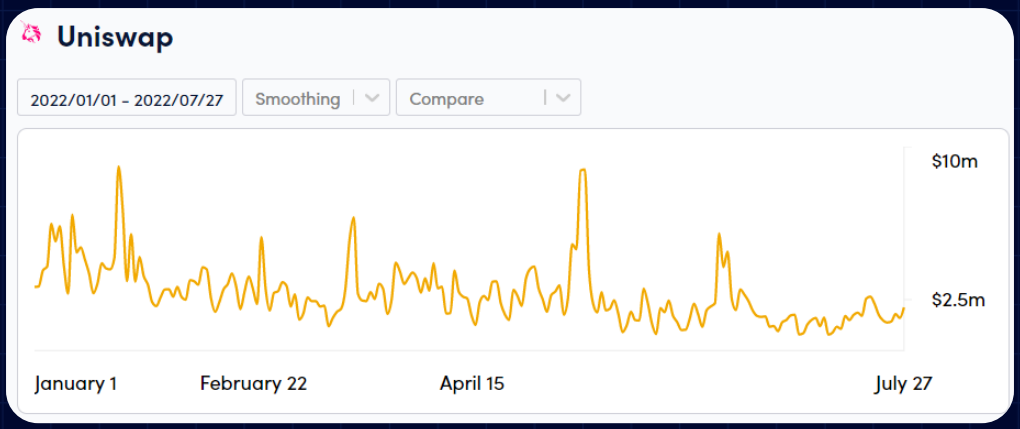
For users, it should now no longer be merely about the lofty promises of high returns and yield without the financial numbers to substantively show for them. In recent times, it has been proven that said lofty promises are too easily (and have been too often) broken by project owners the moment anything remotely turns south. It is now on projects to prove that the returns and yield they are touting are possible and sustainable because of their extant operation, and users should definitely be rigorous about this before even considering any form of investment(s) into said project(s).

At this juncture, a brief aside: the insanely high APRs and liquidity mining incentives that we mentioned above have been criticized as "ponzinomics" by many within and outside of the crypto space. While we do see why they have been criticized as such, we humbly beg to differ. For all intents and purposes, the term "ponzi" is loaded with meaning that belies an intentionality to defraud. To label all DeFi protocols that promised high yield a "ponzi" would be unfair to those that had every intention to provide substantive value to their users, but failed to do so because of the mercenary-nature of the capital that they attracted. Granted, there were definitely some that were built with intentions to defraud (rug), but to be so sweeping about it would be inappropriate.

Going back to the main point, the overt shift in focus towards user-retention (through true value generation) has led to the rise of revenue-generating protocols that, for some like UNI and AAVE, was a second coming of sorts.

It has become clear that users are now looking to invest in substantive value, no longer promised ones. This largely meant operations that are able to generate and accrue fees in a consistent and sustainable manner.
Below, we will explore several protocols that are already doing so, and that others should learn from and/or model after in their bids to be a part of the larger DeFi ecosystem.

Uniswap (UNI), the King of Fee Generation



As the first AMM on Ethereum and the undisputed leader in terms of fees generation, Uniswap has revolutionized how liquidity provision (LP) works by allowing users to provide liquidity within custom price ranges at differing fees tiers.

With an average of $1.6-3M in fees per day in 2022 (as of the time of writing), Uniswap has done exceedingly well to generate various streams of steady revenue considering the turbulent market conditions.

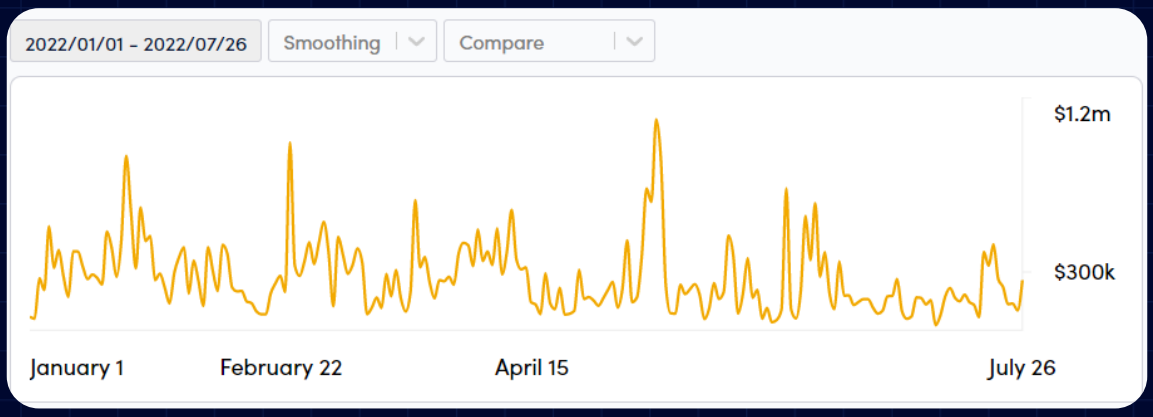
The fees accrued by the protocol are all paid out to LP users, with protocol fees still currently set at zero.

AAVE, the Largest Cross-Chain Money Market

Next, another protocol that has managed to churn out some real substantive value through a stable accrual of fees would be AAVE, the largest cross-chain money market with $6.3b in TVL.

While centralized money markets like Celsius and Voyager ultimately collapsed during this market downturn, AAVE has withstood the test of time, and remains fully functional. In fact, it is even steadily accruing approximately $700-900K in fees on a daily basis for 2022 (as of the time of writing).

GMX, a Rising Star

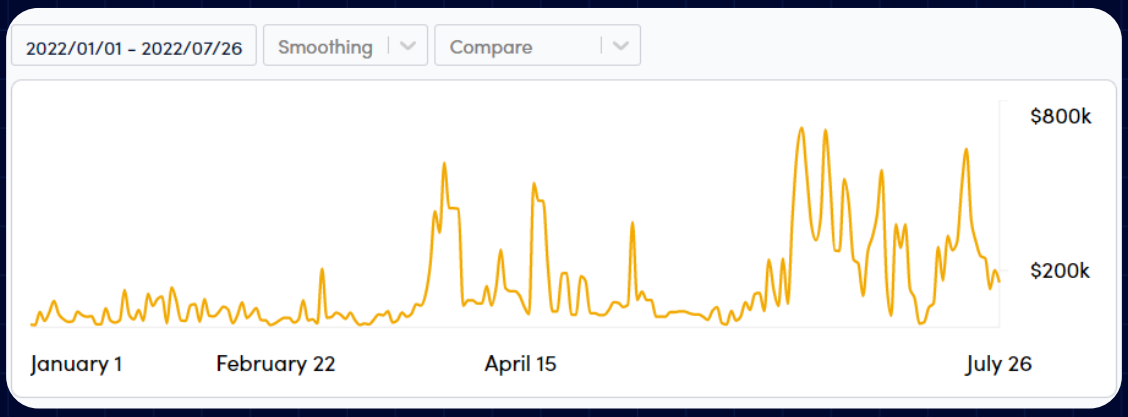


We have also seen the rise of several decentralized perpetual protocols in recent times. For one, GMX is a fast-rising decentralized perpetual exchange built on Avalanche and Arbitrum. The protocol has attracted significant TVL in 2022, soaring from $108m to a significant $289m.

This sharp increase in TVL for GMX reflected the market's desire for a perpetual exchange on a blockchain outside of Ethereum that was free of KYC.
GMX allowed users to leverage up to 30 times of their collateral by tapping on borrowed liquidity from other users in the form of GLP tokens (which are an index of coins such as BTC, ETH, AVAX and stablecoins).

70% of fees accrued by the protocol is shared with GLP holders, while the remaining 30% is shared with GMX stakers.

Synthetix (SNX), a Revenue-Sharing Protocol



Finally, a revenue/fee-sharing protocol that has become really popular of late would be Synthetix (SNX). For some context, Synthetix is a derivative liquidity protocol that allows users to create synthetic assets and trade perpetual futures. Synthetix was also one of the first DeFi protocols which leveraged synthetic assets to bridge the gap between stablecoins, the stock market, and the commodities market.
In recent times, protocols like Kwenta, Lyra , Curve and 1Inch were built on top of Synthetix to tap on the deep liquidity of the Synthetix Debt Pool, and to allow for efficient trades with reduced slippage. As these various protocols route their trades through Synthetix, Synthetix will accrue fees that will subsequently be shared with SNX stakers.
As a result, the fees accrued by SNX in 2022 have increased sharply from $20-80K/day to $150-300K/day (as of the time of writing).

A Shift Towards Sustainable Tokenomics

From the above, we can see how the ability to generate and sustain true substantive value via consistent revenue-generation will now likely come to define this extant new wave of DeFi protocols, as users start looking for the real weight behind easy-to-make lofty promises and APRs. With the DeFi marketcap and total TVL shrinking as much as it has in recent times, those that remain will definitely, and rightly, be infinitely harder to please, tricker to retain, and more rigorous with their capital. Charismatic leaders will no longer cut it; effective operations will have to form the cornerstone of any successful DeFi protocol in this new age.

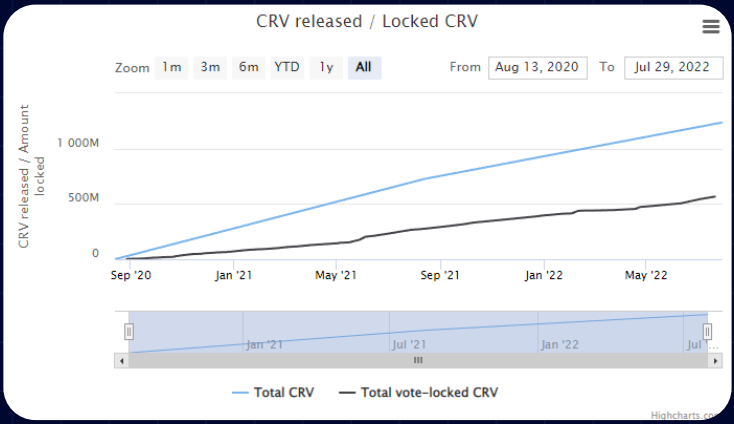
However, this is not enough. While this is a baseline criteria that all DeFi protocols should meet to survive and thrive in this post-bull context, DeFi protocols should also put into place more measures to ensure that they will only attract the right users. A failure to do so will lead to an influx of mercenary capital that, as aforementioned, will likely trickle away en masse in the event that price actions go south. The fact that a protocol's survival is so intrinsically tied to the volatile price actions of the crypto market is not ideal for the longevity and sustenance of any given DeFi protocol, and should be suitably addressed moving forward.

This is where the concept of tokenomics, and by extension, game-theory, come into play. As protocols shift towards substantive models of true value and revenue-generation, they must also ensure that the users who come to them for their services will be aligned with their long-term goals and visions to a large extent. As such, the tokenomics models of DeFi protocols at large must be enhanced and augmented from extant systems to cater for this.

In the early stages of DeFi, and as already mentioned quite a few times throughout this report, protocols offered exceedingly high rewards as a go-to-market strategy to bootstrap liquidity and gain market share within the ecosystem. The high emissions meant that these protocols faced a race against time to capitalize on their market share to overcome the rate of token dilution flowing into the ecosystem.
This issue gave rise to the first attempt at sustainable tokenomics when Curve created the popular ve-Model that is used widely in many protocols today.

The original ve-Model was a simple but effective way for protocols to reduce selling pressure while incentivising long term holders with increased rewards. Curve allowed users to lock their CRV for up to 4 years in exchange for a x2.5 boost in veCRV rewards. The incentivised locking of CRV thus helps to reduce the circulating supply on CRV, and reward those who believe in the project for the long-term, and choose to lock-in for long periods.

The veModel also triggered a secondary impact to the DeFi scene when token bribes for voting power demonstrated how protocols could monetise their governance power.
Convex Protocol aimed to accumulate staked CRV on the protocol to improve their governance sway within the Curve ecosystem. This eventually led to the infamous Curve Wars, where protocols competed to accumulate large amounts of CRV to influence governance proposals on Curve.



With the rise of the veModel, we have started to see a steady progression of various iterations pop up in recent times. In our opinion, this progression will not likely be going away anytime soon, and newer protocols/builders will do well to learn from the best of these iterations.
For some (non-exhaustive) examples of said iterations of the veModel, we will be looking at two protocols that have done relatively well in their own implementations I.

Trader Joe (JOE)

For one, Trader Joe is the largest AMM on Avalanche with $225.34m in TVL. It launched veJOE, sJOE and rJOE in March 2022.

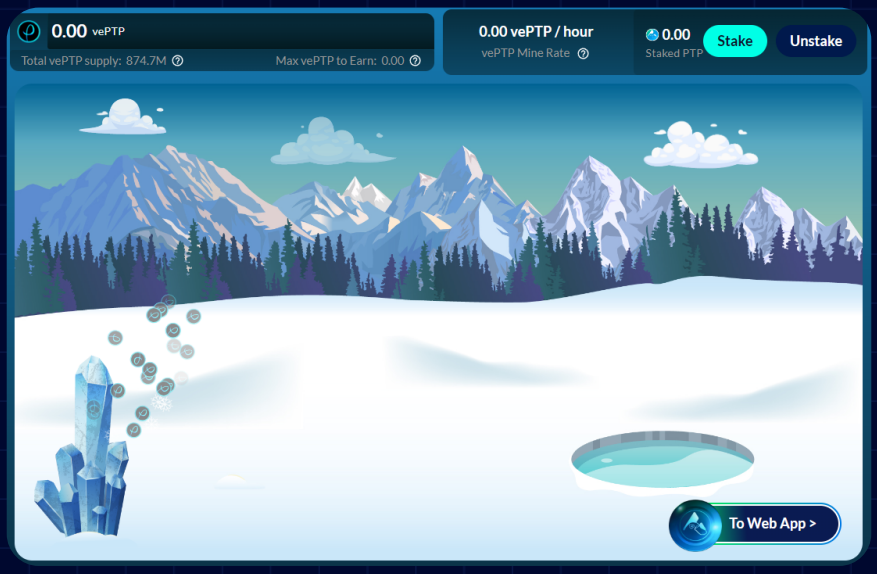
The Trader Joe team chose to fractionalise the use case of the JOE tokens into 3 separate components:
veJOE - Boost in LP rewards & Protocol governance power
sJOE - Profit sharing from protocol fees
rJOE - Allocations from launchpad token sales

By fractionalising these use-cases, Trader Joe attempted to allow users to focus on the aspects of the DEX that best suited their needs.

veJOE also chose to do away with lengthy locks and instead, tried to incentivise long-term staking through a promise of virtual points-accumulation. Their premise was simple and straightforward: the longer you stake, the more virtual points you earn.

Having more virtual points allows users to receive additional rewards from LPing the TraderJoe platform. users can unstake and trade their JOE tokens at any given point in time; they just had to forgo the virtual points that they had accumulated.

Platypus.finance (PTP)



Next, Platypus.finance is an open liquidity and single-sided stablecoin AMM on Avalanche. It uses a single-variant slippage function instead of invariant curves, and allows for single-sided liquidity provision. Currently, it has accrued $191m in TVL.

To expound further on Platypus's tokenomics, $PTP is a governance and utility token that LPs can earn by providing liquidity, while $vePTP is a reward boosting token that is earned by staking $PTP.

For the latter, users can stake PTP to gain 0.014 vePTP every hour, wherein it will take 10 months to hit the vePTP cap. This is a similar model to veJOE, where users will get rewards that are proportional to their vePTP score.

There are also mechanisms in place to limit the impact of whales when it comes to the vePTP model, which can be best represented by this equation:

$$w = \sqrt{deposit} * vePTP$$

To elaborate, the weightage of deposits and vePTP score will always be square rooted to limit the impact of whale-farming of PTP tokens. This is a decent attempt to achieve a fairer distribution of PTP emissions to users, but can be easily circumvented by the more savvy users.

Platypus also utilizes the Platypus Heroes NFT project to imbue some element of gamification into the vePTP model. Here, the Platypus Heroes NFTs will allow users to accrue vePTP scores at an accelerated rate, while also granting them access to gated communities.

How these projects — and more — continue to build and innovate upon the veModel will be interesting to see, and we definitely haven't seen the last of them. As mentioned, up-and-coming protocols will do well to learn from and build on the models of protocols like JOE, PTP, and more.

A Framework for Sustainable DeFi Protocols

Pros and cons notwithstanding, the veModel (and its iterations) revealed the cornerstone framework required for any given protocol that wants to be sustainable and consistent with generating value.

We have summed up said cornerstone framework into a concise table that projects can take reference from when it comes to their operations-planning:

1. Supply — To restrict circulating emissions through locks to minimize selling pressure

2. Demand — To introduce protocol-level demand by incentivising large long-term stakers

3. Revenue Generation — Protocols to be revenue-generating to ensure the long-term viability of business models

4. Revenue Distribution — To share protocol revenue with long-term stakers to allow holders to partake in the success(es) of the protocol

5. Simplicity — To have a simple and easy-to-understand tokenomics model to facilitate an easy onboarding of users

6. Demand and Supply Equilibrium — To model emissions in accordance with the expected demand growth over time

Expanding from the above, there are also 4 lessons that we can derive on the makings of a sustainable and moat-ed protocol:

1. The need to move away from high APRs and liquidity mining to bootstrap liquidity for the sake of it

2. The need to focus on the flywheel of positive loops when it comes to protocol adoption

3. The need to focus on the building of a core community that truly believes in the vision of the protocol (and that is not mercenary capital)

4. The need to move away from dilutive rewards. The alternatives are:
   a. Stablecoin rewards (TRI , JOE , SNX)
   b. Escrowed rewards (GMX, SNX , ILV)

Having said all of the above, this does not mean that the veModel (and its iterations) are necessarily the be-all and end-all of the next wave of DeFi innovations.

In fact, we believe the exact opposite. Within a space as dynamic as DeFi, there is never such a thing as a one-size-fit-all model. Such a mindset will only spell the downfall for any protocol that adopts it.

As such, and as the times (and markets) change, so too should protocols and their respective tokenomics models. The models of protocols should never remain static over time — passivity is never rewarded within this space, and active reflexivity and adaptation will always be required.

In fact, we are already starting to see some protocols push for such reflexive change in their own ways. We will explore some of these new models in the segment below.

A Further Evolution of Tokenomics

Emissionless Protocols

For some context — how YFI structured their launch would probably constitute the best example of an emissionless protocol. To elucidate, tokens that are able to generate revenue can possibly choose to pivot towards an emissionless model post bootstrapping phase. Within such a model, there should be a gradual shift from padded emissions of the native token, towards cash flow rewards generated from protocol fees.

This way, there will be strong incentives for early adoption, as well as a keen focus on the sustainability of the revenue model. Further, the token (and protocol by extension) will be more resistant to sell pressure as supply will be extremely scarce.

Of course, protocols can also choose to adopt a really low emission to account for the gradual growth of the protocol.

Dynamic Emissions

Finally, on the back of our belief (that the DeFi space is one that is always evolving, and that protocols will do well by actively adapting, we believe that tokenomics models will eventually evolve into concepts that are ever-changing as well as robust and dynamic in their implementations. Such models will, at a high-level, involve the shaping of token releases in accordance with demand and profits to provide a minimal floor to said token(s).

In this way, dynamic emissions allow for protocols to be conservative, and not over commit towards any particular emission structure.

However, a concern here would be that the team might use the dynamic nature of emissions for their own selfish and/or malicious means. To mitigate this, we can probably look to Soulbound NFTs — non-transferrable NFTs that can essentially act as digital CVs — to ensure the credibility of all governing DAO members involved.

Further, the adding of time-duration limitations can also ensure that changes will be gradual and no sudden changes can occur. This might be something that we will be thinking more about at a deeper level, so do keep an eye out for that!

The Rise of Synthetic Assets and Derivatives

New tokenomics models aside, another sub-vertical that has come up (and will likely continue to) within the DeFi space in recent times are synthetic assets and derivatives domains, wherein synthetic assets are a form of tokenized derivatives.

Within traditional finance, the cash flow from synthetic assets is largely mainly derived from other assets. Within DeFi, however, the cash flow can be derived from both synthetic assets and the underlying asset(s).

This promotes greater capital efficiency and flexibility by allowing users to determine their own desired parameters for which to base the synthetic asset upon.

These parameters include (very concisely):

1. The collateral ratio

2. The type of asset — commodity, index, stablecoin

3. Fees

4. Profit-sharing

5. The pegging mechanism for the synthetic asset (i.e. leveraged token from TracerDAO)

The ability for users to configure the above parameters will wholly increase capital efficiency within the ecosystem. Underlying assets will continue to accrue value while synthetic assets are traded freely. Synthetic assets also act as a form of leverage for users, which, granted, is a double edged sword. However, and if it is used prudently, this can greatly optimize for capital efficiency.

For more context with regard to the aforementioned capital efficiency, and in sticking with the SNX example, users often complain about the 400% Collateralization ratio (c-ratio) as they often use the c-ratio of money markets as a comparison for capital efficiency.

This is where we have to make a distinction. For most money markets, users will typically provide collateral for a loan that they can trade or generate yield with. For SNX, users will receive SNX rewards and protocol fees from the SNX staked, while also still being able to trade/generate yield with the sUSD Minted. Users are also not required to pay back their debt positions until his/her c-ratio hits 150%.

Flowing from this, if a user wishes to get as much free capital from an underlying collateral as possible, then a money market or taking a sUSD loan on his/her ETH collateral (130% c-ratio) on SNX would be deemed more capital efficient.

If a user wishes to generate as much passive yield as possible from a long term position, then SNX might still be deemed more capital efficient as the position can be left until it hits the floor ratio of 150% whilst still generating additional yields from said position.

Going back to our main point in this segment, synthetic assets will also allow for any uncorrelated assets to be created and traded. This serves as a form of hedge against the volatile crypto market, and also provides investors with more diverse options for investments.

Additionally, this has the potential to open up familiar markets to non-web3-native tradfi investors (even those in emerging economies and/or those without access to the necessary financial services and instruments to tap on these markets), constituting the lower-hanging fruit(s) that they can latch on when entering the web3 world.

In doing so, Synthetic Assets latently democratizes the access to such services and instruments for all around the world.

This is not all that Synthetic Assets can offer though. We believe that within this sub-vertical, the future is extremely bright.

Below are two forms of innovations that we believe will gain traction within the space in the near-to-mid-term.

Fixed Rate Bonds Coupons

Fixed rate bonds coupons will allow for protocols to use their treasuries to provide users with fixed rate bonds in the form of synthetic tokens, wherein users will be able to over-collateralise the corresponding underlying asset(s) to mint a representative synthetic bond.

This bond can only be redeemed on maturity for the base price and the promised fixed rate, and can be freely traded on the open market to whoever is willing to take on the risk of undertaking the bonds.

This will give projects additional options to finance themselves, and will also help to ensure that everything will remain transparent and on-chain.

Structured Products

For some context, structured products are financial instruments whose performances are linked to an underlying basket of assets.

Most derivative-based structured products allow for investors to buy or sell assets at predetermined prices or strike prices. Additional conditions can be built into the products to ensure that the product is sufficiently attractive to both issuer and investor (i.e execution price is at a premium to strike price).

Such structured products also allow for issuers to hedge their risks in volatile market conditions, and allow for investors to undertake the risks for a suitable premium. However, a caveat: structured products should only be catered towards sophisticated investors who understand the complexities and nuances involved within such products.

Regulation and DeFi: What's Next?

For DeFi to be reborn, we cannot afford to be inward-looking. Whilst improvements to tokenomics designs and protocols are extremely vital, the space also has to be reflexive to external developments too.

In recent weeks, several such external developments (and huge ones at that) have taken place. On the 7th of August, 2022, the now infamous privacy mixer Tornado Cash was sanctioned by the Treasury Department's Office of Foreign Asset Control (OFAC), together with 40+ Ethereum and USDC wallets that are associated with it.

This represented a momentous shift with regard to OFAC's modus operandi, wherein previous sanctions were typically targeted at specific entities that utilized a particular tool for malicious acts, instead of them going after the entire tool, or in this case — source code — directly. The fallout from this was swift.

Popular decentralized exchange dYdX swiftly blocked accounts that had any interactions with Tornado Cash, Github suspended the mixer's account, whilst Circle moved to freeze $70, 000 worth of USDC on the mixer's platform in tandem with banning any address that is connected to Tornado Cash from gaining access to USDC.

On the other hand, Tether Holdings Limited, the firm behind the world's largest stablecoin by market cap, USDT, has declared that they would not be unilaterally blacklisting or freezing addresses that are connected to Tornado Cash.

Non-profit research and advocacy center Coin Center has also mounted a legal challenge to OFAC's ruling.

What Does This Mean for DeFi?

OFAC's sanctioning of Tornado Cash will have repercussions for the space beyond all that has already happened (as aforedescribed). There will be several factors to consider and think about.

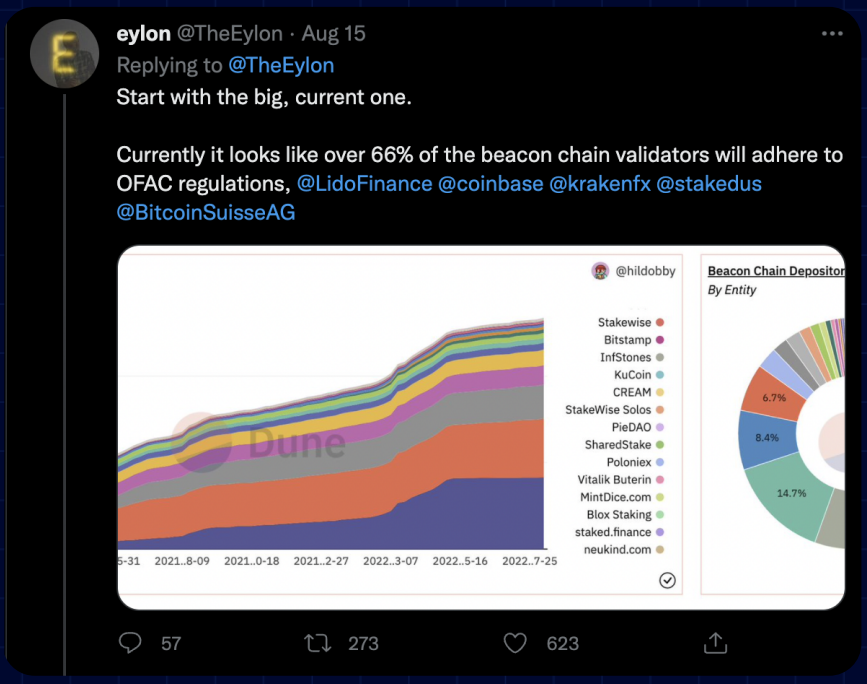
The Censorship-Resistant Value of L1s Must be Protected and Preserved

First, the value of L1 blockchains like Ethereum (that Tornado Cash is built on) has really come to the fore from this incident. Whilst OFAC has laid the banhammer on Tornado Cash's source-code, that code is still very much alive today. To put this into perspective, and according to data from Nansen-on the 8th of August, 2022 (post-sanction), there was an outflow of 13, 800 ETH from Tornado Cash, a hefty day-on-day increment from the outflow of 1, 400 ETH just the day before (pre-sanction). In other words, whilst the front-end of Tornado Cash may have been taken down vis-a-vis its website, the back-end code is still there, unstoppable and unable to be killed.

Within the blockchain world, code is always king; it is censorship-resistant, and cannot be bent to even the whims of large centralized entities like governments. Illegal cases notwithstanding *(we are not condoning the illegal acts of money laundering for illicit gains by any means)*, this certainly has value in the privacy-starved world that we live in today. The Tornado Cash incident has proved that to a large extent.

This value is something that we must protect and preserve at all costs for the sake of not just the DeFi space, but also the broader Web3 one. There is a reason why we have raised this point.

Twitter user @TheEylon put forth a very pertinent and thought-provoking thread on Ethereum. In it, he discussed how the Ethereum validator-community is ostensibly not decentralized enough to truly be censorship-resistant.



If @TheEylon's hypothesis is correct, and over 66% of beacon chain validators will not sign blocks that are associated with Tornado Cash (thereby adhering to OFAC regulations), how is Ethereum then different from any given centralized platform? What then, in that context, is the point of blockchains?

Therefore, the decentralization/diversity of validator-communities is something that the industry as a whole definitely has to first think about carefully if we even want to experience a rebirth of any sort.

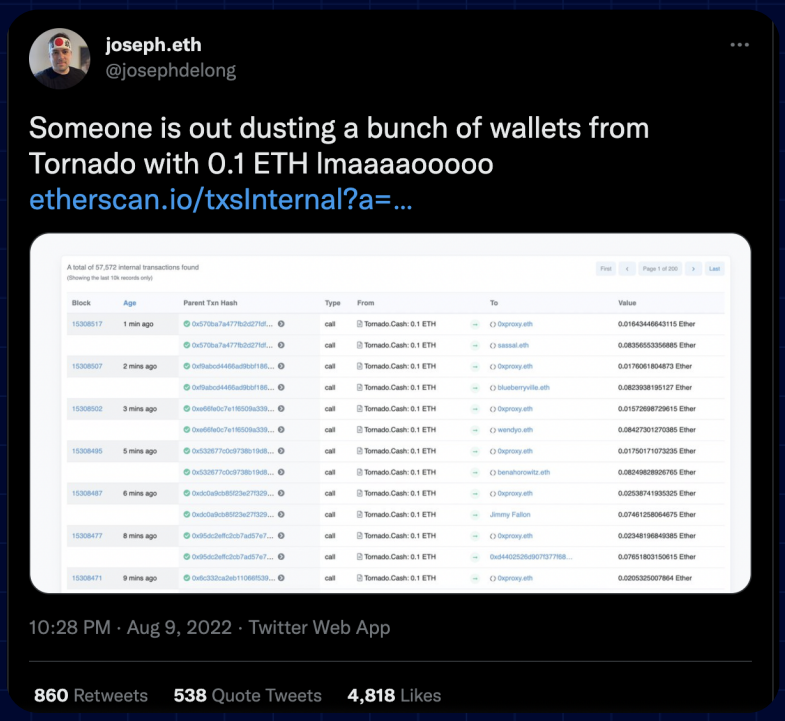
The Need for Grassroots Legislative Intervention

Whilst what has happened is pretty unfortunate for the DeFi space in general, it is not as dire as many have made it out to be. In any given nascent industry, there will always be turning points that will help said industry mature, if only they deal with it appropriately.

We believe that the Web3 industry is currently at one such turning point. How we move on from here will be of paramount importance, and the discussions and dialogues that are birthed from this must be done so meticulously and effectively. In looking at the sanction from another light, this is a chance for the Web3 community to voice out their concerns (with regard to legislation of the space), as well as to fight for a chance to define some parameters when it comes to said legislation of the space.

We now have a reference point, albeit a pretty extreme one, to work with; we have to fight hard to have a strong say in this crucial conversation that will likely shape the Web3 landscape for years to come.

At a very high level, there is already so much nuance that OFAC's ruling lacks. For one, this may be a sanction that hurts innocent parties more than insidious and malicious ones. This post-sanction dusting attack proves just that.



More than that, the above also proves how said sanction may be so overreaching and all-encompassing that it risks overwhelming the system with cases (in this context, innocent recipients of the ETH dust) that are insignificant to say the least, rendering it unable to deal with the real "bad guys" effectively.

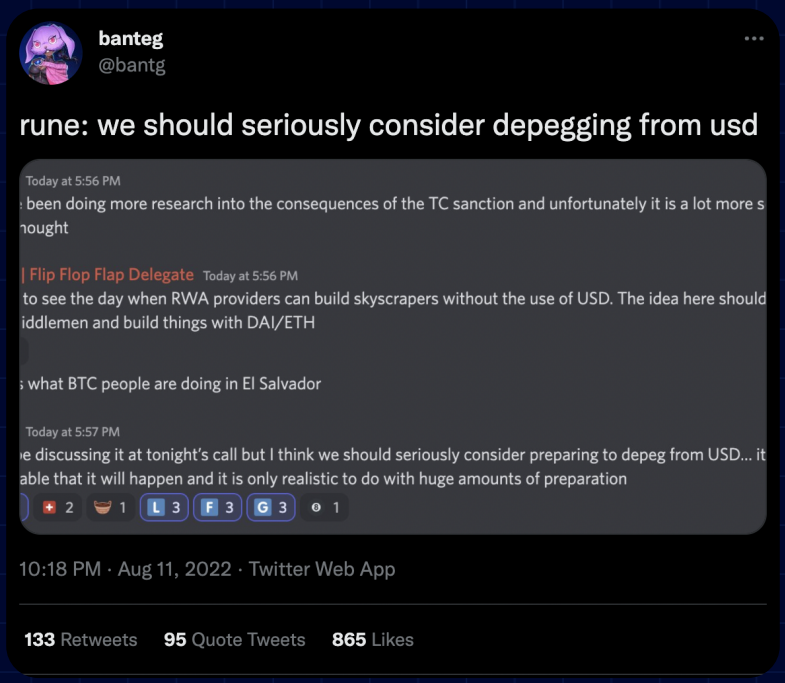
Whilst laws should always be framed broadly enough to prevent people from easily finding loopholes or workarounds, OFAC's ruling definitely isn't perfect by any means. Here is our chance, as a community, to kick-start a conversation with regard to it. If we can have a substantive one, then we may very well be given the power to shape our own future for years to come when it comes to the domain of legislation and regulation in Web3. That is not to be taken lightly at all.

The Over-Reliance on Centralized Entities

Finally, the Tornado Cash incident has also divulged the strong need for protocols to not rely too heavily on centralized entities for their survival and thrival.

This is perfectly encapsulated by MakerDAO's current situation in light of OFAC's sanctions. For some context, DAI, MakerDAO's native stablecoin, is currently predominantly collateralized by USDC. MakerDAO is a major DeFi protocol with an extremely significant (in relation to DeFi's total TVL) TVL of almost $11 billion. Therefore, their (over)reliance on USDC, an asset that has proven to be so overtly within the reach and purview of government sanctions, should definitely be a concern to all within the space.

In fact, Rune Christensen, founder of MakerDAO, has come out to openly discuss the possibility of depegging DAI from USDC, a move that is clearly informed by USDC's response to OFAC's regulation.



This is something that goes way beyond MakerDAO and DAI; objectively, for a decentralized community, ecosystem and industry to survive, it cannot be heavily premised on centralized elements that are prone to the control and influence of centralized entities.

Once again, and as already mentioned, we are not, in any way, condoning the bad actors that utilize Tornado Cash and/or any given decentralized protocols for their ill gains. It is only that for Web3 to live up to its very purpose in the first place, this is something that must be acknowledged.

Closing Thoughts

In our piece, we traced the progression of DeFi from a mere thought experiment, to the vibrant and diverse ecosystem that it is today.

Whilst the total DeFi market cap and TVL may be down significantly from the all-time-highs that came to dominate the DeFi summer of 2020 (and to some extent, 2021), DeFi is definitely not dead by any means.

The trials and tribulations of the past few months will definitely shape and improve the DeFi space for months and years to come, and we are already seeing some semblances of that in several of the protocols that we have discussed in this report.

What people sometimes fail to remember is that DeFi is not a monolithic entity. It is also not a static one. It is a sum of many moving parts, and it is constantly adapting and evolving dynamically.

What people sometimes fail to also remember is that the concept of web3 and crypto was never really given a fighting chance at the very beginning. We were always dead (and still are) to the misperceiving eyes of many. And yet, we have managed to come this far in our collective journey anyway, with many more leagues to go.

After all, what is dead may never die.