PRODUCTS
APPLICATION SUITE (/APPLICATION-SUITE)
ORCHESTRATE (/ORCHESTRATE)
WORKFLOW (/WORKFLOW)
ASSETS (/CODEFIASSETS)
MARKETS (/MARKETS)
PAYMENTS (/PAYMENTS)
NETWORKS (/NETWORKS)
STAKING (/STAKING)
COMPLIANCE (/COMPLIANCE)
DATA (/DATA)
DIGITAL ASSETS
OVERVIEW (/ASSETS-OVERVIEW)
BENEFITS (/ASSETS-BENEFITS)
FEATURES (/ASSETS-FEATURES)
USE CASES (/ASSETS-USE-CASES)
CASE STUDIES (/ASSETS-CASE-STUDIES)
REQUEST A DEMO (/ASSETS-REQUEST-A-DEMO)
INITIATIVES
CASE STUDIES (/CASE-STUDIES)
INSIGHTS (/OUR-INSIGHTS)
BLOG
ALL POSTS (/ALL-BLOG-POSTS)
PRODUCT ANNOUNCEMENTS (/BLOG-PRODUCT-ANNOUNCEMENTS)
CLIENT ANNOUNCEMENTS (/CLIENT-ANNOUNCEMENTS)
CODEFI ACTIVATE (/BLOG-ACTIVATE)
NEWSLETTER (/NEWSLETTER)
ABOUT
WHO WE ARE (/WHAT-WE-DO)
MEDIA (/MEDIA)
PRESS (/PRESS)
CONTACT (/CONTACT)

May 19, 2020

Security Risks in Ethereum DeFi

Technology News (/blog/category/Technology+News)

Approaches to monitoring and protecting against risks

2020 has proven a critical year for the Ethereum DeFi ecosystem. In addition to celebrating over $1bn USD locked in DeFi and significant platform milestones, the industry has been subject to frequent occurrences of minor and major security incidents across both new and established DeFi applications.

5 DeFi security incidents (https://mp.weixin.qq.com/s/rv5-w2308Jdjumvho6doTQ) **that happened in April:**

- Uniswap: on 18th, $340k USD stolen through a reentrancy attack vector
- Lendf.me: on 19th, $25m USD stolen through a reentrancy attack vector; funds are re-issued after team's negotiation with hacker.
- Curve: A stablecoin exchange platform, revealed that they found and solved a bug in the

Archive

September 2020 (3) (/blog?month=09-2020)
August 2020 (6) (/blog?month=08-2020)
July 2020 (7) (/blog?month=07-2020)
June 2020 (5) (/blog?month=06-2020)
May 2020 (4) (/blog?month=05-2020)
April 2020 (7) (/blog?month=04-2020)
March 2020 (2) (/blog?month=03-2020)

sUSD reserve contract.

- PegNet: A cross-chain DeFi platform PegNet suffered a 51% attack when 4 miners in their network controlled 70% hashrate.
- Hegic: 28k USD of liquidity locked in expired options contract by a bug in contract, for which the team promised to compensate affected users with their own funds.

month=03-2020)
February 2020 (7) (/blog?month=02-2020)
January 2020 (1) (/blog?month=01-2020)
December 2019 (4) (/blog?month=12-2019)
September 2019 (2) (/blog?month=09-2019)

Uniswap and Lendf.me - The Reentrancy Attack on ERC-777

The bZx and Maker events of February and March have been well-covered (https://pages.consensys.net/ethereum-decentralized-finance-report-alethio), but we have pulled some data and insight into recent events on the Uniswap and Lendf.me protocols, specifically around the compromise of the ERC-777 token standard that allowed hackers to drain $25m worth of crypto on April 18th & 19th.

The imBTC token is an ERC-777 token released by Tokenlon (https://tokenlon.im/imBTC?locale=en), a DEX running on the 0x protocol. In both the Uniswap and Lendf.me incidents, the hacker(s) exploited a reentrancy vulnerability that arose from the incompatibility between the ERC-777 token standard and the DeFi protocols. Broadly speaking, the reentrancy vulnerability allowed the hacker to essentially re-spend initial deposits of imBTC, effectively providing them with unlimited capital to enact trades or borrows.

Uniswap

The attack was made possible because Uniswap V1 does not have measures in place to guard against this type of reentrancy attack when interacting with the ERC-777 standard. In total, the hacker made away with ~$300k USD in imBTC and ETH (~$141k ETH + ~$160k imBTC).

Interestingly, this attack vector was not unknown to Uniswap or to the crypto community at large. Almost exactly a year before the Uniswap attack, ConsenSys Diligence (http://diligence.consensys.net/) - the security audit service offered by ConsenSys - identified and published (https://medium.com/consensys-diligence/uniswap-audit-b90335ac007) the ERC-777 reentrancy attack vector. Uniswap had plans to address the attack vector, as outlined in their March 23 blog post (https://uniswap.org/blog/uniswap-v2/) about the features of Uniswap V2.

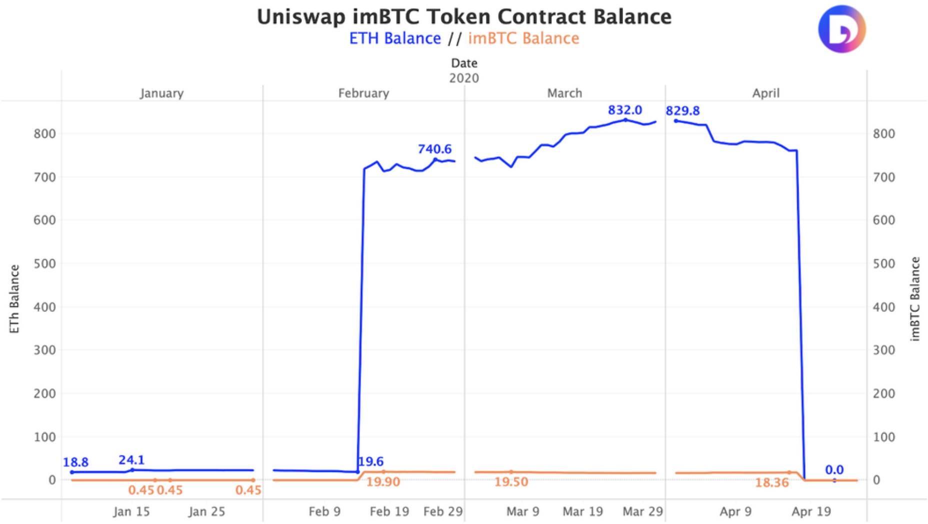

Fig 1. Uniswap imBTC Token Contract Balance

Lendf.me

The Lendf.me incident exploited the same reentrancy vulnerability made available by the incomplete compatibility between the lending protocol and the ERC-777 token standard, but to a far more extensive degree of success. Nearly 100% of Lendf.me's funds - over $24m USD - was drained during the attack on April 19.

Unlike in the Uniswap event, the stolen funds were not limited to just ETH and imBTC. Though the majority of stolen funds were WETH ($10.8m), USDT and HBTC made up for an additional $9.7m, followed by at least 16 other tokens. The graphs below show the asset distribution of compromised followed by at least 10 other tokens. The graphs below show the asset distribution of compromised funds and the monthly token volumes on Lendf.me leading up to the attack on April 19.

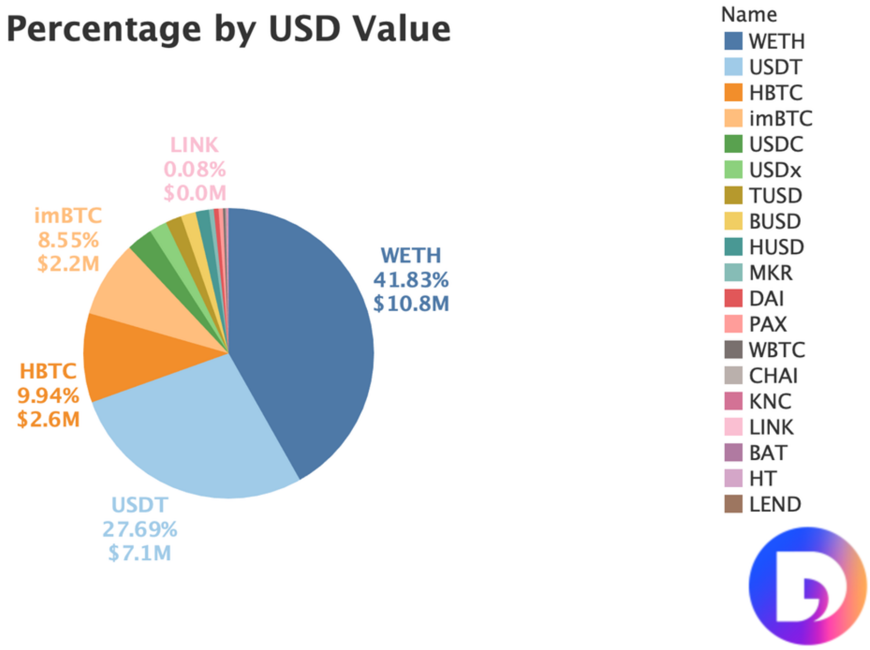

Fig 2. Distribution of Lost Funds by Token Type

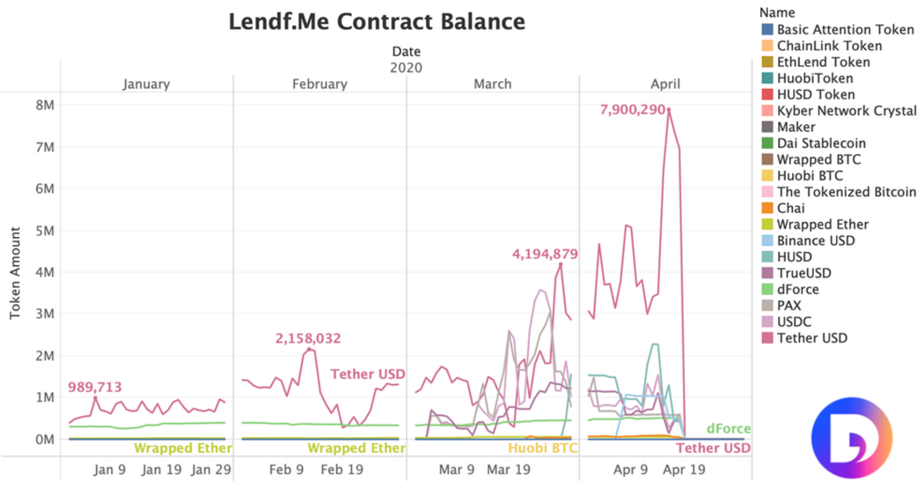

Fig 3. Lendf.Me Contract Balance

In an unexpected turn of events, the Lendf.me hacker(s) returned the stolen funds to the protocol, reportedly because they accidentally exposed an IP address (https://twitter.com/RyanSAdams/status/1252574107159408640) during the attack. The Sankey diagram below shows the flow of funds after the hack. Funds left the Lendf.me contract (green), went through the handler contract (gray), and to the hacker's address (black). After the IP was revealed, the hacker transferred the funds back to the Lendf.me admin address, which then transferred the funds to a recovery address (both in purple). The far right of the graph, where the diagram flows out into many individual fund streams, marks the moment when Lendf.me returned funds (https://medium.com/dforcenet/lendf-me-hack-resolution-part-i-asset-redistribution-plan-9cefee49f209) to individual users.

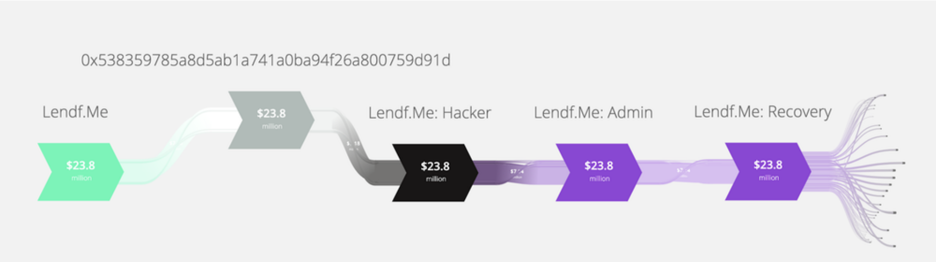

Fig 4. Funds Flow Throughout Lendf.Me Incident

It’s amazing to see how DeFi applications are chained together for a full financial cycle of behavior, and how the dynamics of leverage, arbitrage, lending and trading played out. The synergy between DEX, Loans (also Flashloans) and Oracles opened up opportunities for more financial elements development on Ethereum, as well as lowered the barriers for smaller participants as an inclusive finance world.

What can we do to protect DeFi assets?

Smart Contract Audits

Audit services are able to identify potential contract vulnerabilities through rigorous testing and white hat hacking prior to a protocol or feature launch. Though third party automated tools can identify sets of common vulnerabilities, these tools are most effective when combined with on-hands auditing services.

The Uniswap attack in April was foreshadowed by the audit service ConsenSys Diligence. Moreover, the incidents in 2020 seem to have sparked a new era of transparency among DeFi developers regarding security issues. A developer from the trading protocol Hegic published an open ‘post-mortem’ (https://medium.com/@molly.wintermute/post-mortem-hegic-unlock-function-bug-or-three-defi-development-mistakesthat-i-feel-sorry-about-5a23a7197bce) about a bug in her code that rendered some funds inaccessible. Exchange protocol Loopring identified a front-end vulnerability, paused the exchange, announced to the community (https://twitter.com/loopringorg/status/1258183635338854403), and worked to fix the issue. This sort of transparency is crucial to building trust among new and existing users and to scaling a more secure network of DeFi protocols.

As DeFi protocols grow in number, complexity, and interconnectedness, more security vulnerabilities and compromises are likely to occur. Though regrettable, these incidents are crucial to the secure development of any emerging technology. The more we can use the services and tools available to us to identify and protect against these attack vectors, the more confidently people will interact with the emerging open financial ecosystem.

Monitoring and Ranking tools

Leveraging the openness of the Ethereum blockchain, a host of DeFi-related monitoring tools are available to the public to more confidently interact with financial applications. Codefi Inspect (https://inspect.codefi.network/) is an open source tool to aggregate critical security information about DeFi protocols, including public audits, admin key details, oracle dependency, and on-chain activity. Codefi’s DeFi Score (https://defiscore.io/) is a value of platform risk that can be compared across protocols to better inform users’ decisions when choosing between DeFi applications.

MONITORING NETWORK HEALTH: FOR INDIVIDUAL USERS

On lending platforms, users’ deposits are at risk of being liquidated (https://medium.com/alethio/overlooked-risk-illiquidity-and-bank-runs-on-compound-finance-5d6fc3922d0d) once collateral ratios drop under certain thresholds due to price fluctuations. Figure 5 shows the amount of funds that were “bitten” on Maker’s platform. In November 2018 and March 2020, over $17 million USD of collateral was liquidated on Maker when ETH prices hit historical lows (~$110/ETH in November 2018 and ~$105 in March 2020).

With proper monitoring tools, users can better protect themselves from being the unwilling recipients of automated liquidations on lending platforms. For lending products, a required level of collateral ratio (value of deposit assets, dividing value of borrowed assets, measured in USD in most cases) defines the safety line for vault owners. Once the collateral value drops, the ratio drops, and the vault becomes open for liquidation. Users can track the collateral ratio and decide to repay the borrows or add deposits to keep the vault in a safe condition and out of range of repay the borrows or add deposits to keep the vault in a safe condition and out of range of liquidation. Monitoring tools will play a significant role in users' confident interaction with lending protocols if those tools are providing real-time, reliable oracle price feeds for various assets in order to alert users to take action beforehand.

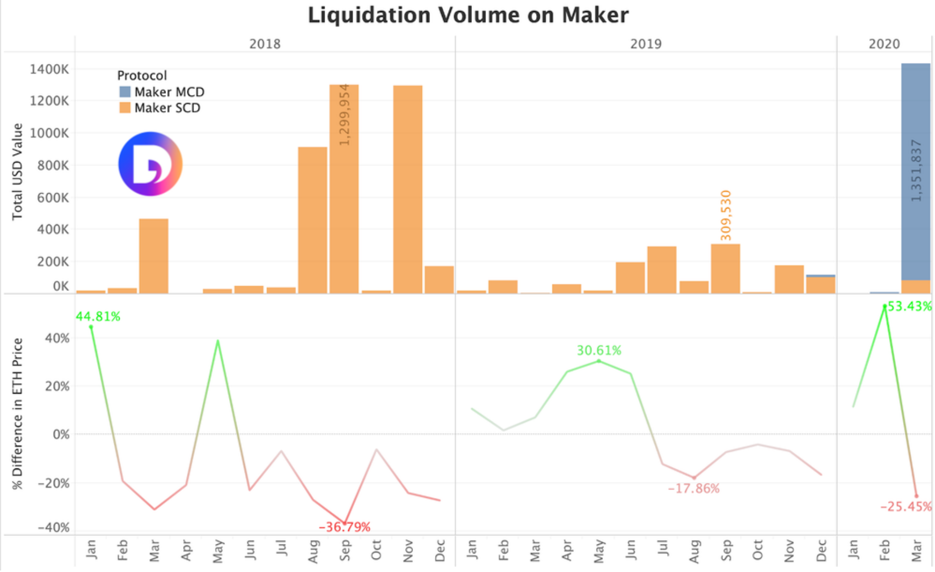

Fig 5. Liquidation Volume on Maker

Another metric to monitor on lending platforms is the *utilization ratio* of the asset liquidity pool. The utilization ratio is calculated by dividing the total amount of outstanding debt by the supply volume in the liquidity pool. If all the funds in the pool are borrowed and not repaid, the utilization ratio reaches nearly 100%.

A dramatic change in utilization ratio can reflect market changes (e.g. the ETH price drop in March) that cause group reactions, or flag the risk of a hacker draining the pool (e.g. the Lendf.me case). Figure 6 shows the asset utilization ratio % for Maker, Lendf.me, and others. In March, we can see the utilization ratio on most platforms spike, likely as a delayed reaction to the market events on March 12th.

The drop in ETH price caused the total supply value (if backed by ETH) on most of these protocols to fall, which caused the utilization ratio to spike suddenly. Meanwhile, because the collateral ratio fell because of the ETH price, a massive amount of outstanding debt was cleared due to liquidations. Over time, therefore, the utilization ratios across many of these platforms decreased.

Lendf.me stands out as an example of what a utilization ratio graph for a hack might look like. In April, we see the utilization ratio for all tokens spike up to 100% almost instantly, which indicates the hacker's exploitation of the ERC-777 reentrancy vulnerability.

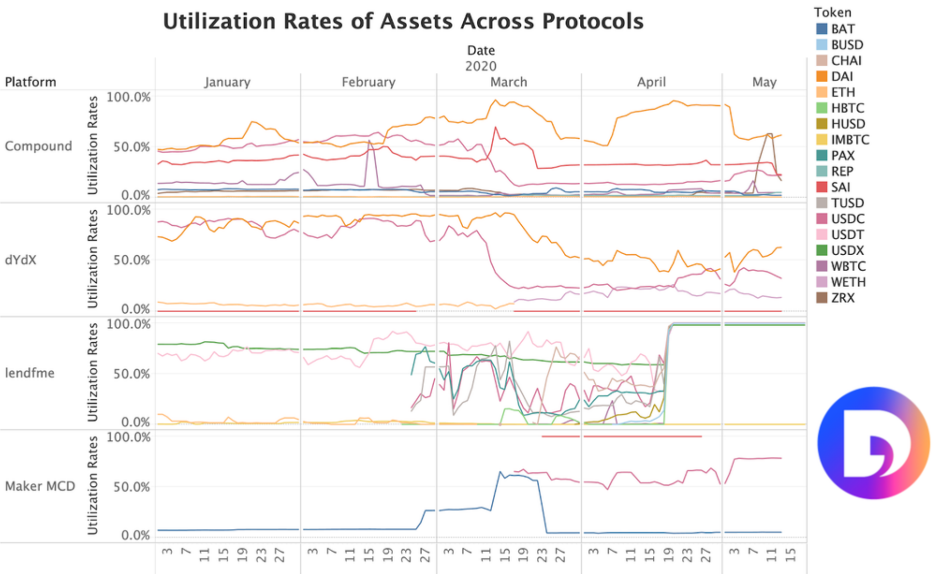

Fig 6. Asset Utilization Rate Across Protocols

On decentralized exchanges, liquidity pool sizes can help users decide which platform is the more resilient reserve. DEXes are one of the most important gates in the arbitrage chain, proven in the bZx case (https://medium.com/@peckshield/bzx-hack-full-disclosure-with-detailed-profit-analysis-e6b1fa9b18fc). Uniswap is one of the most actively-used DEXes, and its liquidity pools are connected to many DeFi/DEX protocol interfaces. Figure 7 shows the size of liquidity pools on Uniswap. The sharpest drop occurred on February 18th, which was the timing of the second bZx attack. On February 18th, Uniswap's liquidity pool dropped because the exploiter borrowed a large amount of WBTC on bZx via the KyberUniswap reserve. The second largest drop occurred on March 13, when crypto markets fell. On March 13, the Uniswap liquidity pool dropped because crypto holders were concerned about market fluctuations and withdrew large amounts of their liquidity from the Uniswap pool. Despite significant drops in the liquidity pool size, however, Uniswap weathered the vulnerabilities and market fluctuations of the past few months very well - demonstrating the resilience of a DeFi protocol with a larger liquidity pool.

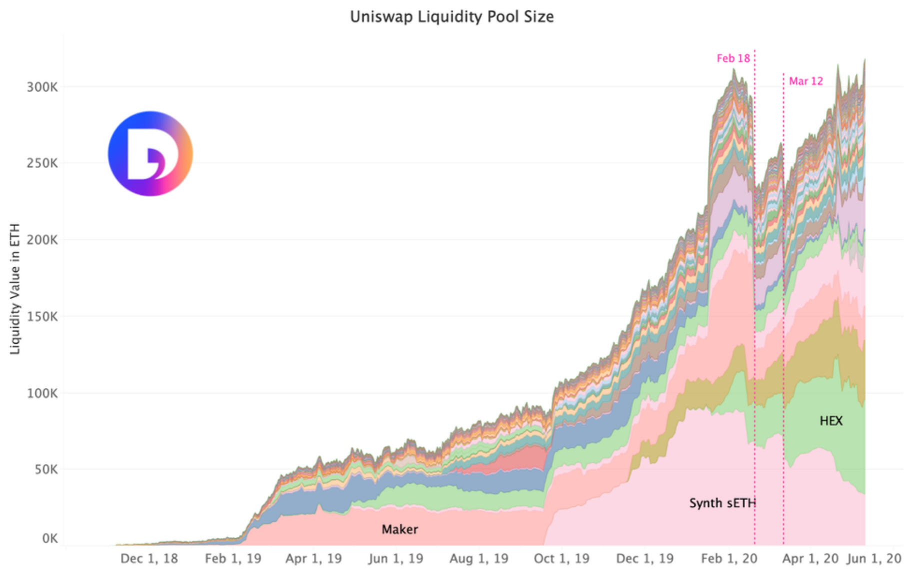

Fig 7. Liquidity Pool Size on Uniswap

A handful tools - like pools.fyi (https://pools.fyi/#/) - can help DeFi users to find the largest liquidity pools across major DEXes.

MONITORING NETWORK HEALTH: FOR PLATFORMS

Monitoring risks for DeFi platforms involves anomaly detection. Generally, abnormal behaviors can be categorized 5 ways: 1) large value transfers, 2) high frequency of transactions or calls towards a function (especially those that are not exposed to the public) within a short time period, 3) actions of fixed amount, occurring every other same fixed time period (bots), and 4) a "super user's" actions on multiple platforms and/or ownership of alarmingly high fund volumes.

Once abnormal behavior is detected, protocol teams can use some admin control designed in the smart contract, for example:

1. Brakes to terminate some/all functionalities of smart contracts or protocols.
2. Add a pending session to some large amount transactions.
3. Revert suspicious transactions.

To elaborate on the categories of abnormal behaviors:

1. Transfers of large fund values

Large value actions happening on chain - including borrowing, depositing, trading, and liquidation beyond a threshold - should trigger alerts, as it may shake the stability of a pool or a platform, or indicate suspicious movements (hacks on funds, money laundering, or fiat exit after attack). Stablecoins can play a particularly indicative role in large value transfers as their values are benchmarked towards fiat money.

2. High frequency of actions (including transactions, or calls to specific functions) within a certain time range

A high frequency of function calls, especially those that are not exposed externally, can be a signal of attacks. Re-entrancy is a typical attack to drain funds, where a function is called recursively multiple times within the same transaction. In a more general case, if platforms collect benchmark statistics about normal metrics of contract usage (i.e. a function will typically be called “x” times) and monitor the transactions where the numbers are much higher, it’s likely they can capture the abnormal behavior as soon as it happens.

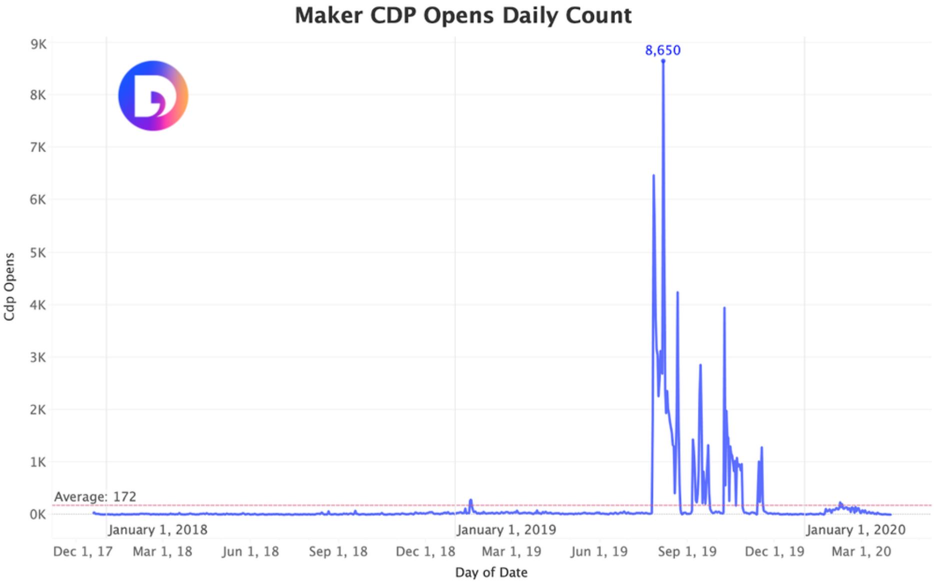

Fig 8. Maker’s CDP Open Over Time

Figure 8 shows an example of a high frequency event on Maker’s platform. In Q3 2019, daily CDP opens reached 8.7k, which is far above the historical average of 172/day. A few more batches of high CDP opens occurred in the following weeks and months. We believe these data spikes were from campaigns (https://twitter.com/coinbase/status/1154827433435996160?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1154827433435996160&ref_url=https%3A%2F%2Fblockonomi.com%2Fcoinbase-earn-dai-lesson%2F) targeting user acquisitions, but it does show that manual push will leave a trace and we can monitor it to stay alert.

3. Fixed Behavior Pattern (detecting bots)

It is legitimate practice for individuals or teams to build arbitrage bots to interact with (some) DeFi protocols, but the platform dev team may have concerns towards bots’ effects on the user base experience. By defining specific rules and patterns indicative of automated bot behavior (fixed number of actions in every other fixed window of time), it is possible to build mechanisms to detect bots and monitor their influence on a pool.

4. Super Users (whales)

Active whales in the user base of DeFi protocols can have significant influence on the stability of the system. Another approach to general systematic security, therefore, is to understand the behavior of “super users” and to have a deeper thinking towards potential risks.

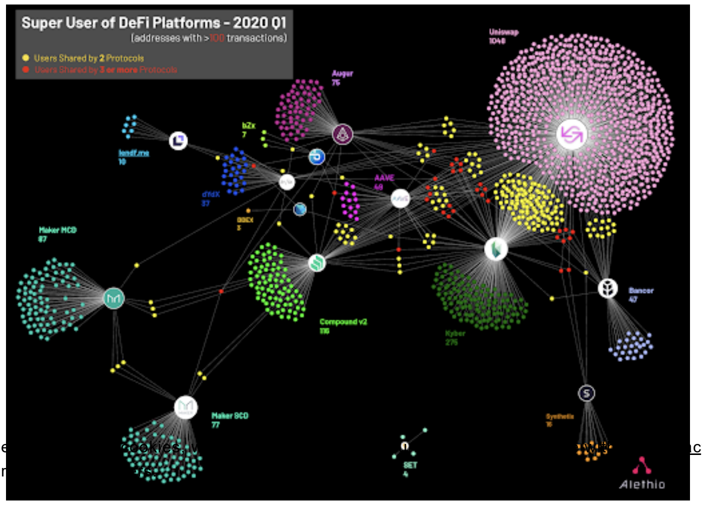
Super User of DeFi Platforms - 2020 Q1
(addresses with >100 transactions)
Users Shared by 2 Protocols
Users Shared by 3 or more Protocols
Uniswap
1048
Augur
75
bZx
7
lendf.me
10
dYdX
37
AAVE
48
0BEX
3
Maker MCD
87
Compound v2
116
Kyber
275
Bancor
47
Maker SCD
77
Synthetix
16
SET
4
Alethio

Fig 9. Large DeFi Users' Movement. Graph from the Alethio Q1 DeFi report (https://pages.consensys.net/ethereum-decentralized-finance-report-alethio).

Risk Management Products

Blockchain-based insurance has been around for a while, but has been brought sharply into focus these past few months. Nexus Mutual (https://nexusmutual.io/)- an blockchain insurance veteran who acted (https://defirate.com/nexus-mutual-first-payouts/) as the first respondent for victims in bZx exploit - and more recently Opyn (https://opyn.co/) have (re)emerged as top players in this adjacent DeFi industry, serving as hedge options against the protected assets. According to The Block (https://www.theblockcrypto.com/genesis/15376/mapping-out-ethereums-defi), a few other similar products to name include Etherisc, iXledger, VouchForMe and aigang. These widgets serve for similar needs while also can secure as an extra layer for each other - Nexus insurance can be purchased against Opyn options as an “Reinsurance”.

ConsenSys has launched Codefi Compliance (http://codefi.consensys.net/compliance), an automated and agile regulatory and compliance platform for digital assets. Codefi Compliance is part of the Codefi product suite, which collectively powers commerce and finance by optimizing business processes and digitizing financial instruments. As a next-generation solution for anti-money laundering (AML) and countering the financing of terrorism (CFT), Codefi Compliance ensures digital assets meet regulatory expectations without compromising market and business requirements, regardless of jurisdiction and design. It is the only compliance solution designed exclusively for Ethereum-based assets and built by ConsenSys, the leader in Ethereum development. Codefi Compliance delivers advanced compliance capabilities that include know-your-transaction (KYT) frameworks, high-risk case management, and real-time reporting.

Awareness

Though many tools and resources are already developed to help customers engage more confidently with DeFi, the ecosystem requires a higher level of awareness. Looking back at the incidents in February, March, and April, it is important to acknowledge that the DeFi space is:

1. **Still fragile among some protocols.** Though the ecosystem as a whole is fairly resilient, individual protocols can still be severely impacted. In particular, limited liquidity pool volumes can easily cause price slippages.
2. **Subject to the 'lego' architecture of Ethereum.** DeFi lives on top of Ethereum, and still - at least for the time being - relies on the health and stability of ETH's price. This was demonstrated particularly during the March market events.
3. **A nascent and consequently attack-prone ecosystem.** As proven by incidents in the past few months, the immense opportunity of blockchain technology does not protect it from the same tendency to have bugs and attack vectors that traditional tech has.

The net result of all these incidents, however, is positive. And these attacks are not new for the Ethereum community - as demonstrated by the waves that the DAO attack made in the crypto ecosystem in 2016. Attacks have made most of the teams and participants care more about the security of different products. And with that awareness, we believe more mature metrics and tools will be developed to serve the need and help hedge against risk.

Developer teams' understanding, maintenance and improvement of codebases is crucial to the whole ecosystem's health and prosperity. Unexamined forks of others' existing work can result in critical consequences. Once the protocol is released on mainnet, it effectively becomes a honeypot - open and exposed to all potential malicious attacks. These financial protocols are complex and loaded with value, yet still quite young and therefore particularly capable of violating users' trust.

Despite these waves of security incidents on DeFi protocols, the industry is still overwhelmingly positive (https://twitter.com/TrustlessState/status/1258503785992744960) about the opportunities of DeFi and the momentum it is bringing to Ethereum. Objective DeFi statistics support positive sentiment. In response to security events this year and considerable market pressures beginning in March, locked ETH has decreased from an all-time high in February. However, levels have dipped only to December 2019 numbers.These statistics, even in the face of high-profile security incidents, suggests the DeFi ecosystem as a whole has surpassed some point of 'no return.' Though confidence in individual protocols has suffered, overall commitment to the emerging paradigms of decentralized finance has remained strong.

Written by Danning Sui and Everett Muzzy

Disclaimer

Codefi Data has no preference or prejudice towards any of the projects mentioned above. The range of protocols discussed is limited and we will keep working on adding more in the list to achieve a more holistic view. This article should never be used as a guide for any malicious practice or trading suggestion.

Share

Newer Post
ConsenSys Launches Codefi Compliance (/blog/consensys-launches-codefi-compliance)

Older Post
NEWSLETTER #5: Thoughts on DeFi Security (/blog/newsletter-5-thoughts-on-defi-security)

OUR PRODUCTS

Codefi Application Suite (/application-suite)

Codefi Orchestrate (/orchestrate)

Codefi Workflow (/workflow)

Codefi Assets (/codefiassets)

Codefi Markets (/markets)

Codefi Payments (/payments)

Codefi Networks (/networks)

Codefi Staking (/staking)

Codefi Compliance (/compliance)

Codefi Data (/data)

ConsenSys (http://consensys.net)

OUR PROJECTS

Mata Capital (/mata-capital)

HMLR (/hmlr)

MythX (/mythx)

DeFi Score (/defi-score)

BLOG (/BLOG)

PRESS (/PRESS)

MEDIA (/MEDIA)

LEGAL

Terms of Use (/terms-of-use)

Terms of Service for Codefi Assets (/tou-codefi-assets)

Privacy Policy (/privacy-policy)

SUBSCRIBE TO THE CODEFI NEWSLETTER

SUBSCRIBE (HTTPS://SHARE
__HSTC=148571112.FCA8C0E694863E4D09674BF2B71E674B.159947732(

(ht
(htt
(ht