Q4 2020

DeFi Report

An analysis of Ethereum's decentralized finance ecosystem in Q4 2020.

CONSENSYS Codefi

Authors

JAMES BECK

James Beck is Director of Communications and Content at ConsenSys. He has ghost-written commentary and articles for ConsenSys executives that have appeared in Wired, Quartz, and other industry publications. James is passionate about the increasing crossover between non-fungible tokens and art, as well as web3 models for collectives savings accounts like *susus*.
Get in touch with James.

TOM HAY

Tom Hay is the Head of Developer Relations at ConsenSys. He is also a member of ConsenSys Academy's instructional team, a product manager, and a data analyst. He writes about software development best practices over on the ConsenSys blog. Get in touch with Tom.

With thanks to: Mattison Asher, Lex Sokolin, Corbin Page, and Nicole Adarme

About ConsenSys Codefi

ConsenSys Codefi is the blockchain application suite powering next-generation commerce and finance. Our vision is to lead the convergence of existing and decentralized financial technologies to create more accessible and equitable financial services for everyone, everywhere.

We work with financial institutions, global enterprises, and Ethereum projects to optimize business processes, digitize financial instruments, activate markets and networks, and deploy production-ready blockchain solutions.

LEARN MORE

Outline

Executive Summary

Even as the “DeFi summer” cooled, the breadth of invention and adoption of DeFi kept pace in Q4 of 2020, building on all the major themes of this year: the swift rise of stablecoins, the new types of assets seeking the liquidity of Ethereum, and the growth of new types of financial products, marketplaces for unique art, and even community based social tokens.

This report covers the main DeFi trends in Q4 2020 and what we are anticipating in 2021.

1. THE SWIFT RISE OF STABLECOINS

Today, 74% of all stablecoins are issued on Ethereum and worth about $20 billion as of January 1, 2021. As ERC-20 tokens, stablecoins have the benefits of other Ethereum tokens: the cost to produce them is low, they have global reach making it easy to transact across borders, they are fully auditable, and importantly for decentralized finance, they are interoperable with the rest of Ethereum. One of the newest developments in Q4 of 2020 were the increasing number of interest-bearing stablecoins, such as cDAI (compound.finance) and yUSD (Yearn.finance). As stablecoins have risen in prominence, they've also become increasingly the subject of regulatory discussion.

2. FROM INSTITUTIONS TO WRAPPED BITCOIN: EVERYONE WANTS ACCESS TO DEFI LIQUIDITY

One of the major trends in Q4 was the increased demand from institutions and other blockchain-based protocols to access the liquidity and economic activity on Ethereum. This is largely due to the new ways in Ethereum has managed to attract digital assets from other blockchain protocols. From wrapped Bitcoin and Filecoin, to institutional funds and professional traders interacting seeking alpha on DeFi protocols, Q4 saw new inflows of value tokenized on Ethereum. We predict that in 2021 we will see more additional protocols launch wrapped versions of their tokens on Ethereum. While real world assets like real estate and bonds have been tokenized on permissioned versions of Ethereum, such as a €350 million real estate fund on ConsenSys Quorum, there are still regulatory and technical challenges to bringing traditional financial assets to decentralized finance. New types of standards, like the Universal Token for Assets and Payments, could provide a solution.

3. HOW DEFI BEGAN INCORPORATING ART, MUSIC, SOCIAL REPUTATION, AND COMMUNITY MANAGEMENT

Since non-fungible tokens (NFTs) represent the financialization of digital goods, NFT designs and marketplaces have become an undeniable growing sector of DeFi. Just as Ethereum has used ERC-20s to represent digital assets, NFTs can be understood as ownership rights for digital art, virtual items, and tokens to access a digital community. With art galleries around the globe closed due to COVID-19, and more cultural experiences occurring online, Ethereum found a growing niche for creators to share art and interact directly with an enthusiastic community of collectors. Nonfungible.com, which tracks more types of marketplaces, counted 5 million unique NFTs sold for a total nearing $150 million. Design patterns in the DeFi space are blending into the NFT marketplaces as well, such as Aavegotchi's, which earn yield from Aave's a tokens (such as aUSDC or aETH) and has DAO-governed game mechanics.

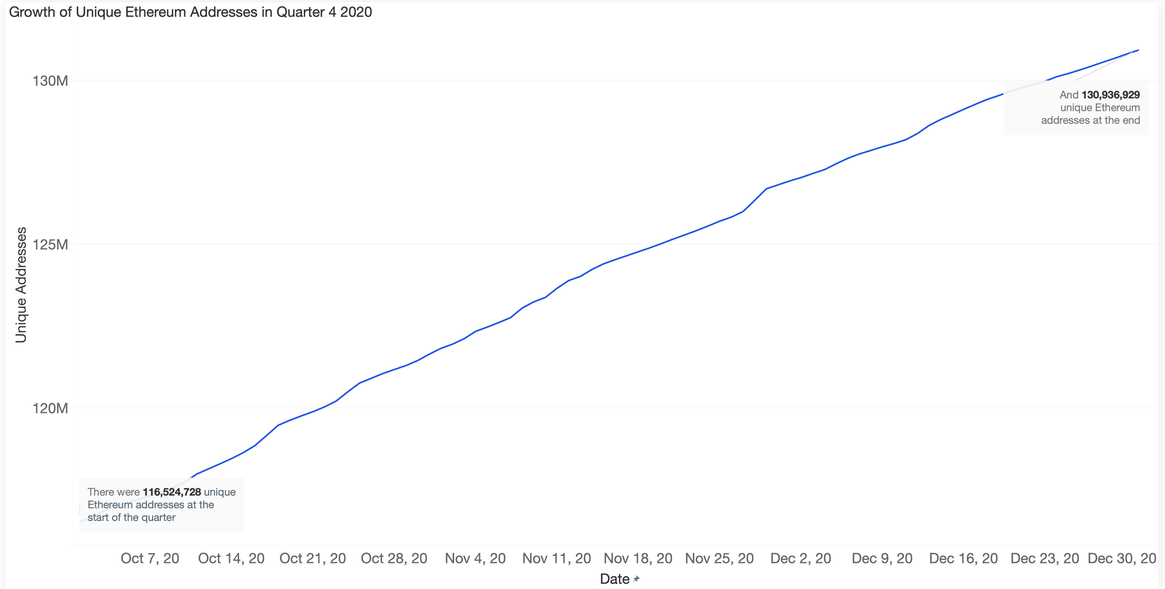
4. THE HACKS, EXPLOITS, AND TRULY NOVEL DEFI INVENTIONS THAT PUSHED INNOVATION

It wouldn't be a DeFi report without describing some exploits of DeFi protocols. Smart contract security has long been a critical area for avoiding potentially catastrophic vulnerabilities after launch. ConsenSys Diligence combines hands-on review from veteran smart contract auditors with open source security analysis and runtime verification tools like MythX and Scribble. But in other cases, it is a truly novel invention, such as Aave's "flash loan" or the "flash swap" by Uniswap, that have enabled arbitrage schemes at a scale and speed not previously imagined. Several DeFi protocols have been the victims of flash loan-based exploits in Q4 2020. Harvest Finance lost $34 million, Cheese Bank lost $3.3 million; Akropolis suffered a $2 million loss and Value DeFi lost $6 million.

Introduction: Q4 2020 DeFi

If Bitcoin proved a global digital store of value is possible, this year Ethereum proved that an entire decentralized financial (DeFi) ecosystem is inevitable. At first glance, you wouldn't be at fault for mistaking the billions of dollars in financial activity through trading, borrowing, lending, options, and derivatives as sophisticated parallels to existing finance. But by spending a little time uncovering the DeFi ecosystem's logic, it quickly becomes clear how an interweaving set of protocols and applications built on different assumptions of trust deliver powerful new patterns of creating and distributing value for communities. As the cost of creating digital assets continues to become more accessible to anyone with an internet connection, so does the ability for individuals around the globe to engage in financial transactions without the need of trusted intermediaries, like escrow accounts, banks, or lawyers. Coming to consensus without a central actor is a profound evolution of the social contract.

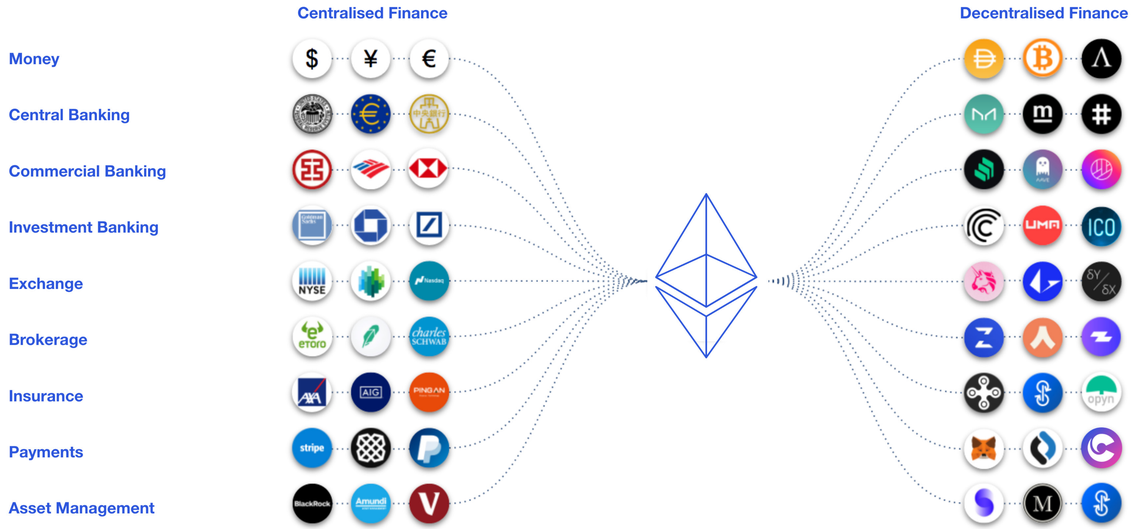
1 | On Average, 100k new addresses were created daily in Q4 2020.



[Source: Dune Analytics]

When Marco Polo first came back from the China, his tales of people using paper representations of value drew skepticism — not far from the skepticism of cryptographically secured bits of data flowing around the global Ethereum mainnet that may represent a dollar, a bond, a unique work of art, or even someone's identity. Cognitive scientist Margaret Boden said, "Some of the most important human creations have been new representation systems. These include formal notations, such as Arabic numerals (not forgetting zero), chemical formulae, or the staves, minims, and crotchets used by musicians. Programming languages are a more recent example."

2 | Mapping traditional finance to decentralized finance.



It's with appreciation to how Ethereum is enabling new representations of value and organizational structures of distributing this value that guides this Q4 DeFi report. And if the best way to understand something is to experience it, we invite you to start your DeFi journey by downloading MetaMask, which is available both as a browser extension and as a mobile app. You've now equipped yourself with a key vault that only you can access, a secure login, a wallet to view your tokens, and a way to exchange tokens or access the decentralized web. Think of it as a way of managing your money, digital assets, unique art and identity as you traverse the decentralized financial landscape. With MetaMask, you can acquire some ETH, swap that ETH for a stablecoin like DAI or USDC to lend and earn rewards, or provide liquidity to a decentralized exchange. With services like Zapper or Zerion, you can view the performance of your token portfolio, and even invest or provide liquidity to other DeFi protocols. MetaMask is the gateway to the new Web3.0 world.

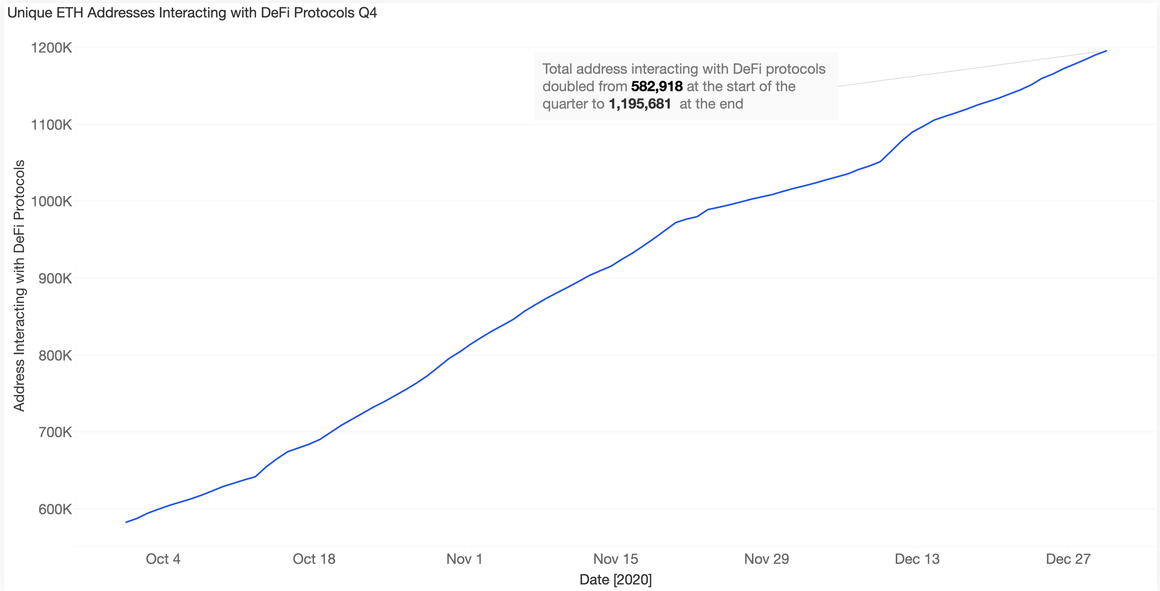
Banking in the 21st century may initially seem to be evolving alongside the way that data and information flow instantly over the internet. But even as we spend more of our lives online, opening a bank account, connecting it to a brokerage or exchange, and trying to move your money around seems cumbersome once you get used to a paradigm where your financial identity, accessible through MetaMask, can follow you around and interact with any Web3 application, regardless of your access to a bank account or loan. It's estimated that 1.7 billion people on the planet do not have access to basic traditional financial services. Despite financial technology companies providing services that enable smoother user experiences, the critical infrastructure and computer languages on which they run have not changed much in 60 years.

Composability is often credited as one of the reasons why it is easier for developers to build new products and services on Ethereum. Composability is a term used to describe the intertwining relationships applications can build, like different pieces of legos that can be stacked on one another to build a far superior structure.

For developers, DeFi is unique in that they can leverage any combination of open source DeFi protocols together without needing permission, as most of DeFi is built with open source code. New combinations are thus able to be built upon the work of previous developers, like the creation of ERC token standards (which stands for Ethereum Request for Comments). It's agreed upon token standards like the ERC-20 that make stablecoins, governance tokens, and derivatives possible. Other token standards, like the ERC-721 make it possible to represent unique data, such as art, music, or virtual in-game items as non-fungible tokens (NFTs) on the Ethereum blockchain.

Standards help ensure smart contracts remain composable. For instance when a new project issues a token, it remains compatible with existing decentralized exchanges or lending protocols. The increasing composiblity of Ethereum has been a boon for developers creating new services and financial products. Borrowing and lending may not have been worthwhile on Compound without the creation of a stablecoin like DAI. Furthermore, it's also the Ethereum standards that are making it possible for other types of assets to be represented on Ethereum. These smart contract patterns are bringing about entirely new types of automated finance.

3 | 1,195,000 unique Ethereum addresses now interact with DeFi protocols. Q4 2020 added at least 607,000 unique addresses.

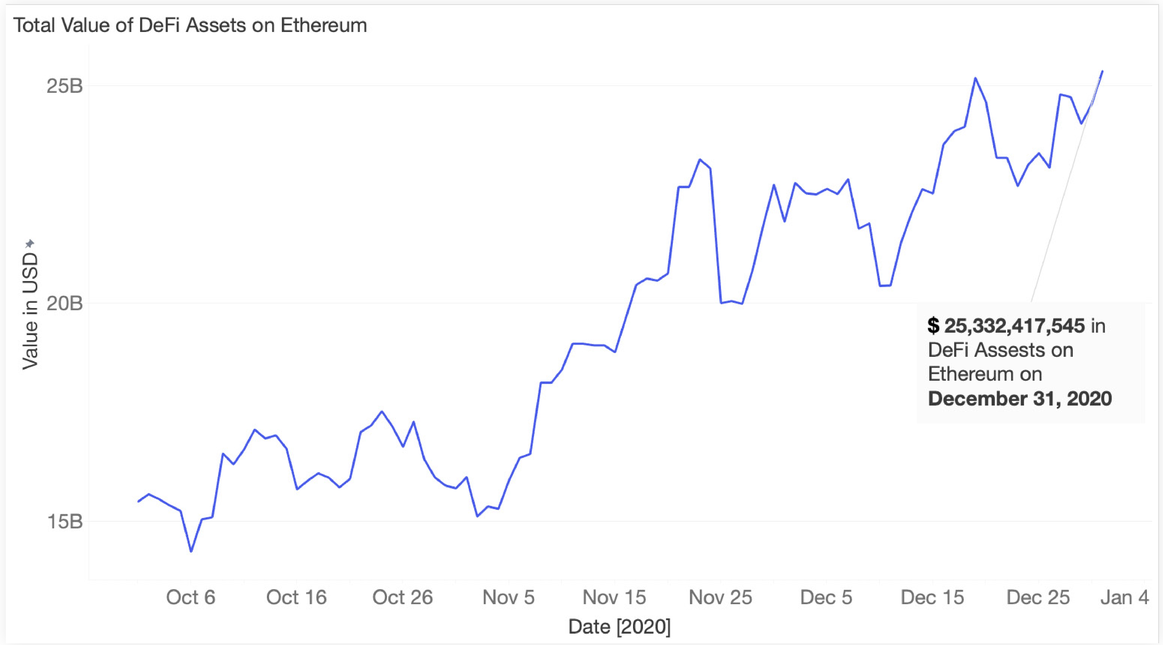


[Source: Dune Analytics]

Yet composability on its own does not drive the transformation of finance. The true transformations come in the ways in which value accrues to those involved in the process. Most of the applications and protocols discussed in this report are community owned, some even started by anonymous groups of individuals. The traditional world of capital formation sees value accruing to investors and employees. Now the very users of projects become the owners and use their ownership to vote on the future of a protocol or community. Figure 4 and 5 show that there is tremendous growth in fees expended on decentralized applications on Ethereum.

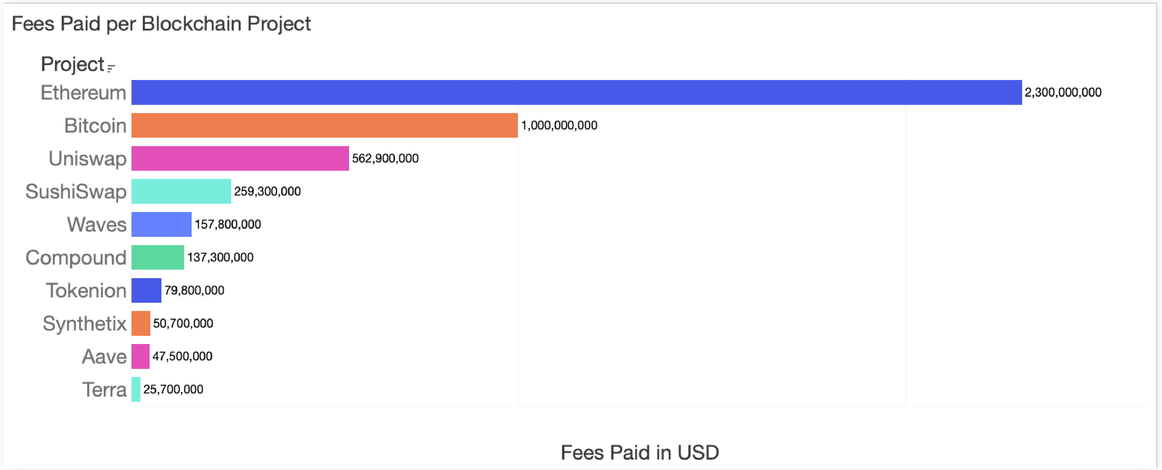
These fees do not just go to the team that built these applications, but also the users of these applications that provide liquidity for trading pairs on decentralized exchanges (DEXes) or collateral for loans.

4 | The total value of DeFi assets on Ethereum exceeds $20 billion.



[Source: CoinGecko]

5 | Increasingly, users of protocols are realizing the upside of fees.



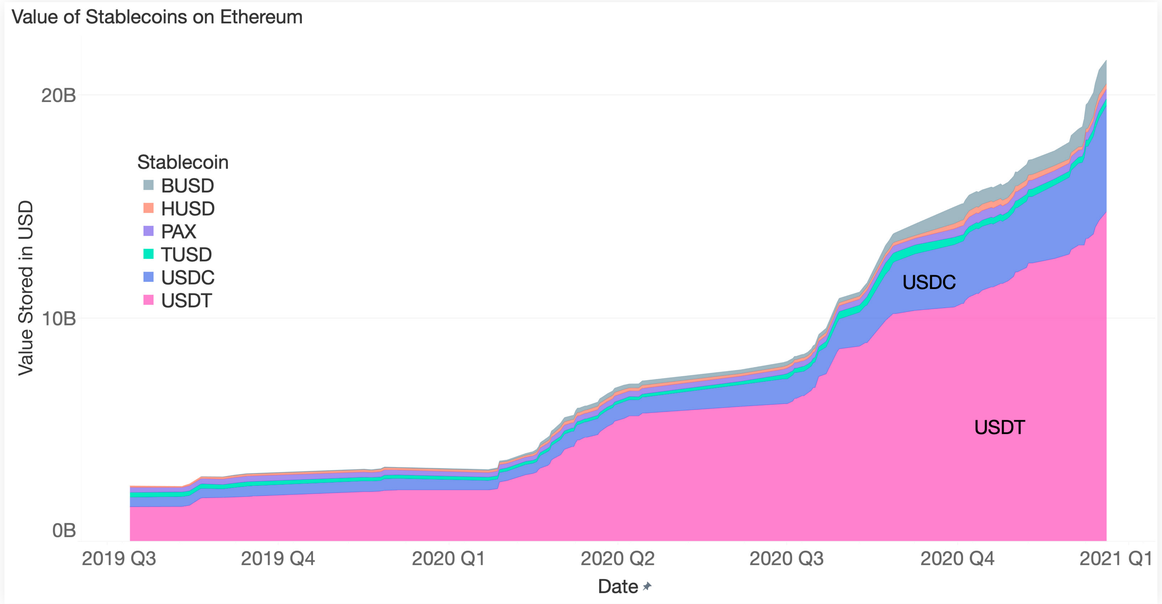
[Source: Token Terminal]

The Swift Rise of Stablecoins

When ConsenSys first wrote about stablecoins in 2019, the sector was taking off with over 200 different stablecoins issued by companies around the world, nearly half of which were issued on Ethereum. Today, 74% of all stablecoins are issued on Ethereum and worth about $20 billion as of January 1, 2021. As ERC-20 tokens, stablecoins have the benefits of other Ethereum tokens: they are efficient to produce and manage issuance; they have global reach making it easy to transact across borders; they are fully auditable; and importantly for decentralized finance, they are interoperable with the rest of Ethereum.

Introduced as a means to represent a more familiar unit of account (dollars) and solve for the daily volatility of digital assets like Bitcoin and Ethereum, they have also helped decrease volatility of overall crypto markets, since traders don't have to exit exchanges and transfer fiat to when hedging against price declines. Additionally, stablecoins also strengthen the bridge between traditional finance and crypto markets since activities like borrowing, lending, derivatives need a stable and reliable base value. Furthermore, as some journalists have begun noting, stablecoins are increasingly serving as an option for avoiding inflationary fiat currencies. For example, individuals in Brazil are turning to USD denominated stablecoins as an alternative to the Brazilian real, which hit a record low against the USD this year. The swift rise of stablecoins has also compelled governments around the world to explore the ways in which Central Banks could issue their own currencies on smart contract platforms like Ethereum.

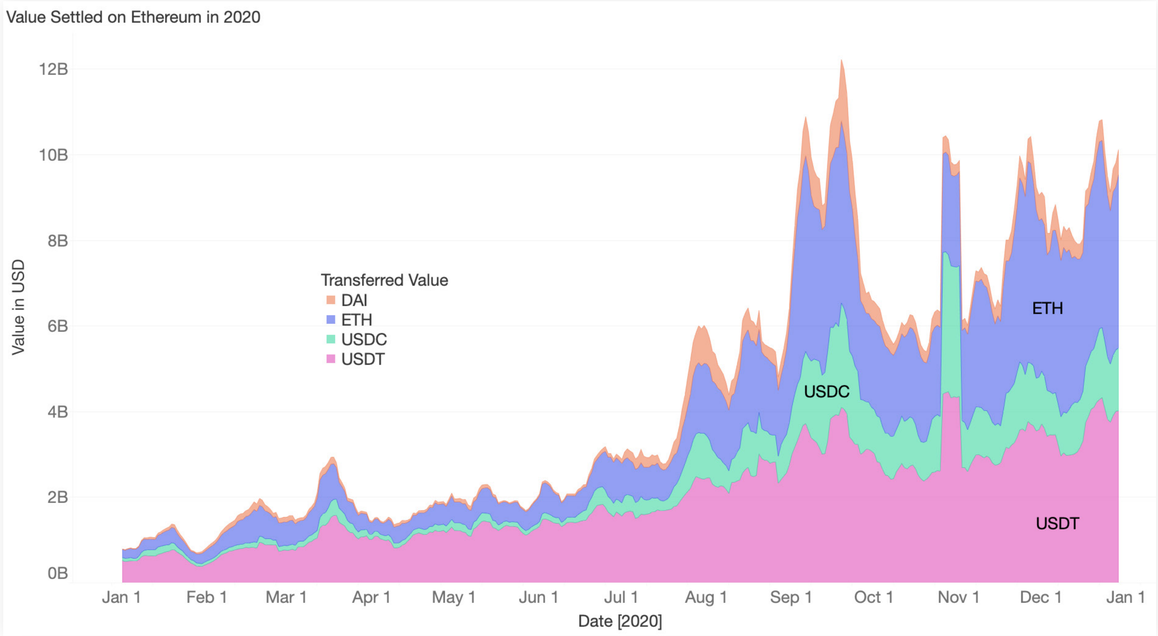
6 | Total issuance of stablecoins on Ethereum.



[Source: Dune Analytics]

Stablecoins have seen such a rise in 2020 that they are now responsible for more trade volume on Ethereum than the asset that pays for computation — ether (ETH) — itself. The annual transaction volume for ETH this year was $385 billion, but Tether's USDT token settled $580 billion on Ethereum, Circle's USDC stablecoin settled $239 billion on Ethereum, and MakerDAO's DAI stablecoin settled $98 billion. **All told, nearly $1.6 trillion USD in stablecoins and ETH transacted on Ethereum.**

7 | Transaction volume of ETH, DAI, USDC, and USDT settled on Ethereum.



[Source: CoinMetrics]

THE MANY NEW FLAVORS OF STABLECOINS

In 2020, stablecoins are one of the best examples of what programmable money can look like, simply because of the different design decisions of how they can be issued or how they retain parity with the U.S. dollar.

Type	Description	Example
Fiat-backed	An Ethereum stablecoin can represent a U.S. dollar, with each token issued backed by a corresponding U.S. dollar in a treasury.	USDC USDT
Crypto collateralized	An Ethereum stablecoin can be issued when collateralized by other digital assets like ETH, BAT, or USDC.	USDT
Interest-bearing stablecoin	An Ethereum token can be created to represent a stablecoin deposit earning interest, also known as an interest-bearing stablecoin.	cUSDC aUSDC aUSDT
Synthetic	An Ethereum token can be synthetic, introduced by Synthetix where sUSD is backed by SNX holders, who are rewarded for providing collateral and stability with fees generated by Synth transactions.	sUSD
Algorithmic	An Ethereum token can be programmed to optimize in search of the highest yield opportunities, or have its treasury managed through the minting and burning of existing supply.	AMPL yUSDC

Most stablecoins are supported by the liabilities of the traditional banking system, such as Circle's USDC where each crypto dollar is backed by a US dollar held in reserve (whether or not Tether's USDT supply is fully backed has been called into question by the NY AG and is out of scope for this paper). Since both of these stablecoins are issued by a centralized entity, they can also be seized, or a user could be denied access.

The most common types of synthetic stablecoins, such as DAI, are overcollateralized by other cryptocurrencies, such as ETH, USDC, and BAT. Newer models of synthetic stablecoins, such as Ampleforth's AMPL, use variable supply, meaning that an oracle monitors the supply and demand and "rebases" to meet a target peg.

One of the newest developments in Q4 of 2020 were the increasing number of interest-bearing stablecoins, such as cDAI (compound.finance) and yUSD (Yearn.finance). Whenever someone deposits a stablecoin as collateral in a borrowing and lending platform like Compound or Yearn, they receive a token which represents the deposit position. For example, if you were to deposit 100 USDC into a Aave lending pool, you will get 100 aUSDC in return, which increases as you earn lending fees akin to a dividend- or coupon-issuing financial instrument. What's unique is that even as aUSDC compounds overtime, it is just like other ERC-20 tokens: it can be traded, or used as collateral for other liquidity pools. Even more advanced yield-generating stablecoins, such as Yearn's yUSD, yDAI, and yUSDT, are programmed to find the greatest return of investment from various lending and borrowing protocols, such as Aave, Compound and dydx.

As the different types of stablecoins offered proliferates, one way to understand their tradeoffs is through the inverse correlation of their complexity and how decentralized they are based on the collateralized assets (or none at all) that help them maintain a stable peg to the USD.

HOW DO GOVERNMENTS SEE STABLECOINS

As stablecoins have risen in prominence, they've also become increasingly the subject of legal discussion. On November 19, 2020, several U.S. lawmakers introduced the STABLE Act, which if passed, would require stablecoin issuers to obtain a federal banking charter and also be required to obtain the approval of both the Federal Reserve and the Federal Deposit Insurance Corporation (FDIC) six months prior to issuance. While the congressional calendar ran out of time to pass the bill in 2020, it is likely it will be reintroduced again in 2021.

In contrast to the STABLE Act, The US Office of the Comptroller of Currency (OCC) issued a letter clarifying that national banks and federal savings associations are allowed to operate blockchain nodes and use stablecoins for payments. Acting Comptroller of the Currency, Brian P. Brooks, wrote, "Our letter removes any legal uncertainty about the authority of banks to connect to blockchains as validator nodes and thereby transact stablecoin payments on behalf of customers who are increasingly demanding the speed, efficiency, interoperability, and low cost associated with these products."

Toward the end of the year, the European Central Bank wrote that widely adopted stablecoins, "could threaten financial stability and monetary sovereignty." While it is still unclear how privately-issued stablecoins will be treated by governments around the globe, increasingly regulators are studying how to make sure stablecoins take place within a more regulated environment, while also researching how Central Banks could issue their own form of programmable digital currencies.

From Institutions to Wrapped Tokens: Everyone Wants Access to DeFi Liquidity

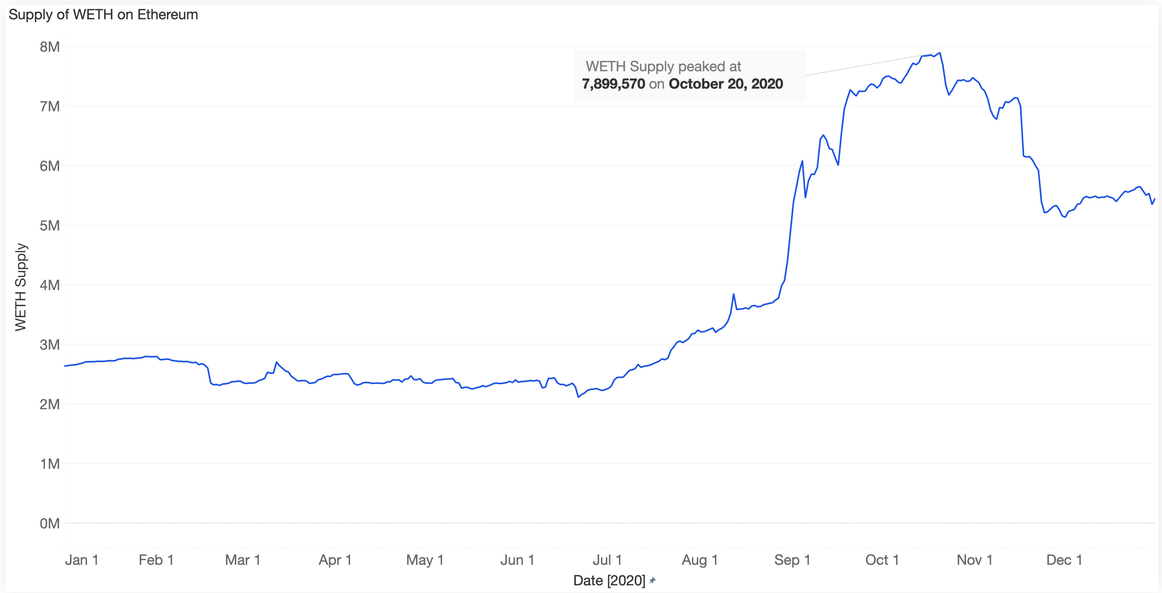
One of the major trends in Q4 was the increased demand from institutions and other blockchain-based protocols to access the liquidity and economic activity on Ethereum. This is largely due to the new ways Ethereum has managed to attract digital assets from other blockchain protocols. From wrapped Bitcoin and Filecoin, to institutional funds and professional traders interacting seeking alpha on DeFi protocols, Q4 saw new inflows of value tokenized on Ethereum. We predict that in 2021 we will see more additional protocols launch wrapped versions of their tokens on Ethereum.

While real world assets like real estate and bonds have been tokenized on permissioned versions of Ethereum, such as a €350 million real estate fund on ConsenSys Quorum, there are still regulatory and technical challenges to bringing centralized finance to decentralized finance. New types of token standards may provide a solution.

WHAT ARE WRAPPED TOKENS?

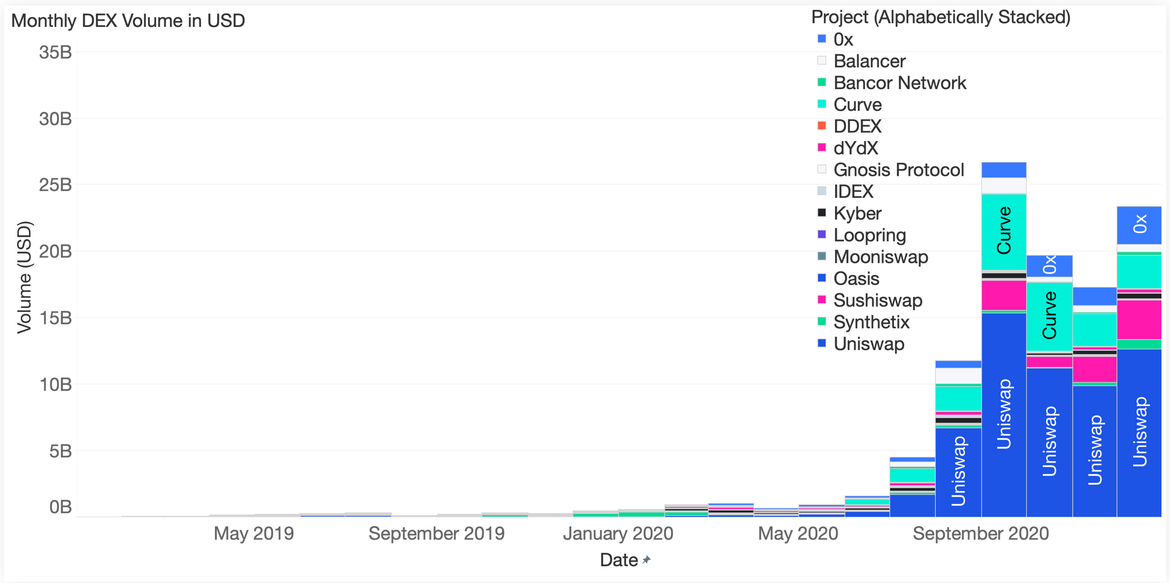
Wrapping tokens on Ethereum describes the process for transforming an existing crypto asset into an ERC-20 token. ERC-20 tokens remain the most widely-used standard for token design, and ensures that the rules of smart contracts remain compatible with applications like decentralized exchanges or lending protocols. The introduction of wrapped tokens actually began with ETH itself, since the ERC-20 token standard came after the attributes for sending and storing ether were established. Wrapped ETH (or WETH) transforms ETH into an ERC-20, which provides all the functionality and transferability of an ERC-20 token. To wrap a token, typically a user “locks” the original token in a smart contract, which then mints an equivalent amount of wrapped tokens. This is analogous to a traditional structured note, issued by a DeFi robot. To unlock your original tokens, you simply trade your wrapped tokens back to the smart contract. “Wrapping” seems like a misnomer, since you’re actually just trading one token for an ERC-20 token of equal value. But this simple action has powerful consequences, evidenced by the 5.5 million ETH transformed into WETH by the end of Q4 2020.

8 | Supply of WETH on Ethereum.



[Source: CoinMetrics]

9 | Monthly trade volume by DEXes.



[Source: Dune Analytics]

As covered in the ConsenSys Codefi Q3 DeFi report, one of the major trends in the middle of 2020 was the rise of decentralized exchanges (DEXes). The total trade volume on DEXes in Q4 topped $60 billion, and one of the main drivers of this activity is because WETH makes it simple to swap ETH for any other ERC-20 token.

The method of wrapping tokens has also been generalized across other types of tokens and protocols, further catalyzing the ubiquity of ERC-20 tokens.

BITCOIN ON ETHEREUM

If you can turn ETH into an ERC-20 token, why not also turn Bitcoin into one so that it can interact with smart contracts and protocols on Ethereum? Wrapped Bitcoin gained significant momentum in Q4 2020. Now over 138,774 BTC (about $3.9 billion USD) exist on the Ethereum network, with WBTC and renBTC as the dominant wrapped Bitcoin. Ultimately, this means that now Bitcoin holders can use their BTC with Ethereum-based wallets like MetaMask and access decentralized financial applications.

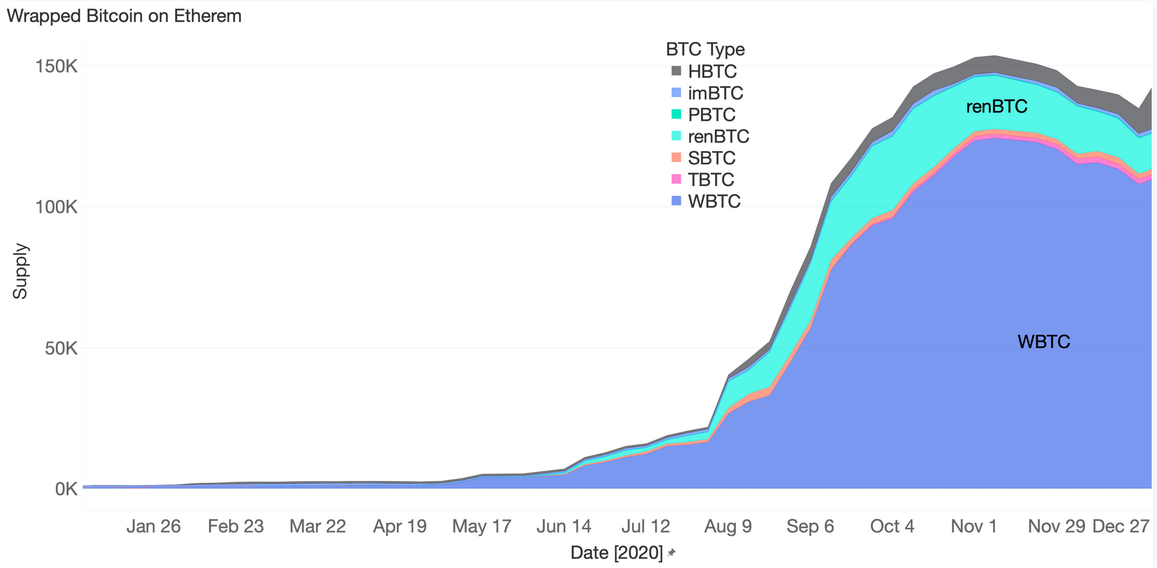
Initiated in January 2019, Wrapped Bitcoin is a collaborative project from BitGo, Ren, Dharma, Kyber, Compound, MakerDAO, and Set Protocol. The project is now controlled by a Decentralized Autonomous Organization (DAO) called the WBTC DAO, which governs the addition and removal of merchants and custodians for WBTC on Ethereum through a multi-signature contract. WBTC has brought greater liquidity for Bitcoin to the Ethereum ecosystem, as WBTC is used to trade on decentralized exchanges, as collateral for borrowing and lending, or for derivatives trading. For example, Compound allows anyone to secure a passive income lending out WBTC to other users in the network. WBTC has also helped shift trade volume away from centralized exchanges to DEXes.

Another method for wrapping BTC that gained momentum in Q4 2020 is the use of synthetic Bitcoin, where a user locks their BTC into a smart contract and receives a synthetic asset with equal value. Synthetix, a derivatives trading platform, pioneered this technique calling their wrapped Bitcoin sBTC. While the synthetic token isn't backed by BTC directly, Synthetix backs each BTC with 800% of BTC's value in SNX tokens, which are also used for governance and providing liquidity.

All this BTC on Ethereum is yielding some interesting trading products. TokenSets, a DeFi company that automates portfolio management strategies, introduced a product that automatically trades between WBTC and ETH to capture gains in both assets by rebalancing the composition of ETH/WBTC depending on the relative price momentum.

By the end of Q4 2020, there was 141,322 BTC on Ethereum, which represents approximately $4.2 billion USD.

10 | Wrapped Bitcoin on Ethereum.



[Source: Dune Analytics]

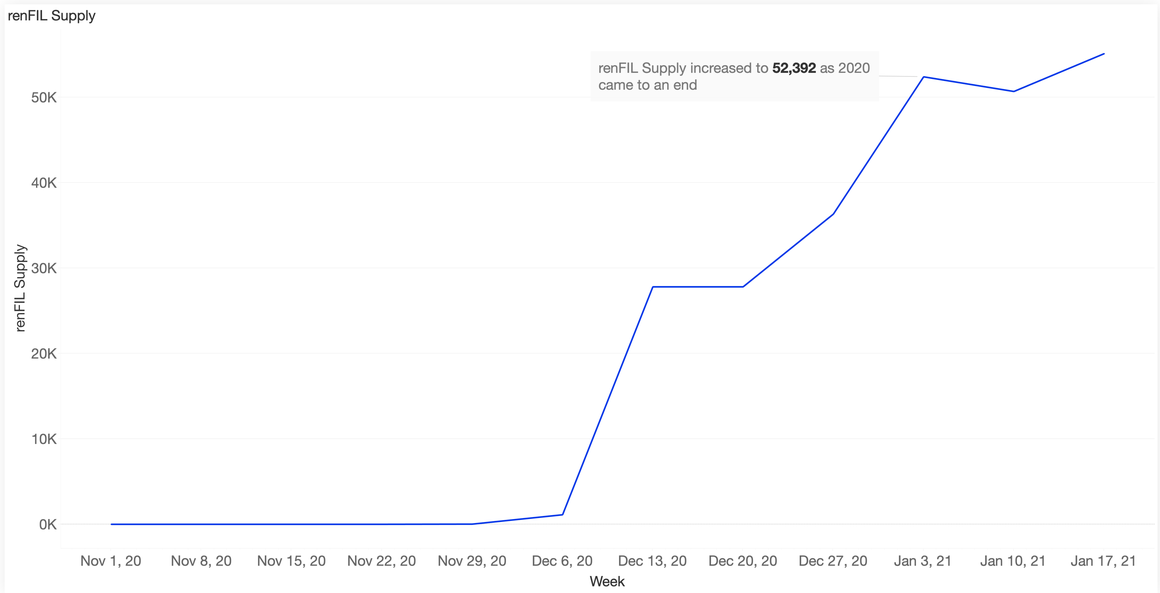
FILECOIN ON ETHEREUM

The launch of Filecoin in Q4 was one of the most anticipated launches in the decentralized protocol space. On the Filecoin Network, FIL is the native currency used to pay for data storage on a global network maintained by storage miners. (Filecoin is a complementary protocol to IPFS; the difference is that Filecoin incentivizes storage and therefore offers stronger persistence guarantees.)

In Q4, ConsenSys Codefi introduced DeFi Bridge in order to convert Filecoin's FIL to an ERC-20 token using the Ren Protocol, which also wraps BTC. Once on Ethereum, FIL holders and miners can deposit their renFIL as collateral in DeFi lending markets to earn interest, or borrow more FIL needed for storage mining operations. Ensuring a liquid supply of FIL through lending markets is a critical element of building out the storage market and driving network utilization of IPFS. Using the Codefi-built platform, storage miners can deposit ETH-based assets as collateral, borrow wrapped FIL, and convert it to native FIL to store data or engage with the Filecoin network.

Since launch, 48,575 renFIL has been issued, or approximately $1,020,075. Other exchanges like Binance and Huobi launched their own versions of wrapped FIL, with 33,000 BFIL and 59,999 HFIL issued, respectively. All told, there is 143,843 wrapped FIL on Ethereum, or more than $3 million USD.

11 | renFIL on Ethereum.



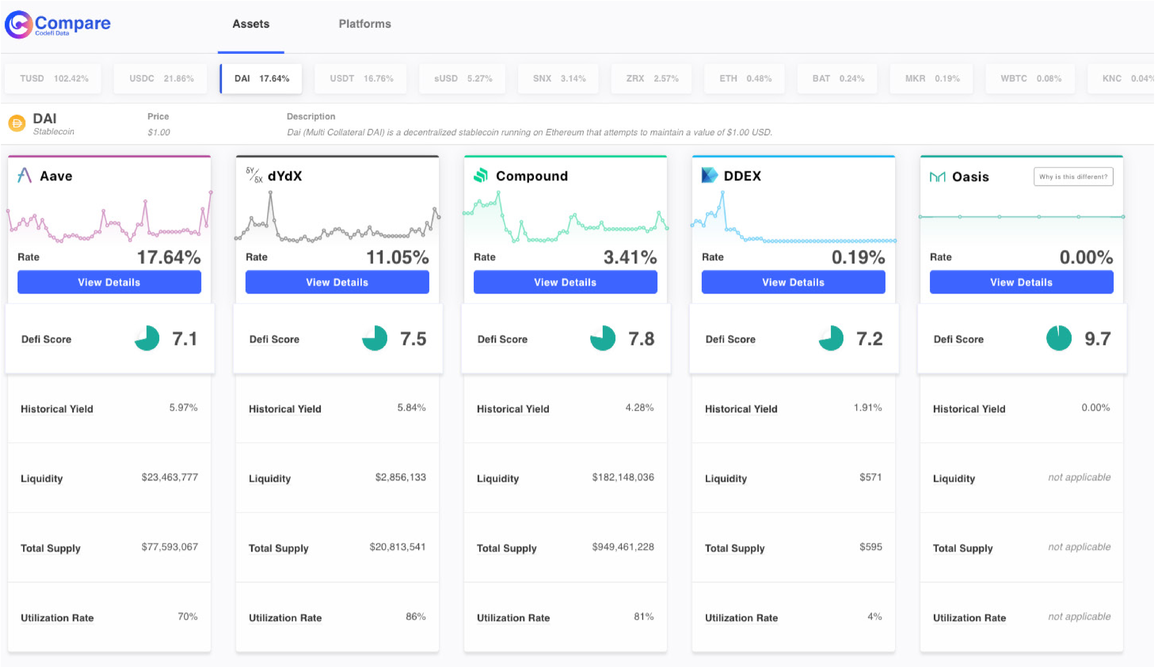
[Source: Dune Analytics]

INSTITUTIONS AND PROFESSIONAL TRADERS ALSO WANT TO ACCESS DEFI

Another trend in Q4 2020 saw custody providers and professional traders increasingly seeking exposure and access to DeFi yield opportunities for their assets under custody. With interest rates on trading pairs or lending protocols in the range of 5-12% APY compared to US treasuries at 0.92% yield, it's easy to see the appeal.

When perusing DeFi Score by Codefi, you can see yields as high as 17% for lending DAI, or 21% for lending USDC. While those rates are highly variable based on liquidity and demand, the historical rates still average between 2-5%.

12 | DeFi Score by Codefi Compare.



Why does institutional interest in DeFi matter? For one, the more funds that get channelled into DeFi, the more that risk and assets diversity is distributed. Financial analysts point to increased liquidity, the narrowing of spreads, better risk profiling and insurance coverage as important benefits of institutional participation.

And yet professional traders are still engaging with DeFi protocols despite having to revert to retail-level use of MetaMask or custom integrations with individual apps as a workaround. Some trading firms choose to not engage without robust reporting for accounting, tax, and P&L purposes.

To solve these pain points, ConsenSys began offering trading firms and crypto custodians an institutional-grade version of MetaMask with new features to enable secure use of DeFi protocols and other applications. Customers can swap tokens, borrow, lend, and invest in Ethereum applications with the same familiar user experience of MetaMask — yet with the operational, security, and reporting features necessary to run a professional DeFi trading desk. ConsenSys' first partner is Curv, which integrates MetaMask with Curv's digital asset security infrastructure.

In Q4 2020, some major announcements, such as PayPal offering crypto custody and trading, as well as Mass Mutual adding Bitcoin to their company's balance sheet, clearly showed that there is an institutional interest in alternative assets like cryptocurrencies. But many make the comparison of Bitcoin to digital gold — a commodity uncorrelated with equities and fiat. As for DeFi, there is still the perception that it is too niche or risky. In Q4 2020, custodians like Trustolgy launched a DeFi product to steer funds and custody clients into vetted DeFi protocols and added smart contract safeguards, like requiring digital signatures from multiple parties in order to execute trades. The Chicago DeFi Alliance, with support from Volt Capital, Jump Trading, CMT Digital, and DRW / Cumberland recently launched a program to teach traditional trading firms how to provide liquidity in DeFi protocols, and the risks they should be aware of.

Beyond chasing yield, there are many reasons why small to medium sized enterprises (SME) would be interested in accessing lending products on Ethereum. There was already a significant funding gap between borrowers and lenders, particularly in emerging markets. COVID-19 has exacerbated the challenge for SME to borrow from their usual banking lenders. Similarly, smaller funds struggle more with sourcing funding than sourcing borrowers. In Europe, Basel IV would rework the approach to risk-weighted assets (RWA) as well as set regulatory capital floors, therefore increasing the capital that banks need to put aside against those risks. It will leave more space for alternative lenders to step in for as long as they can find capital to fund high yield transactions.

WHAT WILL IT TAKE FOR CENTRALIZED FINANCE TO EMBRACE DECENTRALIZED FINANCE

In 2019, Societe Generale issued a €100 million ($112m) covered bond as a security token on public Ethereum. A month prior, Santander settled both sides of a $20 million bond transaction, also on public Ethereum. Both instances represented the first big tests in whether institutions could settle traditional financial assets on a global permissionless network. While real world assets have been tokenized on permissioned versions of Ethereum, such as a €350 million real estate fund on ConsenSys Quorum, there are challenges to bringing centralized finance to decentralized finance.

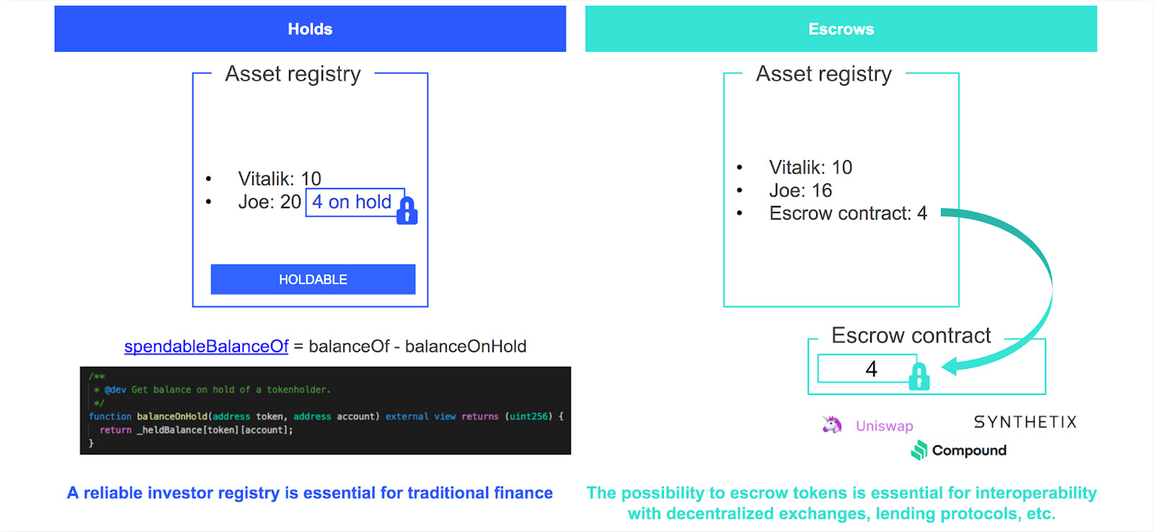
In DeFi, no one but the token holder can decide whether or not to transfer a token, which is one of the core promises of Ethereum: that trust should be in the core of a protocol rather than in a public or private authority.

In traditional finance, the maintenance of a registry falls on large institutions like central security depositories, transfer agents, or even issuers themselves. ERC-20 tokens do not contain a function for allowing a third-party to control who it is sent to, and for what purposes. So for example, if an ERC-20 were to represent a real estate bond, regulators would not be able to prevent valuable assets meant for a country's development from ending up in personal bank accounts or liquidated as luxury goods (like what happened with the 1MDB scandal in Malaysia).

So how can an asset be both permissionless, but still have some controls necessary for legal jurisdictions?

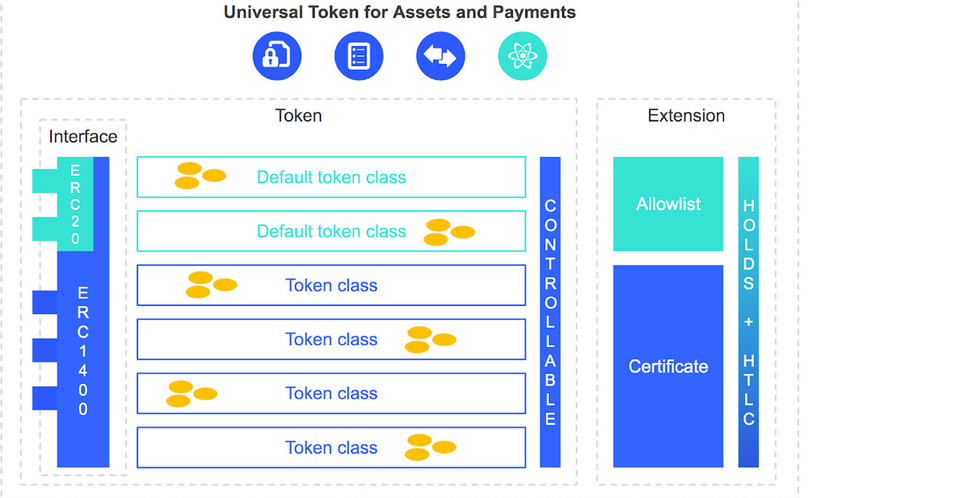
Like most things in Ethereum, the engineering work is happening on the standards level, namely the ERC-1400, which is a hybrid Ethereum token designed for traditional financial assets. The ERC-1400 possesses the property of both a non-fungible token (like an ERC-721) and a fungible token (like the most common ERC-20). Since it is compatible with the ERC-20 standard, it remains compatible with the majority of existing tools and platforms. But it also has more controls so it can comply with requirements for asset issuers.

13 | How tokens with escrow functionality could be interoperable with DeFi



ConsenSys Codefi has taken the ERC-1400 idea further, by proposing a Universal Token for Assets and Payments. Like the ERC-1400, it is compatible with ERC-20s, so it can interact and be transferable on DeFi apps. But importantly, it introduces a new type of token hold, in which a user can grant someone else the power to transfer tokens on their behalf, or forbid a user from spending the tokens for something not agreed upon. This is more optimal than the allowlist / denylist concept in the ERC-1400, because it guarantees the certainty of execution when transferring a token representing a real-world asset with a token representing cash by preventing a user from using the token for something else not defined by the trade order. Bringing up the 1MDB example again, if the development fund had been tokenized according to the Universal Token standard, the government of Malaysia could have prevented the funds from being embezzled by Jho Low in the first place without having to spend millions in auditing and legal fees.

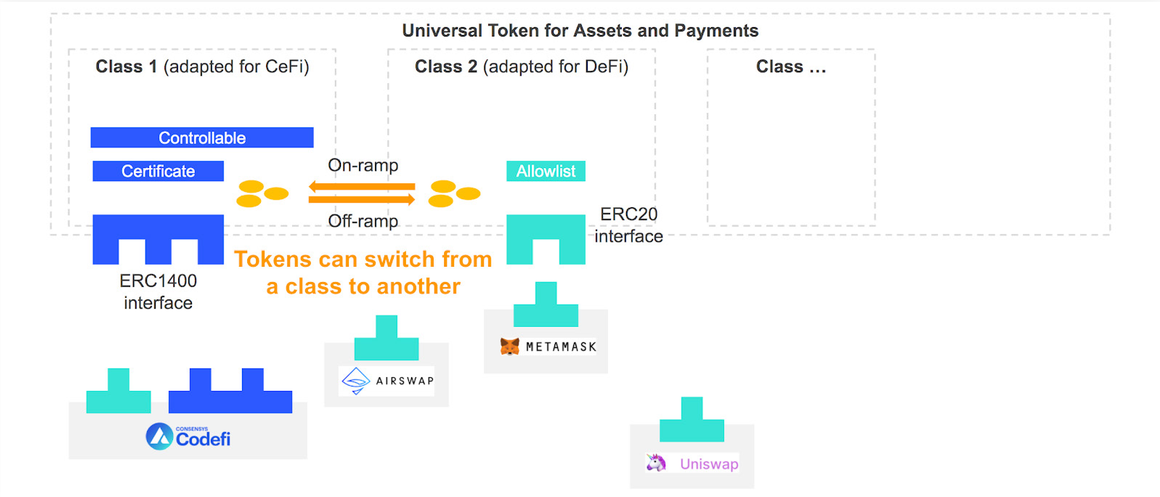
14 | Features of the Universal Token for Assets and Payments



The Universal Token standard has the following features:

- For control mechanisms, it offers a module for certificate checks and a module for allowlist checks + it offers the possibility to force transfers
- For reliability of investor registry, it provides a module to create token holds
- For certainty of delivery-vs-payment (DVP) execution, it includes token holds for atomic DVP, and Hash Time Locked Contract (HTLC) mechanism for non-atomic DVPs
- For interoperability, it offers an ERC20 interface

15 | How the Universal Token for Assets and Payments could switch from CeFi to DeFi



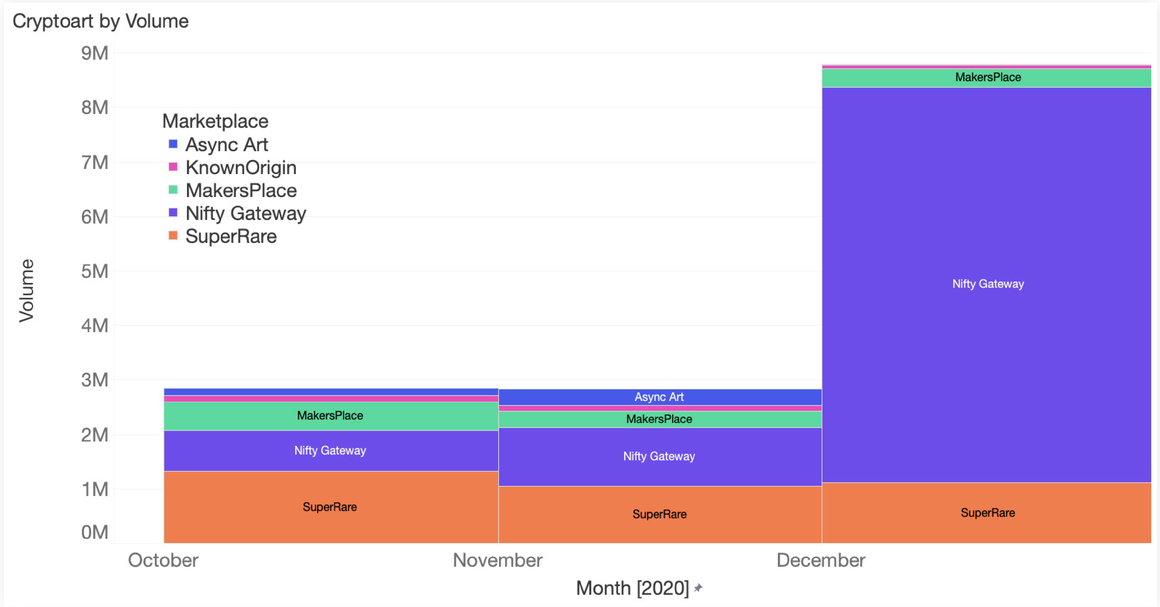
Because Ethereum is so adaptable, it's these types of token standards that will continue to be tested with real use cases in 2021 to more fully bring the centralized finance sector to decentralized finance. For assets to contain the benefits of DeFi, but also satisfy the requirements of traditional finance, a more modular approach is necessary, so that certain features can be turned on and off during a token's life cycle. As laws around tokens evolve, so too can traditional finance slowly migrate towards more "decentralized" arrangements. For existing DeFi applications, soon they too may become compatible with an increasing number of token standards.

How DeFi Began Incorporating Art, Music, Social Reputation, and Community Management

Since non-fungible tokens (NFTs) represent the financialization of digital goods, NFT designs and marketplaces have become an undeniable growing sector of DeFi. Just as Ethereum has used ERC-20s to represent digital assets, NFTs can be understood as ownership rights for digital art, virtual items, and tokens to access a digital community. With art galleries around the globe closed due to COVID-19, and more cultural experiences occurring online, Ethereum found a growing niche for creators to share art and interact directly with an enthusiastic community of collectors.

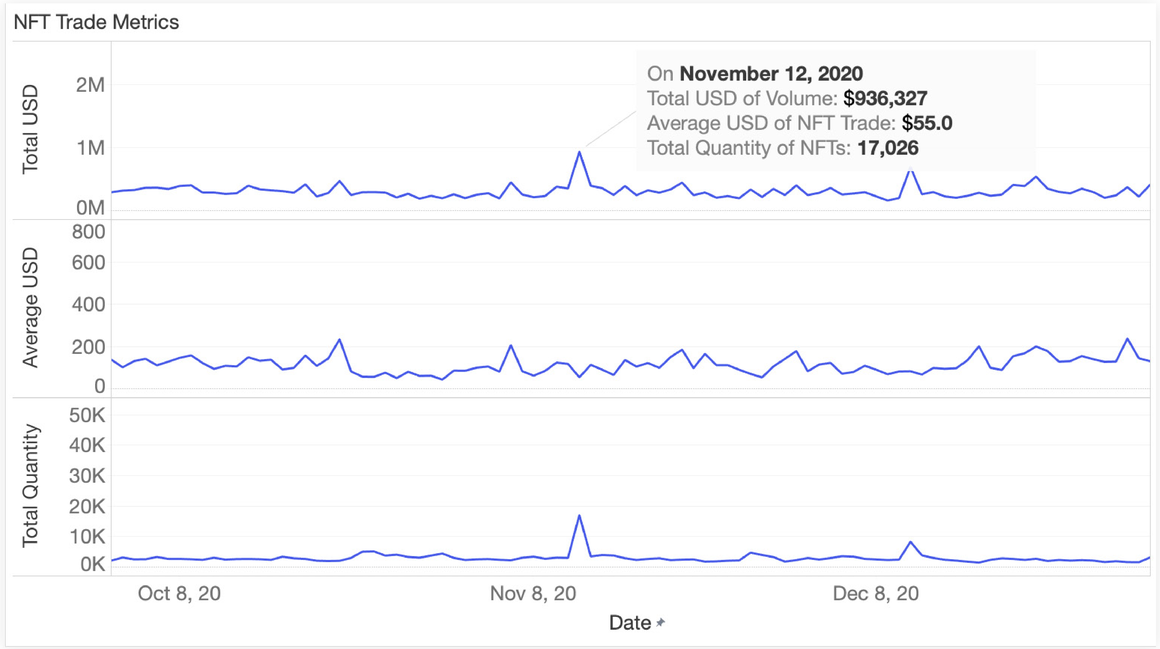
By the end of 2020, the total market value for NFTs was $52,293,650 (42,720 ETH) with 53,663 unique works of art sold on the five largest platforms. Nonfungible.com, which tracks more types of marketplaces, counted 5 million unique NFTs sold for a total nearing $150 million. While this is still a fraction of the $63.7 billion yearly volume of the traditional art marketplaces, the number of unique artists, art, and buyers may be greater in the digital world. In traditional art markets, 1% of artists represent 64% of sales value.

16 | Total NFT market value.



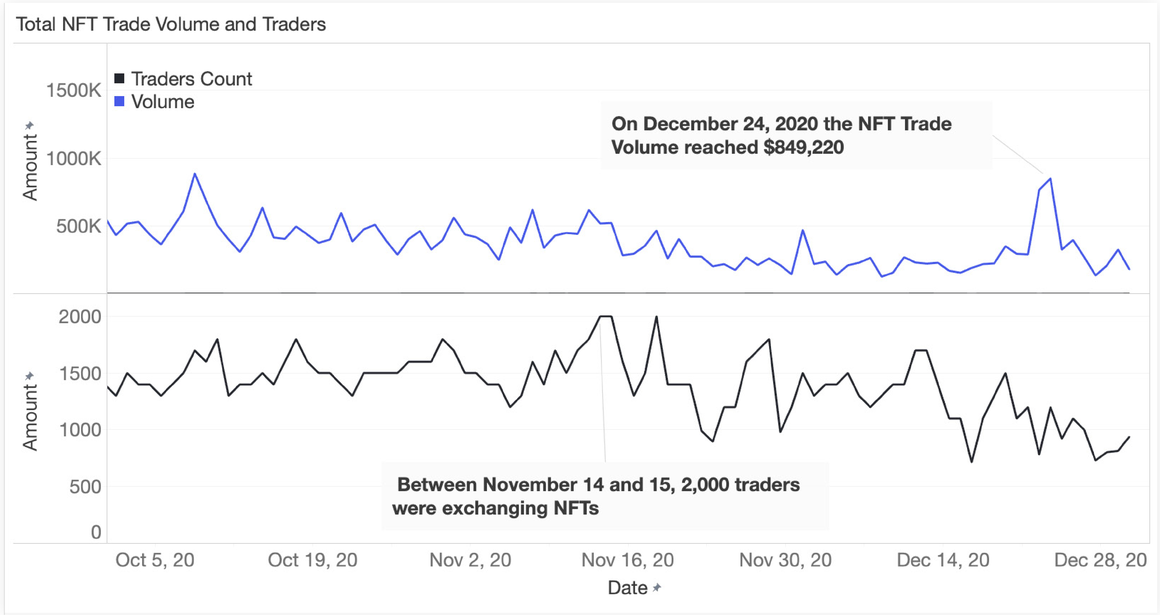
[Source: cryptoart.io]

17 | Total NFT trade volume.



[Source: Nonfungible.com]

18 | NFT Marketplace volume and traders count.



[Source: DappRadar]

Traditional art markets are notoriously illiquid with famous works of art changing hands only a few times over the course of a generation. With digital art on Ethereum, digital art trading is as simple as sending a transaction in MetaMask, and can happen 24/7 every minute. On September 1, 2020, the daily volume of NFT marketplaces was approximately $24,110 with 63 unique traders, and by November 13th, 2020, volume exceeded $618,500 with more than 1,800 unique traders.

With more trading activity and more artists understanding the unique advantages of selling digital art on Ethereum, more mainstream digital artists are also joining the fold. Mike Winklemann, a popular digital artist, who goes by Beeple, sold a collection of NFTs where the winning bid was $777,777.777. NFTs are starting to cross over to traditional art markets, too. In October 2020, the first ever NFT sold at a Christie's art auction for $131,250, and the art is programmed to change its color depending where it is in the world and the time of day.

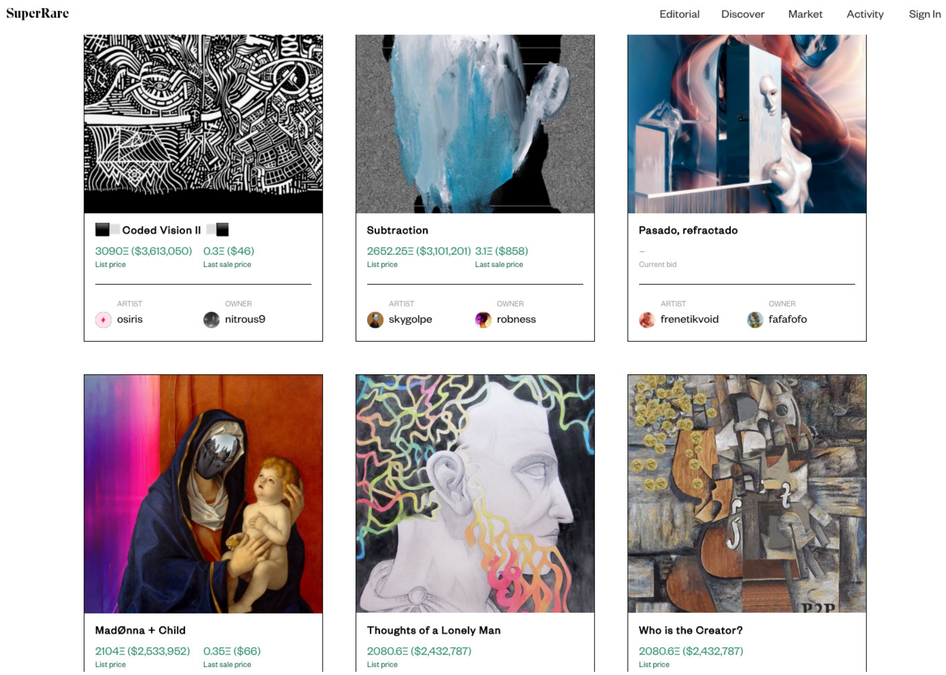
19 | "Block 21" by Robert Alice, the first NFT work of art to sell at Christie's.

NFT MARKETPLACES

There are now at least 27 unique digital art marketplaces on Ethereum, with SuperRare, MakersPlace, Async Art, and Known Origin facilitating between $1-$8 million in sales since they launched.

Other categories of NFT marketplaces include collectibles, such as CryptoPunks (which has had $8.5 million in sales volume all time), CryptoKitties ($38 million in total sales volume) and MLB Champions ($1.5 million all time volume), where NFT figurines can earn rewards alongside live MLB baseball games depending on how well your team performs.

20 | SuperRare art market

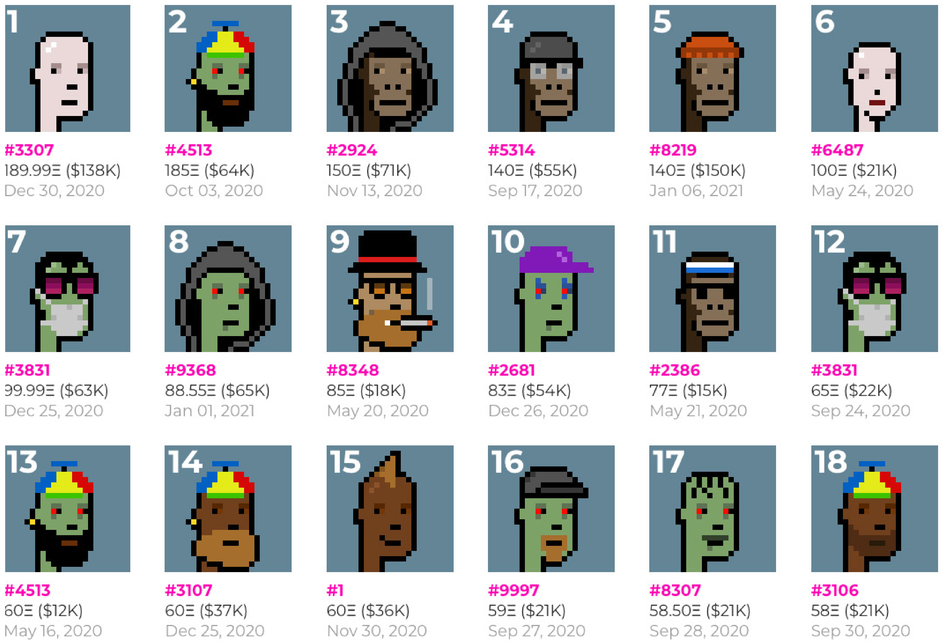


21 | Top CryptoPunks sales by ETH.

CryptoPunks / Top Sales by ETH

Top Sales by Ether Value

(sort by USD)

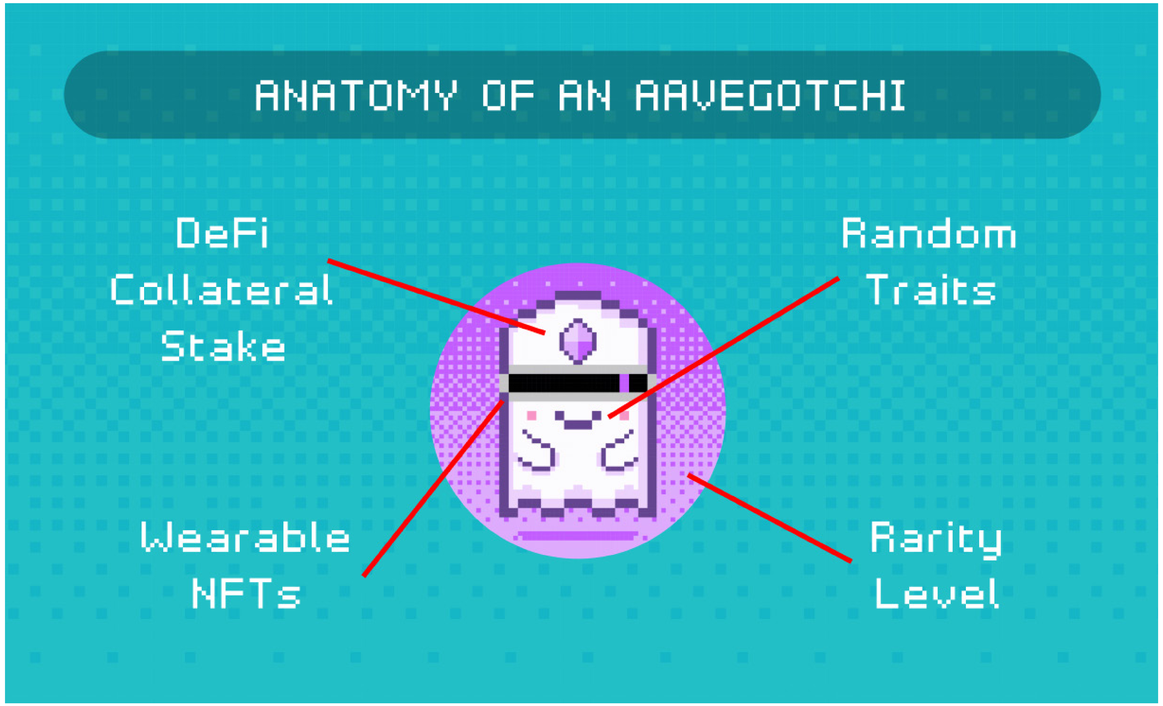


[Source: LarvaLabs]

Design patterns in the DeFi space are blending into the NFT marketplaces as well. Much like DeFi projects before it, Rarible decided to introduce a governance token, RARI, and take steps toward the platform being governed by a Decentralized Autonomous Organization (DAO). RARI token holders (which includes creators and collectors) can vote for platform upgrades and participate in curation and moderation in the marketplace. They are also introducing an NFT index — a portfolio of NFTs for collectors who want to invest in the NFT market, but are unsure of what artwork to choose.

Even more experimental is Aavegotchi, created by Singapore's Pixelcraft Studios, which received investment from Aave and The Lao among others. According to its whitepaper, Aavegotchi aims to "leverage the explosive potential of both [NFT markets and DeFi markets] combined." Like CryptoKitties before it, Aavegotchi's have traits that influence their rarity, such as "kinship" which starts at a fixed value and increases or decreases based on factors like how long the Aavegotchi has been with the same owner, and how often the owner interacts with it. Aavegotchi's have DeFi attributes as well: The Aavegotchi's earn value over time as it earns yield from Aave's a tokens (such as aUSDC or aETH) and has DAO-governed game mechanics.

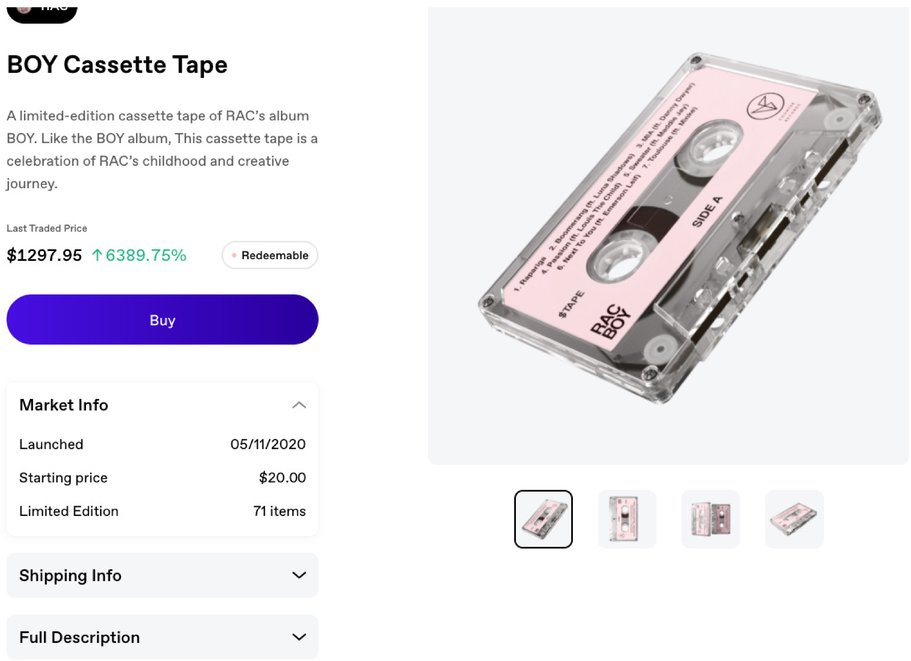
22 | Anatomy of an Aavegotchi.



[Source: Aavegotchi whitepaper]

While the digital art and collectible market grows, what if NFTs could also represent revenue bearing assets, like a song that could be sold as a limited NFT and also allow a musician to profit off of secondary sales? The Grammy-winning artist RAC used the Zora platform to release a new album with this model. Zora aims to disrupt "hypebeast" culture where an collectible item is dropped and sells for ten times the price hours later, by giving each real item a unique NFT that can be redeemed for merchandise, and also carry rights to the real-world sales revenue as the item is resold.

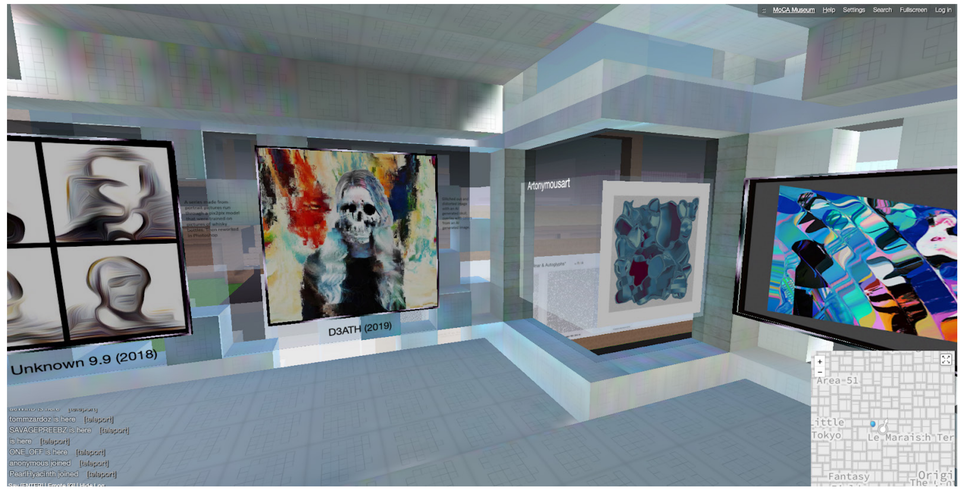
23 | RAC released a limited edition BOY Cassette tape, combining physical goods with NFT rights of ownership.



ENTER THE METAVERSE

If you've made it this far, prepare to enter the so-called MetaVerse, a traversable network of immersive digital worlds. The writer Neal Stephenson might have been the first to coin the term "metaverse" in his 1992 novel Snow Crash, where he imagined an virtual reality world where players would interact with "avatars" representing themselves and other players. There are now several entirely virtual worlds on Ethereum. On Cryptovexels, players can buy land, build stores and even display the NFT art they own in art galleries. On Decentraland users simply connect their MetaMask wallet and can create a virtual avatar and explore a virtual world where they can also buy and sell properties, build worlds, and even attend conferences. Some mini games reward players with NFTs that can then be resold on OpenSea, an NFT marketplace.

24 | A screenshot of the Museum of Crypto Art (MOCA) in Cryptovexels.



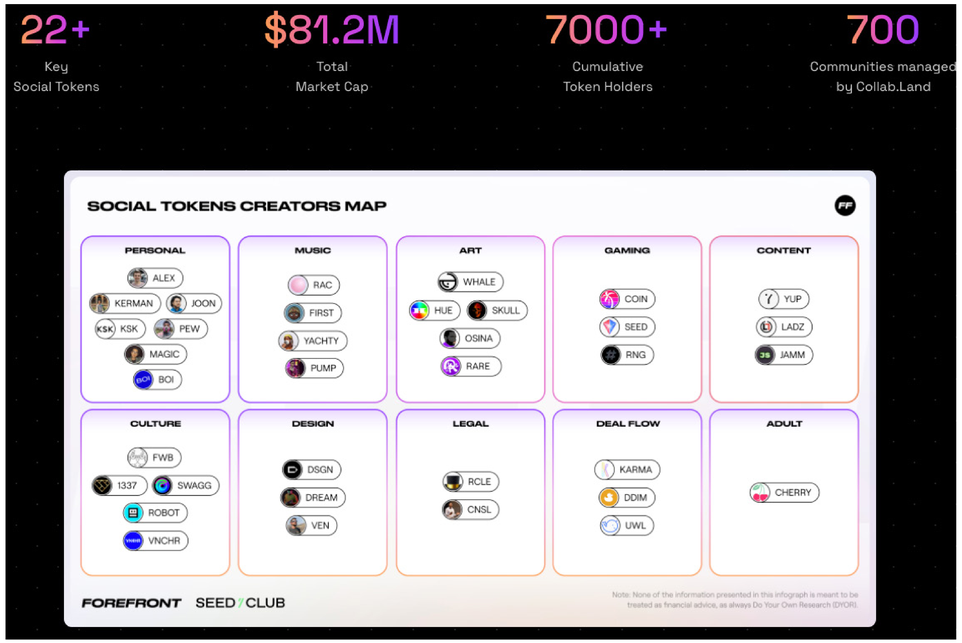
In-game virtual items are already more than a $10 billion market (Fortnite alone sells around $2 billion in-game items a year). But despite this growing market, the existing structures keep the items limited to the world in which they were created, and lack transferable rights. According to Eric Elliot, "Fortnite's digital items only work in Fortnite, and if Epic Games ever decided to shut Fortnite down, those items would be rendered worthless overnight. A multi-billion dollar market would vanish into the ether." Because of the composability and open source properties of Ethereum, the in game items you earn or purchase can be transferable to other Ethereum-based applications, or even traded directly on decentralized exchanges like Uniswap.

25 | Just a lonely avatar wandering around Decentraland.

SOCIAL MONEY FOR COMMUNITIES AND CREATORS

Just like with the growth of digital NFT art marketplaces, COVID-19 has forced artists and creators to rethink how they can connect with their fans and monetize online. One such platform, Roll, is already beginning to catch on with celebrities like Lil Yachty, Akon, and Ja Rule, all of whom are launching social tokens. Roll uses a link-based system so you can instantly send social money to another user on Roll, or withdraw from your Roll wallet to send to a personal Ethereum wallet like MetaMask. With more than 20 different types, the estimated size of the total social token market cap is $81.2 million.

26 | Social token creators map



[Source: Forefront]

Tokens that provide access rights to online communities are now possible because of new tools like CollabLand. CollabLand acts as a bridge between chat applications like Telegram and Discord and your MetaMask wallet. One such community, Friends With Benefits (FWB) uses CollabLand, which to the users appears as a bot that ensures community members are holding enough FWB tokens in their MetaMask wallet to access various Discord channels. CollabLand and FWB will be rolling out a tipping feature in the native FWB token for community members to signal support for substantive contributions to channels that range from music production, NFT discussions, breaking news, memes, Substack articles, and trading advice. While Ethereum-based social media apps that monetize engagement like Peepeth and Pepo have been attempted with varying degrees of success, Q4 2020 showed that grassroots communities using existing popular community platforms like Discord may be the best testing ground for more profound experiments in how to create a social community with its own unit of accounting.

DECENTRALIZED AUTONOMOUS ORGANIZATIONS (DAOS)

Now that we have discussed some of the core innovations of DeFi applications, you might be asking yourself: Who is deciding the future of these applications? Almost all of the major DeFi applications, from Uniswap to Aave to MakerDAO, are now governed by DAOs, which stands for Decentralized Autonomous Organization.

DAOs are governing bodies that oversee the allocation of resources tied to the projects they are associated with and are also tasked with ensuring the long term success of the project they support. This task is no small feat either, as DAOs conservatively oversee more than $480 million.

27 | Total DAO assets under management.

Rank	Name	Platform	USD Value	Total In	Total Out	Members	Proposals	Voters	Voter Particiption
1	BarnBridge Launch...	Aragon	93,554,095.37	211,052,438.19	117,498,342.82	15	40	13	86.7
2	API3 DAOv1	Aragon	93,448,770.21	270,738,873.38	177,290,103.17	30	25	9	30.0
3	PieDAO	Aragon	74,059,951.81	80,956,804.99	6,896,853.18	3633	1	6	0.2
4	Airalab	Aragon	52,692,915.09	167,004,039.03	114,311,123.95	11	127	12	100
5	mStable	Aragon	50,435,713.87	158,023,633.69	107,587,919.82	13	45	7	53.8
6	dxDAO	DAOstack	31,994,475.92	34,312,299.11	1,633,816.36	448	438	113	25.2
7	pNetwork	Aragon	16,795,616.70	18,972,473.71	2,176,857.01	1308	0	0	0.0
8	Aragon Network Bu...	Aragon	11,633,839.68	63,097,107.20	53,486,062.18	3	231	4	100
9	MetaCartel Ventures	Moloch	11,552,298.02	18,880,626.33	7,328,328.31	100	288	64	64.0
10	Aragon Trust	Aragon	8,356,696.76	27,187,072.84	18,830,376.08	5	69	4	80.0
11	The LAO	OpenLaw	7,701,980.21	16,458,541.45	8,756,561.24	89	151	42	47.2
12	Aavegotchi	Aragon	5,633,823.29	48,152,708.25	42,518,884.96	3	5	4	100
13	Moloch DAO	Moloch	3,335,917.86	9,758,593.98	6,422,676.12	99	133	59	59.6
14	Aragon Network	Aragon	3,035,504.35	4,042,716.11	1,007,211.76	5	14	4	80.0
15	Dhedge	Aragon	2,401,096.09	2,633,312.25	514,951.09	7	10	6	85.7
16	Bancor 0x3EcD508...	Aragon	1,706,603.72	6,722,754.46	5,016,150.74	4356	0	0	0.0

[Source: DeepDAO]

Decentralized Autonomous Organizations inscribe as many rights and responsibilities that a corporation or nonprofit typically manages to self-executing smart contracts. Members of DAOs use tokens to vote on the rules of a larger decentralized protocol or system. While the most famous "DAO" was subjected to a major hack in 2016 just when Ethereum was beginning to take off (chronicled in Matt Leising's new book, Out of the Ether), the concept of DAOs has still holds a powerful appeal to projects that want to extend governance decisions to the community of it's token holders. MakerDAO is one such example, where holders of the MKR governance token vote on changes to the DAI stablecoin protocol.

Thus far, most DAOs operate under the following framework. Anyone who holds a certain amount of tokens can suggest changes to the underlying protocol. These proposals can be technical in nature, such as Compound's Proposal #31, which sought to adjust the reserve factors for various Compound markets, or more ideological, such as Dharma's Uniswap Proposal #2 for the Uniswap DAO, which called on Uniswap to reward their users with UNI since they were left out of the initial token distribution.

After a suggestion has been successfully proposed, the community of governance token holders for the respective project must vote on if they are "for" or "against" the proposal. Different DAOs have different quorum requirements in order for a proposal to pass, but as long as that quorum is met, usually majority rules. Each DAO has some core differences just like each democracy around the world varies in how they execute democratic principles. There are distinct levels of checks and balances within the different DAOs.

Because the composition of smart contracts to create DAOs are open source, it's becoming easier to use existing DAO structures, such as Aragon, MolochDAO, or DXdao to manage projects. Aragon is the most popular DAO framework, used by BarnBridge, PieDAO, and Aavegotchi, among others. DAOstack (or dxDAO), developed by Gnosis, manages Omen.eth (a prediction market platform), Swapr.eth (an automated market maker), Mesa.eth (a decentralized exchange), and Rails.eth (a micropayments system). In total, DXdao manages $30.9 million among 448 members.

28 | Top DAOs by assets under management

Top DAOs

Rank	Name	Platform	USD Value	Total In	Total Out	Members	Proposals	Voters	Voter Particiption
1	BarnBridge Launch...	Aragon	123,215,826.17	277,980,006.96	154,764,180.80	15	40	13	86.7
2	API3 DAOv1	Aragon	87,052,221.75	248,524,608.92	161,472,387.17	30	28	9	30.0
3	PieDAO	Aragon	72,472,654.56	79,406,226.68	6,933,572.12	3712	1	6	0.2
4	Airalab	Aragon	52,981,717.21	167,778,593.95	114,796,876.74	11	131	12	100
5	mStable	Aragon	44,810,223.57	140,384,092.26	95,573,868.69	13	45	7	53.8
6	dxDAO	DAOstack	30,908,242.36	33,220,311.85	1,647,352.66	448	450	113	25.2
7	pNetwork	Aragon	14,836,699.69	16,985,704.98	2,149,005.29	1317	0	0	0.0
8	Aragon Network Bu...	Aragon	11,329,543.80	61,346,899.07	51,985,686.63	3	234	4	100
9	MetaCartel Ventures	Moloch	11,240,148.08	18,395,369.12	7,155,221.03	100	291	65	65.0
10	The LAO	OpenLaw	7,875,970.28	16,396,763.03	8,520,792.75	89	152	42	47.2
11	Aavegotchi	Aragon	5,434,314.97	48,721,787.00	43,287,472.03	3	6	4	100
12	Aragon Trust	Aragon	3,645,606.37	26,218,577.43	22,572,971.06	6	69	4	66.7

[Source: DeepDAO]

While many of the DAOs described above are experimenting with novel governance structures, some DAOs have opted to replicate more traditional governance models. For example, The LAO (a limited liability autonomous organization) is an investment DAO that closely resembles a venture capital firm. You must be an accredited investor in order to join this DAO, and once accepted, members discuss various projects to allocate The LAO's funds towards. When a project is seriously being considered, members of The LAO then vote on if the project should receive funding from the group.

DAOs will continue to be a growing force in DeFi and beyond.

The Hacks, Exploits, and DeFi Inventions that Push Innovation

It wouldn't be a DeFi report without describing some exploits of DeFi protocols. Smart contract security has long been a critical area for avoiding potentially catastrophic vulnerabilities after launch. ConsenSys Diligence combines hands-on review from veteran smart contract auditors with open source security analysis and runtime verification tools like MythX and Scribble. Smart contract bugs are found weekly in Ethereum, some by white hat hackers and some intent on exploiting smart contracts for their own profit. Diligence has a regular newsletter that analyzes various hacks and exploits so that developers can be aware of best practices.

As long as there is value on the internet, there are going to be people intent on trying to take it. But in other cases, it is a truly novel invention, such as Aave's "flash loan" or the "flash swap" by Uniswap, that have enabled arbitrage schemes at a scale and speed not previously imagined.

FLASH LOANS AND FLASH SWAPS

A flash loan is a type of Ethereum transaction where a user borrows an asset, transacts with that asset, and then repays the loan — all within a single transaction. The innovation of flash loans is they allow a user to borrow the total amount of assets available from a market without having to post collateral. Since the flash loan must be repaid in the same transaction for that transaction to even be executed, there is no risk that the borrower will not pay the loan back. Since there is no risk of the borrower being unable to pay the loan back, they can borrow an unlimited amount.

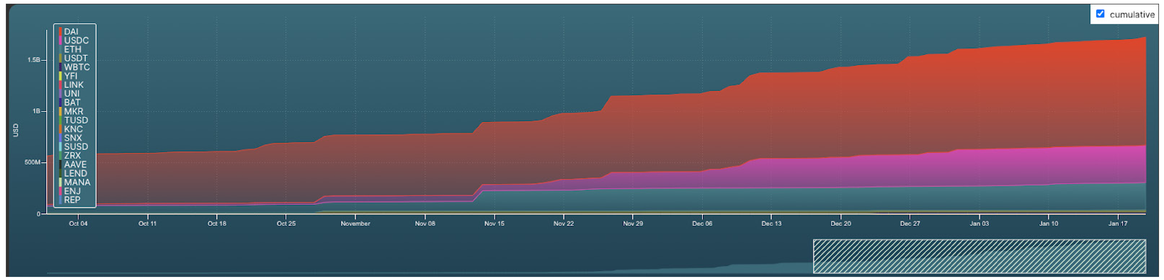
One flash loan use case is to swap the collateral supporting a loan. Another is to liquidate a liquidy pool on a decentralized exchange in order to find a better interest rate. So if you, for example, had a USDC loan on Compound for a 15% interest rate and saw an 8% rate on Aave, you could withdraw the asset from Compound, pay your debt, and then borrow for a lower interest rate on Aave — all within one transaction.

But the most notorious use case is arbitrage, where users exploit the priced differences of an asset across various decentralized exchanges. Stablecoins like DAI and USDC fluctuate slightly day to day. So if you were to take out a 1,000 DAI flash loan (let's say DAI is trading about $0.98), swap it for USDC (trading at $1.02) and then repay the loan, you can pocket the difference. This all within a single transaction where the user only pays for the gas. However, if during the course of the transaction a user is not able to pay back the loan, the transaction fails. Aave charges a 0.09% fee and requires users to pay back the loan in the same asset they borrowed.

Like flash loans, “flash swaps” can also be used for arbitrage, and enable traders to swap assets and use them elsewhere before returning them at the end of the transaction. Uniswap introduced flash swaps, and can allow a user to withdraw all the liquidity of any ERC20 token from Uniswap as long as they 1) pay for the withdrawn ERC20 tokens with the corresponding pool/pair tokens, and 2) return the ERC20 tokens. If you don’t, the transaction also fails, and you lose the cost of gas. Uniswap takes a swap fee and allows users to return flash swaps in either asset that’s being exchanged.

Aave issued $1.7B in flash loans in 2020, tripling demand in Q4 2020 alone.

29 | Aave issued $1,726,089,921 in flash loans in 2021.



[Source: Aavewatch

Several DeFi protocols were also the victims of flash loan-based exploits in Q4 2020. Harvest Finance lost $34 million, Cheese Bank lost $3.3 million; Akropolis lost $2 million, and Value DeFi lost $6 million.

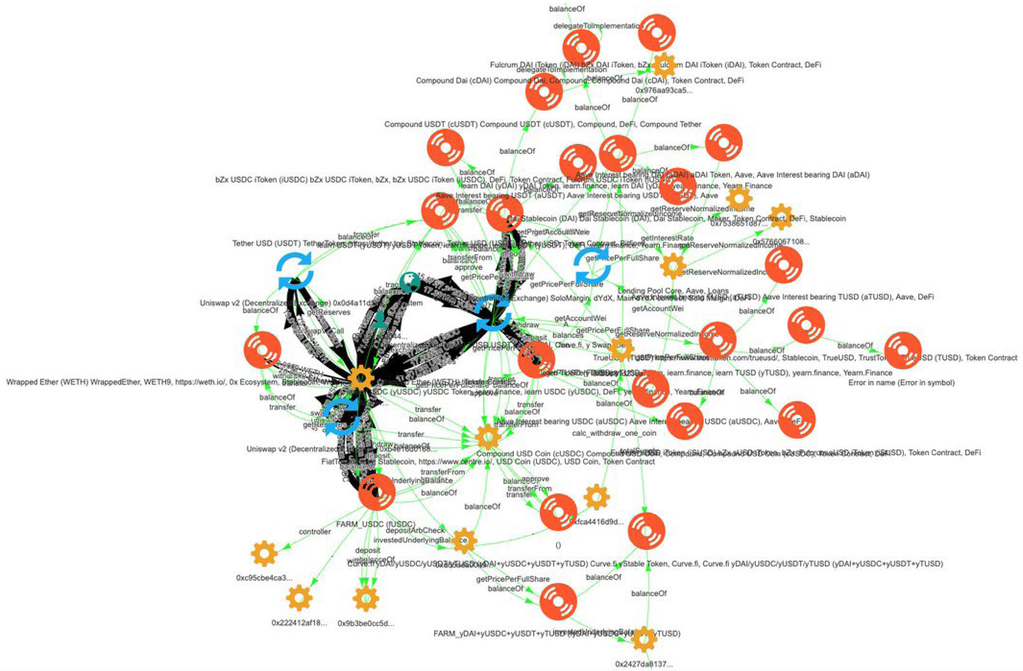
HARVEST FINANCE

In late October 2020, Harvest Finance, a DeFi robo-advisor faced a $24 million dollar flash loan attack. While it initially appeared to be a hack exploiting smart contract logic, upon further investigation it turned out to be a clever exploit in how Harvest Finance’s vault priced the assets that were deposited into it.

Effectively, the market manipulator used a portion of a flash loan to trade 11.4 million USDC to USDT. Because of the large size of this buy, the price of USDT appreciated in value as viewed by Harvest Finance’s oracles. The market manipulator then deposited 60.6 million artificially appreciated USDT into a Harvest Vault. Next, the market manipulator pushed the price of USDT down by selling 11.4 million USDT for USDC. The price of USDT was now artificially depreciated as viewed by Harvest Finance. The market manipulator then withdrew all of their holdings from the Harvest Vault, which came out to 61.1 million USDT, netting a profit of 500,000 USDT. This difference came from the fact that when the arbitrager initially deposited USDT into the vault at the artificially appreciated rate, Harvest Finance credited the user with depositing more value than it should have. Furthermore, when the market manipulator withdrew the USDT, they did so when USDT was artificially depreciated, which meant that Harvest Finance once again credited the market manipulator of having more value in the vault than it should have. You can view the entire transaction history on Etherscan.

Finally, the market manipulator then turned the USDT into ETH, then WBTC, then renBTC, and finally BTC for a portion of the funds to try and cover their tracks, repeating this process until they netted about $24 million in total profits.

30 | The very complex Harvest Finance flash loan arbitrage.



[Source: Julien Bouteloup]

The significance of this exploit is the ways in which decentralized financial protocols are still not immune to price disparities in on-chain data oracles because of market manipulation. The flash loan in this instance was able to push the price of USDT simply by taking out a flash loan and selling it all in one trade. Fitting for decentralized finance, these trades were likely carried out by arbitrage bots. Arbitrage DAO is one such arbitrage fund (built by Stake Capital) which uses a combination of on-chain liquidity and off-chain bots built for arbitrage opportunities. Many more of these types of exploits may occur in 2021; just as the high-frequency traders on Wall Street were called “Flash Boys”, DeFi in 2021 may yield a new crop of “Flash Boys 2.0.”

Looking Ahead in 2021

DeFi has clearly come a long way this past quarter. Even though the DeFi summer cooled, actual user adoption of DeFi applications continued to soar. Monthly volumes on DEXs have reached an all time high, surpassing $30 billion, which is approximately double what they were in September 2020. Furthermore, there are more than $4.5 billion in DeFi loans outstanding, an increase of more than 300% since September 2020. The total market capitalization of stablecoins have risen to more than $23 billion, which is just under double of what they were in September of 2020.

Yet DeFi is still in its infancy as an industry. In fact, there are many new innovations just on the horizon that will further increase the accessibility and variability of DeFi.

TRANCHE LENDING PRODUCTS

One trend in DeFi to watch out for in Q1 2021 are new tranche lending products, which are being spearheaded by BarnBridge and Saffron Finance. There has been significant interest in these products, as evidenced by BarnBridge's nearly $400 million in TVL just for farming its governance token. It is important to recognize that Saffron Finance contracts have not been audited.

What is a tranche lending product, you might ask? One of the biggest issues with DeFi lending is that the interest rates are always variable, which means they are constantly changing. While you might earn 6.7% APY lending your DAI on Aave today, that rate might be 10% tomorrow or 1% a week from now. The volatility in these variable rates impedes any individual or institution that is looking for predictable and stable returns in their lending products. Innovators in DeFi are devising a solution to this problem: tranches. At the most basic level, a tranche works as follows:

- Users deposit their digital assets into a pool, which has a fixed rate attached to it. This pool of assets is then lent out via lending protocols such as Aave or Compound.
- When the user initially deposits their assets, the user has the option to deposit into Tranche A of the pool or Tranche B.
- Depositors in Tranche A are guaranteed to receive the fixed rate attached to the pool over a fixed time period. For example, if the pool has a fixed return of 10% APY and you deposit $100 into Tranche A, you will receive $110 ($100 principal + $10 in interest) in one year.

So, you must be asking yourself, how can a fixed rate be guaranteed to Tranche A depositors when the pool of assets is being lent out via a protocol that only offers variable rates? That is where the speculators who deposit into Tranche B enter. Depositors in Tranche B are effectively speculating on what they think the realized APY of the pool will be. If the realized interest rate is higher than 10% APY after one year, then all of the extra interest that was generated would be distributed to the depositors of Tranche B.

But what happens if the realized interest rate ends up lower than the rate listed on the pool, in this case 10%? Tranche A will still be rewarded their 10%, but in this scenario, the realized interest rate would not cover the listed rate. Thus, the principal of deposits in Tranche B would be reduced in order to compensate the depositors in Tranche A. You can probably see why the depositors in Tranche B are called speculators now!

Tranche lending is only one of the many new innovative technologies being developed in DeFi. Furthermore, tranche lending exemplifies just how composable all of these innovations are. The teams who devised this tranche lending system did not come from Compound or Aave, yet they built an entirely brand new product on top of the existing lending protocols.

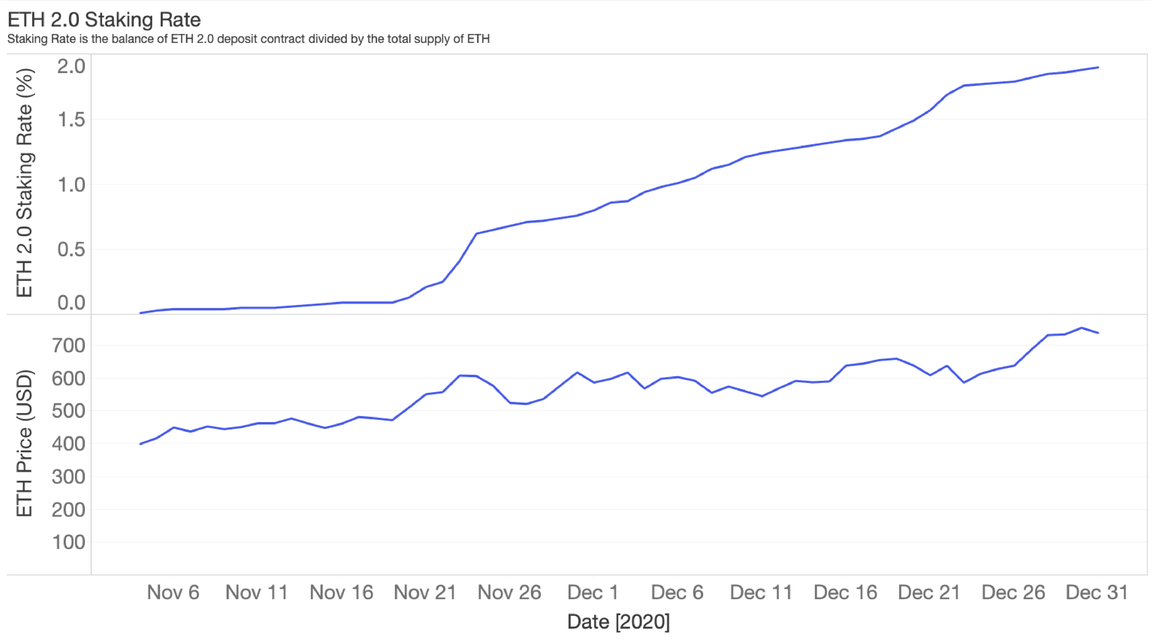
That being said, there are inherent risks to the composability of Ethereum smart contracts. The more that various financial products rely on one another, the more intertwined the risks of these products become. If one of the underlying protocols fails, they present a systemic risk to the other related products that interact with the protocol. The crypto market crash on March 12th, 2020 is a recent example. Over the course of 36 hours the price of ETH fell sharply, rendering MakerDAO vaults inaccessible due to network congestion, which also caused price oracles to fail and ultimately, cost users millions in losses.

One must not overlook the other inherent risk in the tranching of assets, especially given the mortgage-backed securities crisis that precipitated the 2008 financial crash. Tranches of junk mortgage-backed securities were repackaged as CDOs, further sold. Few anticipated the dynamics of how these new structured products would interact with macro economic trends, like a housing market crash. Another distinct risk with these tranche products is that they are largely new types of structured products being built by non-financial experts. Structuring products is an incredibly complex practice usually only done by the saviest financial engineers at investment banks. Conveying a robust understanding of how these structured products in DeFi will work to market participants will be imperative in order to avoid significant financial loss.

ETH2 DERIVATIVES

In the Q3 DeFi report, we predicted that the returns in DeFi protocols might cause some users to hold back in delegating ETH to the deposit contract. It appeared that was the case until a sudden rush of deposits in the final 36 hours on November 24th, 2020 met the 524,288 ETH threshold to launch the Beacon Chain. Since the successful launch of the Beacon Chain 2,778,946 ETH has been staked, which is 2.2% of the entire supply of ETH in circulation (According to CoinDesk, some Ethereum investors believe the percentage of ETH used for staking will grow to be as high as 30% in the future).

31 | Eth staking rate.



[Source: CryptoQuant]

Everyone that committed ETH to stake and validate on the Eth2 Beacon Chain went in knowing that they might not be able to withdraw their ETH until for a couple years. However, there are already a number of DeFi solutions for stakers wanting liquidity and mobility on their staked ETH. LiquidStake, for example, allows users to take out a USDC loan on their staked ETH. Coinbase is promising the ability to trade a derivative version of ETH on the ETH a user locks in the Beacon Chain. Lido provides users with a derivative, stETH, in return for staking with their service. The stETH is already trading on decentralized exchanges, which raises an interesting new type of ETH derivative: one that gains value in accordance with the staking rewards issued to validators successfully attesting blocks on Eth2.

DEFI ON ETHEREUM LAYER 2 AND OTHER PROTOCOLS

If you had taken our advice at the beginning of the report and tested out a few of these DeFi protocols, you might have been taken aback by the gas costs to execute a trade, mint an NFT, or interact with a protocol. While the community anticipates a more scalable and cheaper Eth2, scalable solutions like Layer 2 protocols that batch transactions before attesting to the Ethereum mainnet.

One such Layer 2 technology is rollups, which take much of the burden of computation and storage out of the blockchain, and use the chain just enough to benefit from its security guarantees. Rollups are starting to attract gas guzzling DeFi protocols. Loopring's zkRollup solution now holds more than $100 million, and the derivatives platform, Synthetix announced that SNX staking would go live on Optimism, which uses optimistic rollups. Rollups will increasingly play a role in the Eth2 roadmap as well. As Ben Edgington of ConsenSys' Teku client noted, "With the rollup centric roadmap, shards only need to take care of ordering data. Rollups are data-hungry; the more data they have the faster they can go."

With high gas fees on Ethereum, different types of blockchains may increasingly try to attract Ethereum-based DeFi applications. FTX, a popular crypto exchange in Hong Kong, decided to build its decentralized exchange called Serum on Solana. In November 2020, Serum generated $111 million in volume, significantly less than

the $17 billion in volume on Ethereum-based DEXes in the same month, but also not negligible. The 1inch.exchange-backed project, Mooniswap, also decided to go with the Near Protocol for its automated market maker (AMM) DEX. Sergej Kunz, the co-founder of 1inch, claimed, "By building on NEAR, we'll be able to experiment with sharding and be prepared for the arrival of Ethereum 2.0."

The network effects of Ethereum are one of the major reasons why more DeFi applications haven't been quick to rewrite their smart contracts in a new protocol. It's why so many crypto assets like Bitoin and Filecoin are being tokenized on Ethereum, a trend we expect will accelerate in 2021. Though growing quickly, the overall DeFi market size is comparably small compared to other commercial and financial markets. Many of these sophisticated new types of financial products and services seek initial liquidity from the groups of traders already familiar with Ethereum-based crypto wallets like MetaMask, a strong track record of network uptime, robust auditing tools and services, and on chain data feeds and oracles.

Interoperability between blockchains remains an active research space, and while we predict more more projects to consider moving to other protocols ahead of Eth2, we think the gravity of Ethereum will push more activity to Layer 2 protocols already interoperable with Ethereum. Additionally, since Layer 2 technologies like rollups are increasingly becoming incorporated in the Eth2 roadmap, DeFi applications might be better off waiting to see how research teams figure out cross-rollup data execution and consensus before venturing too far from widely-adopted Ethereum standards.

CBDCS: WHAT HAPPENS WHEN FIAT CURRENCY LANDS ON MAINNET?

Public Ethereum already has digital dollars — more than $20 billion (see Figure 6). When ConsenSys published its whitepaper, "Central Banks and the Future of Digital Currency," at the World Economic Forum in January 2020, the backdrop was a dramatic shift in the mechanics of money. Since then, ConsenSys announced four distinct Central Bank Digital Currency (CBDC) projects with the Hong Kong Monetary Authority, Bank of Thailand, Australian Reserve Bank, and Societe Generale. Each of these projects uses ConsenSys Quorum, a variant of the Ethereum mainnet which allows for permissioned networks, built-in privacy, and higher transaction throughput. What might it look like for a CBDC to be deployed on the Ethereum mainnet?

The design decision around designing CBDCs often splits into (1) wholesale CBDCs, which largely reinforce and optimize the role of banking institutions relative to the central bank's money management authority, (2) retail CBDCs, which would bypass the banks and go directly into the wallets of consumers. The first option is about efficiency and industry cost mutualization. The second is more deeply transformative, and analogizes more closely to owning an Ethereum token and using it to transact.

China's own CBDC project (they call it a Digital Currency and Electronic Payments System or DCEP) is an interesting example of what a digital currency could look like that is managed by a centralized database; as digital yuan are transferred to different phone-based wallets and commerce sites, the total circulating supply would be reconciled with a database held by China's central bank. This is not too different

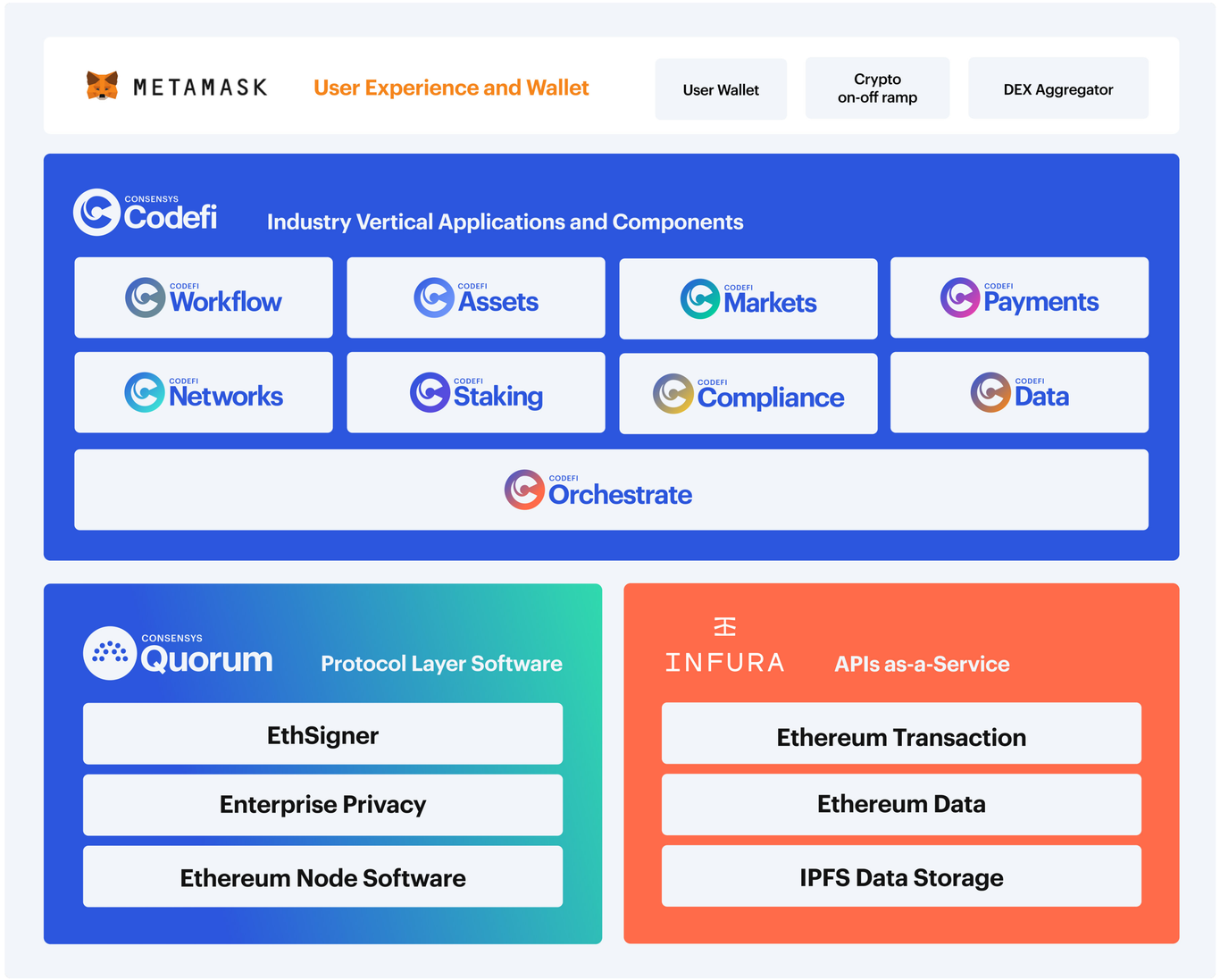
from the ways in which financial institutions already hold accounts at central banks. There are ways in which programmable assets themselves, like a digital yuan could be disruptive — you could build taxation directly into consumer transaction flows, or implement universal basic income, or deliver Covid-related distributions with ease. But at its essence, the data by which the system relies on is only responsible for settling digital yuan.

With the proliferating programmable token standards on Ethereum, new types of business logic can be incorporated directly in Ethereum, rather than sitting outside of the network. Instead of gateways and business logic that used to sit outside of the network. The CBDC projects today ask the question of how to move money around. Bitcoin has answered this question, and perhaps an applied architecture like permissioned Ethereum will solve this for national currencies. The deeper question is — what does an economy connected to a CBDC look like? What is the shape of merchants and applications that accept digital currency? Where do they perform their economic functions? If we think the venue for computing will increasingly be on blockchains, that suggests that CBDC rails should come not just with pre-installed national money, but also pre-installed applications for the use of that money. A payment rail will only be adopted if it is useful, and if it is applicable to a meaningful portion of human economic activity. Would you rather store value, or create it?

Appendix

THE CONSENSYS PRODUCT STACK

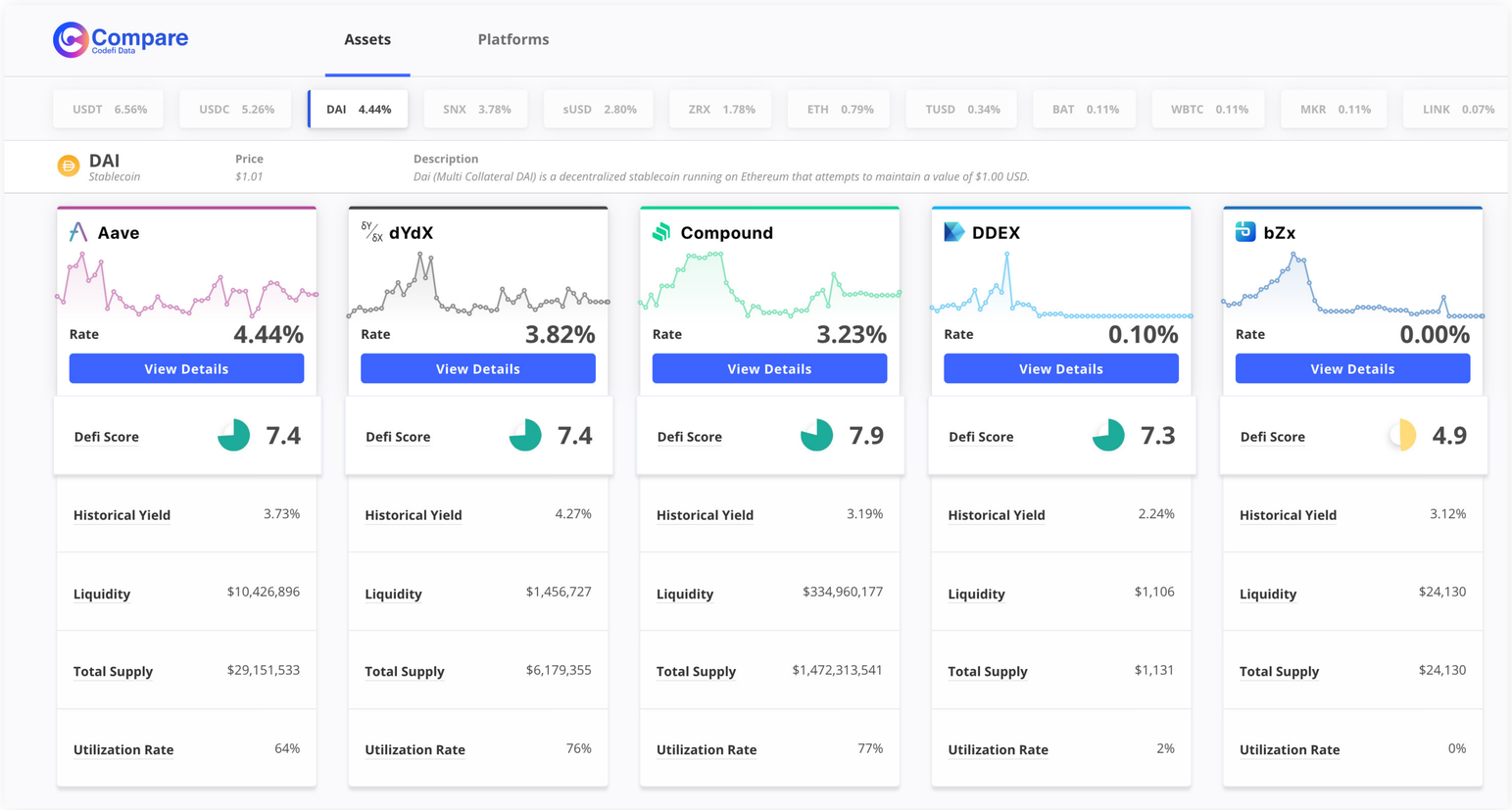
ConsenSys is the leading Ethereum software company. We enable developers, enterprises, and people worldwide to build next-generation applications, launch modern financial infrastructure, and access the decentralized web. Our product suite, composed of Infura, Quorum, Codefi, MetaMask, Truffle, and Diligence, serves millions of users, supports billions of blockchain-based queries for our clients, and has handled billions of dollars in digital assets. Ethereum is the largest programmable blockchain in the world, leading in business adoption, developer community, and DeFi activity. On this trusted, open source foundation, we are building the digital economy of tomorrow. To explore our products and solutions, visit consensys.net.



OTHER DEFI OFFERINGS BY CONSENSYS

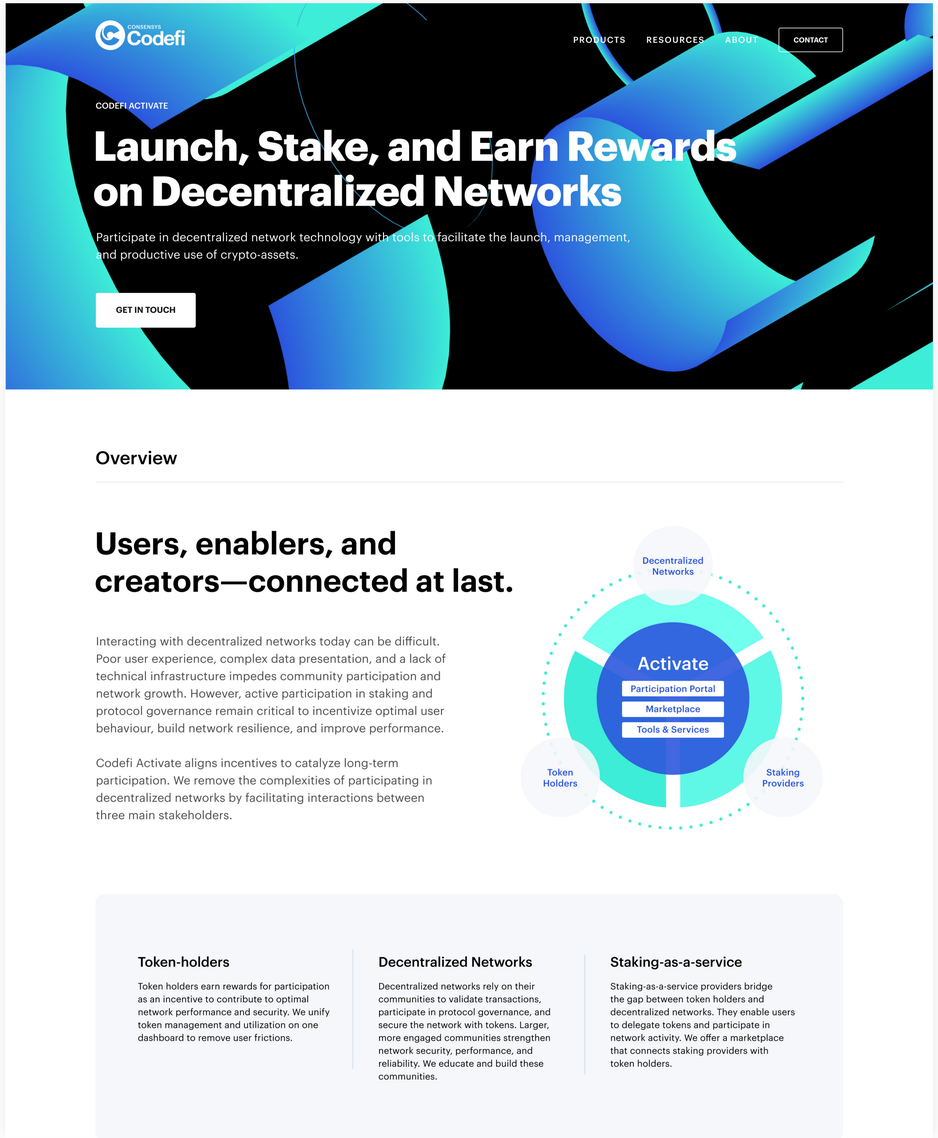
Analyze risk and assess performance on DeFi protocols with DeFi Score.

DeFi Score allows users to assess platform risk by measuring smart contract security, centralization, collateralization, and liquidity.



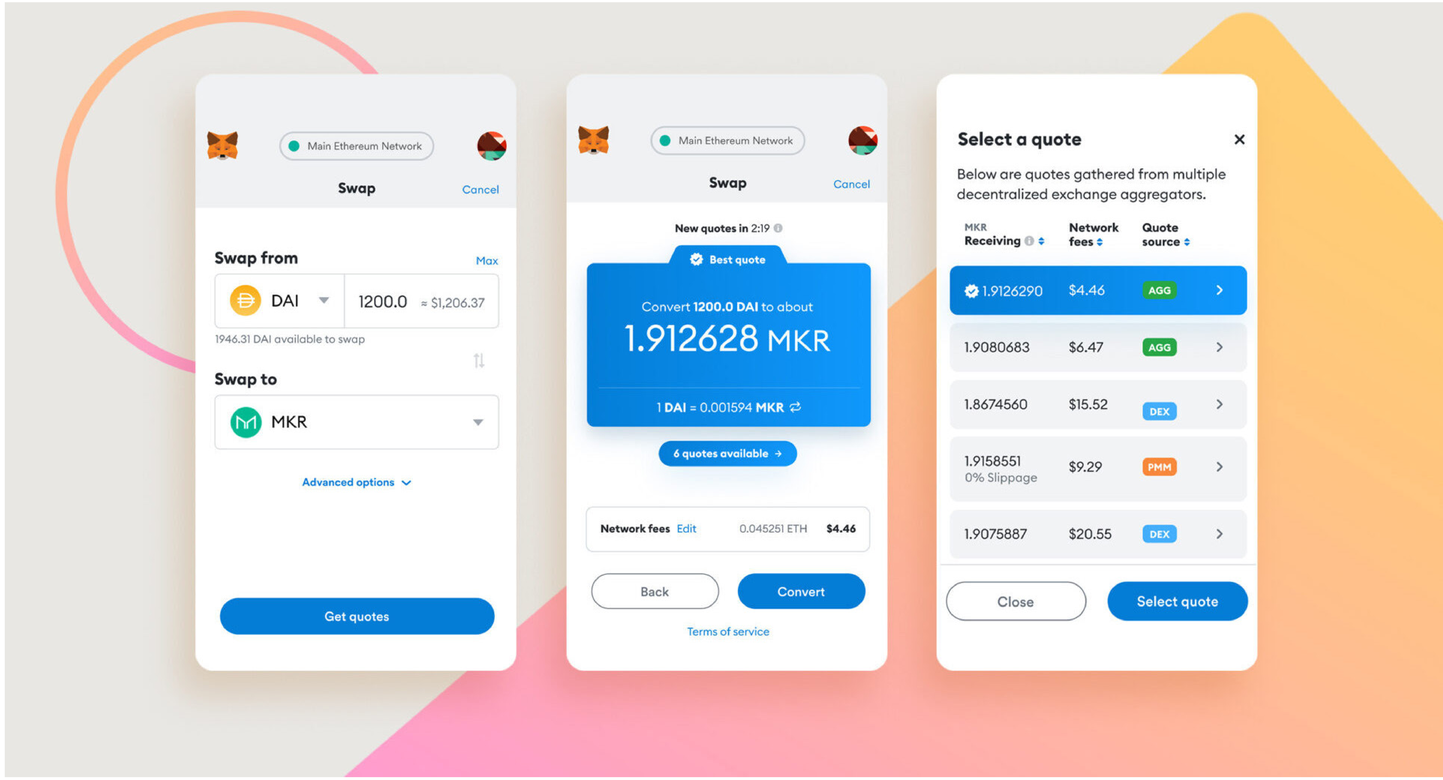
LAUNCH, STAKE, AND EARN REWARDS ON DECENTRALIZED NETWORKS WITH CODEFI ACTIVATE

Codefi Activate removes the complexities of participating in decentralized networks. We unify token management and utilization on one dashboard for token holders, and we build strong decentralized communities and help skale Ethereum projects.



USE DEFI PROTOCOLS WITH METAMASK.

MetaMask provides an essential utility for blockchain newcomers, token traders, crypto gamers, and developers with over a million downloads and counting. You can now swap tokens directly using the desktop extension, with swap features on mobile coming very soon.



CONSENSYS DILIGENCE

Ensure smart contract security on DeFi protocols with audits from ConsenSys Diligence.

ConsenSys Diligence uses industry-leading blockchain security analysis tools, combined with hands-on review from veteran smart contract auditors to ensure smart contract security.