Electronically issued
Délivré par voie électronique : 17-Dec-2021
Toronto

Court File No.

ONTARIO
SUPERIOR COURT OF JUSTICE

B E T W E E N:

(Court Seal)

DILLON KELLAR and LAURENCE DAY

Plaintiffs

and

ANDEAN MEDJEDOVIC

Defendant

Proceeding under the *Class Proceedings Act, 1992,* SO 1992, c 6

NOTICE OF ACTION

TO THE DEFENDANT

A LEGAL PROCEEDING HAS BEEN COMMENCED AGAINST YOU by the Plaintiffs. The claim made against you is set out in the following pages.

IF YOU WISH TO DEFEND THIS PROCEEDING, you or an Ontario lawyer acting for you must prepare a Statement of Defence in Form 18A prescribed by the *Rules of Civil Procedure*, serve it on the Plaintiff's lawyer or, where the Plaintiff does not have a lawyer, serve it on the Plaintiff, and file it, with proof of service in this court office, WITHIN TWENTY DAYS after this Statement of Claim is served on you, if you are served in Ontario.

If you are served in another province or territory of Canada or in the United States of America, the period for serving and filing your Statement of Defence is forty days. If you are served outside Canada and the United States of America, the period is sixty days.

Instead of serving and filing a Statement of Defence, you may serve and file a Notice of Intent to Defend in Form 18B prescribed by the *Rules of Civil Procedure*. This will entitle you to ten more days within which to serve and file your Statement of Defence.

IF YOU FAIL TO DEFEND THIS PROCEEDING, JUDGMENT MAY BE GIVEN AGAINST YOU IN YOUR ABSENCE AND WITHOUT FURTHER NOTICE TO YOU. IF YOU WISH TO DEFEND THIS PROCEEDING BUT ARE UNABLE TO PAY LEGAL FEES, LEGAL AID MAY BE AVAILABLE TO YOU BY CONTACTING A LOCAL LEGAL AID OFFICE.

IF YOU PAY THE PLAINTIFF'S CLAIM, and $100,000 for costs, within the time for serving and filing your Statement of Defence you may move to have this proceeding dismissed by the Court. If you believe the amount claimed for costs is excessive, you may pay the Plaintiff's claim and $400 for costs and have the costs assessed by the Court.

TAKE NOTICE: THIS ACTION WILL AUTOMATICALLY BE DISMISSED if it has not been set down for trial or terminated by any means within five years after the action was commenced unless otherwise ordered by the court.

Date ______________________ Issued by _

Local Registrar

Address of court office: Superior Court of Justice
330 University Avenue, 9th Floor
Toronto ON M5G 1R7

TO: Andean Medjedovic
[redacted]

CLAIM

1. The plaintiffs claim:

   (a) An order certifying this action as a class proceeding under s. 5(1) of the *Class Proceedings Act* and appointing the plaintiffs as representative plaintiffs for the Class (capitalized terms defined below);

   (b) Damages in the amount of at least $16.5 million [1] as compensation for losses suffered by the direct holders of DEFI5 and CC10 tokens;

   (c) Damages in an amount to be determined at trial, but at least in the amount of $10 million as compensation for losses suffered by the indirect holders of DEFI5 and CC10 tokens;

   (d) An order rescinding and setting aside any contract(s) between the defendant and any Class members relating to the Attack;

   (e) An order recognizing or imposing a constructive trust over the digital assets held in the Wallet controlled by the defendant;

   (f) Punitive and exemplary damages;

   (g) An interim and interlocutory *Mareva* order freezing the defendant's assets, including the digital assets held in the Wallet;

---

[1] All dollar values are in USD.

(h) An interim and interlocutory order for the preservation of the digital assets held in the Wallet;

(i) A representation order under r. 10.01 of the *Rules of Civil Procedure* appointing the plaintiffs as representatives of the Indexed Finance DAO (an unincorporated association);

(j) Prejudgment and postjudgment interest;

(k) The costs of this proceeding; and

(l) Such further and other relief as this Honourable Court may deem just.

Overview

2. On October 14, 2021, the defendant, Andean Medjedovic (**"Andean"**), launched a sophisticated cyber-attack (the **"Attack"**) against Indexed Finance, a decentralized financial platform for cryptocurrencies and other digital assets. As a result of the Attack, Andean routed approximately $15.8 million from Indexed Finance's index pools to his "wallet" (account) on the Ethereum blockchain with public address: 0xba5ed1488be60ba2facc6b66c6d6f0befba22ebe (the **"Wallet"**).

3. To achieve this, Andean used computer hacking techniques to bypass Indexed Finance's trading controls. He executed a series of trades, using approximately $159 million in borrowed assets, that he knew would distort the algorithm used by Indexed Finance to set trading prices. This allowed Andean to purchase those assets at artificially deflated prices, thus acquiring assets

representing over 90% of the value of the DEFI5 and CC10 pools at a tiny fraction of their true value.

The Parties

4. The defendant, Andean, is a 19-year-old mathematics prodigy who has completed a master's degree in mathematics at the University of Waterloo. He is a resident of Ontario.

5. The plaintiff, Dillon Kellar is a co-founder of Indexed Finance and a resident of the City of [redacted]

6. The plaintiff, Laurence Day is a full-time contributor to Indexed Finance, where his responsibilities include communications, technical writing, and research. He is a resident of the City of Leeds in the United Kingdom.

7. Indexed Finance is a project focused on the development of passive portfolio management strategies for digital assets on the Ethereum blockchain. Indexed Finance is an unincorporated association of its users, or "tokenholders." It is a "decentralized autonomous organization" (or "**DAO**"), a common governance model in the crypto world. Indexed Finance has no physical offices and no centralized location.

Background

8. Index pools are the crypto world's equivalent of index funds. They allow users to purchase a digital "token" that represents a pool of digital assets, allowing users to gain diversification through exposure to a broader index of digital assets at a low cost. Index pools are "non-custodial", meaning that the underlying assets are owned by its users (and not by Indexed Finance).

9. The Attack targeted two index pools:

- **DEFI5:** the "DeFi Top 5 Tokens Index" (or **"DEFI5"**) focuses on large cap decentralized finance protocols across the Ethereum network;

- **CC10:** the "Cryptocurrency Top 10 Tokens Index" (or **"CC10"**) covers the most popular medium to large-cap cryptocurrencies on the Ethereum network.

10. Index pools are like exchange-traded index funds (**"ETFs"**) in traditional finance. Like a share of an ETF, each token of an index pool represents a fractional stake in a set of underlying assets. Like the shares of an ETF, index pool tokens are traded on an exchange. Like an ETF, the trading price for an index pool token is regulated so that it tracks the net asset value (**"NAV"**) of its underlying assets. Like an ETF, the actual trading price of an index pool token may diverge from its NAV. When this occurs, arbitrage traders can exploit the divergence and earn a profit, at the expense of the pool's tokenholders. Index pools use a complex mechanism to ensure that the pool token's trading price matches its NAV. Unlike an ETF, however, an index pool allows users to issue and redeem their own pool tokens directly from the index pool in exchange for the index token's trading price.

11. Adding a new token to the pool is akin to adding a new stock to the bundle of stocks included in an ETF. When a new token is added to one of Indexed Finance pools, the index pool recalculates the trading price for pool tokens using a benchmark called "Total Pool Value" which is used to approximate the index pool's NAV (the **"Benchmark"**). The index pool sets a trade volume limit that restricts the number of new pool tokens that can be issued at the new trading price to a maximum of 1.5% of the Benchmark's value.

The Attack

12. The Attack used market manipulation and computer hacking techniques to trigger a glitch in the pricing mechanism for the DEFI5 and CC10 index pools. The glitch caused the index pools to set a trading price for the DEFI5 and CC10 pool tokens at a tiny fraction of their NAV. The Attack then purchased assets at the depressed trading prices, i.e. to exploit the pricing glitch that the attacker himself had created.

13. The Attack involved the deployment of customized computer code developed by Andean, involving dozens of trades and hundreds of commands. It occurred over a period of just a few minutes, first targeting the DEFI5 index pool and then the CC10 index pool. While the mechanics of the Attack were highly complex, the plan of the Attack involved three basic components. For the DEFI5 Attack:

(a) **Benchmark Manipulation:** Andean used over $150 million in borrowed assets (more than 10 times DEFI5's NAV) to execute a series of trades designed to manipulate the Benchmark by temporarily distorting the price of its reference asset (the asset price by which the Benchmark is set).

(b) **Hacking the Trade Volume Limits:** by manipulating the Benchmark, Andean caused the DEFI5 index pool to set an artificially low price for the DEFI5 pool token relative to its NAV. Due to the index pool's trade volume limit, Andean should only have been able buy a limited number of pool tokens at prices influenced by the Benchmark manipulation (to a maximum of 1.5% of the Benchmark's value). However, Andean devised a hack by which he disabled the trade volume limit, permitting him to issue an enormous number of pool tokens at manipulated prices.

(c) **"Arbitrage" Trades:** the combined effect of manipulating the Benchmark manipulation and circumventing the volume limit was that the DEFI5 index pool set a price for issuing new pool tokens that was vastly below their NAV. Andean executed trades by issuing new pool tokens at the price that his actions had deflated, then immediately redeeming the pool token into its underlying assets. Andean repeated this pattern until he had drained over 90% of DEFI5's NAV.

14. The Attack repeated the above process on the CC10 index pool, with similar results.

15. Andean funded and coordinated the Attack through the Wallet.

16. Andean sought to conceal his identity by running the cryptocurrency used to pay the transaction costs for the Attack through a sophisticated "privacy mixer" called Tornado Cash.

Liability

17. Andean's conduct constitutes civil fraud on the holders of DEFI5 and CC10 tokens. In the course of the Attack, he knowingly made a false representation by manipulating the value of the Benchmark. This constituted a misrepresentation by conduct and/or active concealment of a material fact. By manipulating the Benchmark, Andean induced the DEFI5 and CC10 index pools — the contents of which were owned by the tokenholders – to sell him the pools' underlying assets at dramatically deflated prices, causing them to suffer significant losses.

18. To the extent that the trades involved in the Attack involved the formation of any contract(s) between or among Andean and any Class members, any such contracts would be void *ab initio*, or voidable, and should be rescinded and set aside on grounds of misrepresentation, mistake, unconscionability, and/or fraud/illegality.

19. Further, Andean violated the duty of honest performance in respect of any such contracts.

20. Andean has been unjustly enriched as a result of the Attack at the expense of the DEFI5 and CC10 tokenholders. There is no juristic reason for Andean's enrichment. The Attack involved conduct that is prohibited by provisions of the *Criminal Code* relating to computer hacking (s. 342.1) and fraud (s. 380(2)).

21. In taking the digital assets and storing them in his own Wallet, Andean interfered with the tokenholders' immediate right of possession over the digital assets and is liable in conversion.

Remedy

22. The digital assets stored in the Wallet are the rightful property of the tokenholders and a constructive trust should be recognized or imposed over the Wallet.

23. The holders of DEFI5 and CC10 tokens suffered direct losses of approximately $12.5 million and $4.0 million, respectively. Furthermore, additional losses were suffered by token holders who held their tokens indirectly, i.e. who owned tokens through other "pools" (the equivalent of a "fund of funds"). The effect of the Attack on the NAV of the DEFI5 and CC10 tokens caused severe disruptions in the prices of any pool token on the blockchain that held DEFI5 and CC10 tokens. In the immediate aftermath of the Attack, these disruptions caused massive and

predictable losses to arbitrage traders. The Plaintiffs continue to investigate the quantum of these losses but estimate that they exceed $10 million.

24. Andean was, at all times, aware that his conduct would harm the tokenholders. His conduct was high-handed, oppressive, harsh, vindicative, reprehensible, malicious, and in disregard of the rights of the DEFI5 and CC10 tokenholders.

The Class

25. The plaintiffs seek to represent the following proposed class (the **"Class"**):

> *All persons or entities anywhere in the world who owned tokens of DEFI5 or CC10, whether directly or indirectly, immediately prior to the time of the Attack, being October 14, 2021 at 6:37:43 pm (UTC) for DEFI5 and 6:39:49 pm (UTC) for CC10.*

26. At the time of the Attack, the plaintiff Dillon Kellar directly held DEFI5 and CC10 tokens. The plaintiff Laurence Day directly held DEFI5 tokens, and he indirectly held both DEFI5 and CC10 tokens. The Indexed Finance DAO itself directly held tokens of CC10 and DEFI5 and indirectly held tokens of each.

December 17, 2021

STOCKWOODS LLP
Barristers
Toronto-Dominion Centre
TD North Tower, Box 140
77 King Street West, Suite 4130
Toronto ON M5K 1H1

Gerald Chan (54548T)
Tel: 416-593-1617
GeraldC@stockwoods.ca

Fredrick Schumann (59377L)
Tel: 416-593-2490
FredrickS@stockwoods.ca

Stephen Aylward (66556E)
Tel: 416-593-2496
stephena@stockwoods.ca

Alexandra Heine (83514R)
Tel: 416-593-1669
AlexandraH@stockwoods.ca

Tel: 416-593-7200
Fax: 416-593-9345

Lawyers for the Plaintiffs/Moving Parties

DILLON KELLAR et al. and ANDEAN MEDJEDOVIC Court File No.

Plaintiffs Defendant

ONTARIO

SUPERIOR COURT OF JUSTICE

Proceeding commenced at TORONTO

NOTICE OF ACTION

STOCKWOODS LLP
Barristers
Toronto-Dominion Centre
TD North Tower, Box 140
77 King Street West, Suite 4130
Toronto ON M5K 1H1

Gerald Chan (54548T)
Tel: 416-593-1617 / GeraldC@stockwoods.ca

Fredrick Schumann (59377L)
Tel: 416-593-2490 / FredrickS@stockwoods.ca

Stephen Aylward (66556E)
Tel: 416-593-2496 / stephena@stockwoods.ca

Alexandra Heine (83514R)
Tel: 416-593-1669 / AlexandraH@stockwoods.ca

Tel: 416-593-2496
Fax: 416-593-9345

Lawyers for the Plaintiffs

Court File No. CV-21-00673984-00CP

ONTARIO
SUPERIOR COURT OF JUSTICE

B E T W E E N:

DILLON KELLAR and LAURENCE DAY

Plaintiffs

and

ANDEAN MEDJEDOVIC

Defendant

Proceeding under the *Class Proceedings Act, 1992,* SO 1992, c 6

FACTUM OF THE MOVING PARTIES
(*MAREVA* AND RECEIVERSHIP ORDERS)

December 17, 2021

STOCKWOODS LLP
Barristers
Toronto-Dominion Centre
TD North Tower, Box 140
77 King Street West, Suite 4130
Toronto ON M5K 1H1

Gerald Chan (54548T)
Tel: 416-593-1617
GeraldC@stockwoods.ca

Fredrick Schumann (59377L)
Tel: 416-593-2490
FredrickS@stockwoods.ca

Stephen Aylward (66556E)
Tel: 416-593-2496
stephena@stockwoods.ca

Alexandra Heine (83514R)
Tel: 416-593-1669
AlexandraH@stockwoods.ca

Tel: 416-593-7200
Fax: 416-593-9345

Lawyers for the Plaintiffs/Moving Parties

TABLE OF CONTENTS

PAGE

FACTUM OF THE MOVING PLAINTIFFS

PART I - OVERVIEW

1. On October 14, 2021, the defendant, Andean Medjedovic, executed a sophisticated cyber-attack (the **"Attack"**) against Indexed Finance, a decentralized financial platform for cryptocurrencies and other digital assets that oversees "index pools"—the crypto equivalent of index funds. The plaintiffs, Laurence Day and Dillon Kellar held "tokens" in the affected index pools and, as such, were among the victims of the Attack.

2. The defendant orchestrated the Attack by developing and deploying customized computer code, which allowed him to bypass Indexed Finance's trading controls and exploit its systems. Specifically, he used $159 million[1] in borrowed assets to execute a series of trades that he knew would distort the algorithm used by Indexed Finance to set trading prices. This allowed him to purchase assets at artificially deflated prices. He inflicted losses of approximately $16.5 million on the affected index pools. His net gain (after transaction costs) was approximately $15.8 million worth of digital assets. He transferred these digital assets to a "wallet" (account) on the Ethereum blockchain (the **"Wallet"**).

3. The defendant is not legally entitled to the digital assets. There is a grave risk that he may hide or dissipate the digital assets, which will put them beyond the reach of the plaintiffs and this Court. Accordingly, it would be just and equitable for this Court to grant interim relief, primarily to preserve the digital assets that the defendant has misappropriated.

[1] All amounts are in USD, the conventional currency used to quote prices for crypto and digital assets.

4. On this motion, the plaintiffs request an order, in the form of the draft *Mareva* (Tab 5 of the Motion Record). The relief sought is necessary and appropriate. The plaintiffs have a strong *prima facie* case that the defendant obtained the assets in the Wallet through fraudulent and dishonest means. There is an imminent risk that the defendant will dissipate the assets in the Wallet unless this court intervenes.

5. The plaintiffs also seek an order for a receivership of the assets in the Wallet (Tab 6 of the Motion Record). Due to their nature, special measures are required to secure them pending trial. In traditional finance, assets are generally held by reputable financial institutions, which will cooperate with the court in freezing a defendant's assets. There is no equivalent to this for digital assets, i.e. there are no institutions or entities that have the power to freeze the assets in the Wallet. As such, the only way to secure them pending trial is to transfer them to a trusted third party. Raymond Chabot Administrateur Provisoire Inc. (**"RCAP"**), a subsidiary of Raymond Chabot Grant Thornton LLP, a reputable firm with experience with digital assets, has consented to be named as a receiver of property over the digital assets.

PART II - SUMMARY OF FACTS

6. The workings of Indexed Finance's index pools, the Attack, and the evidence that the defendant was the Attacker, are complex. The following summarizes the most salient facts.[2]

[2] The full factual record is contained in the Affidavit of Laurence Day, sworn on December 9, 2021 ("**Day Affidavit**"), Motion Record ("**MR**") vol 1, Tab 2, and the Affidavit of Adam Avenir, sworn on December 6, 2021 ("**Avenir Affidavit**"), MR vol 2, Tab 3.

A. The Parties

7. The defendant, Andean, is a 19-year-old with a master's degree in mathematics from the University of Waterloo. He is a resident of Ontario.

8. Indexed Finance is a project focused on the development of passive portfolio management strategies for digital assets on the Ethereum blockchain. Indexed Finance is an unincorporated association of its users, or “tokenholders”, with no centralized location.

9. The plaintiff Dillon Kellar is a co-founder of Indexed Finance. The plaintiff Laurence Day is a full-time contributor to Indexed Finance, where his responsibilities include communications, technical writing, and research.

10. Indexed Finance is a non-custodial platform, meaning that assets held through its index pools remain the property of individual tokenholders. As such, the vast majority of the losses related to the Attack were sustained by individual tokenholders, not Indexed Finance itself. The plaintiffs intend to commence a proposed class action against the defendant on behalf of the affected tokenholders. A draft unissued notice of action is included at Tab 4 of the Motion Record. The plaintiffs intend to commence the action as soon as the Court decides this motion.

B. How Indexed Finance’s Index Pools Work

i. Overall Index Pool Mechanics

11. Indexed Finance is a decentralized financial platform for cryptocurrencies and other digital assets. It operates “index pools”, which allow users to purchase a digital “token” that represents a pool of digital assets, allowing users to gain diversification through exposure to a

broader index of digital assets at a low cost.[3] The two index pools targeted in the Attack were "DEFI5" and "CC10." Both pools hold digital assets, including cryptocurrencies.[4]

12. Index pools are like index exchange-traded funds (**"ETFs"**) in traditional finance. There are three salient and important differences between the two:

(a) Index pools are "**non-custodial**", meaning that the underlying assets of Indexed Finance's pools are owned by its users (not by Indexed Finance).[5] By contrast, the underlying assets of an ETF are owned by a financial institution.

(b) Index pools **decentralize** the function of "rebalancing", i.e. ensuring that the weights of assets held in the pool ("**Pool Weight**") match the weights of assets in the index ("**Index Weight**"). An index ETF rebalances centrally and directly, by having a fund manager buy and sell the underlying assets. An index pool, by contrast, sets the relative prices of assets such that there will be an incentive for others to carry out trades that rebalance the pool.[6]

(c) Index pools allow **users to control pool token supply**. Ownership in an index pool is represented by a "pool token", so there are DEFI5 tokens and CC10 tokens. Users can create ("mint") pool tokens by providing underlying assets to the pool and receiving pool tokens, and redeem ("burn") pool tokens by providing pool tokens and

[3] Day Affidavit, paras 4 and 6, MR vol 1, Tab 2, p 13.
[4] Day Affidavit, para 7, MR vol 1, Tab 2, p 14.
[5] Day Affidavit, paras 6 and 46-47, MR vol 1, Tab 2, pp 13, 25-26.
[6] Day Affidavit, para 45, MR vol 1, Tab 2, p 25.

receiving underlying assets. By contrast, the supply of shares of an ETF is centrally managed.[7]

13. Indexed Finance created the indices that its index pools track, including the DEFI5 and CC10 indices that the Attack targeted.[8] It maintains them by setting criteria for the selection of underlying asset tokens and their Index Weights, and using a computer program (the "**index controller**") to execute those criteria.[9]

14. Occasionally, market changes will mean that one token must be removed from the index, and replaced with another token. This is a "**Re-Indexing**": it is executed by the index controller, and it can be triggered by any user.[10] Similarly, changes in market value will mean that the Index Weights of the tokens must be adjusted. This is called a "**Re-Weighting**": it is also executed by the index controller, and can be triggered by any user.[11]

15. The index pools set exchange rates for the underlying tokens relative to one another, and relative to the pool token, allowing users to exchange them for one another ("**Pool Prices**"). The index pool rebalances itself not by centrally buying and selling assets, but by setting Pool Prices in a way that creates incentives for traders to make trades with the pool that will move them towards rebalance.[12]

16. The index pool does this with an automated exchange (an "**Automated Market Maker**" or "**AMM**"). The index controller sets internal weights ("**AMM Weights**") for the

[7] Day Affidavit, paras 48-53, MR vol 1, Tab 2, pp 26-28.
[8] Day Affidavit, para 54, MR vol 1, Tab 2, p 28.
[9] Day Affidavit, paras 55-56, MR vol 1, Tab 2, p 28.
[10] Day Affidavit, paras 57-59, MR vol 1, Tab 2, pp 28-29.
[11] Day Affidavit, paras 60-65, MR vol 1, Tab 2, pp 29-31.
[12] Day Affidavit, paras 69-74, MR vol 1, Tab 2, pp 32-34.

tokens in the pool. The AMM uses the AMM Weight to set the Pool Price for a token. Generally, the AMM Weight of a token equals its Index Weight. If the Pool Weight of a token is less than its AMM Weight, the Pool Price will be greater than the market price, creating an incentive for trades that increase the number of that token held (its "**balance**"), thus increasing its Pool Weight towards its AMM Weight. If the Pool Weight of a token is greater than its AMM Weight, the Pool Price will be less than market price, incentivizing trades that decrease the balance of that token, decreasing its Pool Weight towards its AMM Weight.[13]

17. The AMM Weight/Pool Price structure creates a supply-and-demand dynamic inside the pool. The more of a token that users swap into the pool, the lower its Pool Price. Conversely, the more of a token that users swap out of the pool, the higher its Pool Price. Importantly (for the purposes of understanding the Attack), the relationship between Pool Price and balance is non-linear: as the balance of a token decreases towards zero, its Pool Price will increase towards infinity.[14]

18. Critically, there are limits on index pool transactions. The pool will only permit a user to swap in up to 50% of the pool's balance of a single token in a single swap (the **"50% Swap-In Limit"**). As well, the index pool will only allow a user to swap-out up to one-third of the pool's balance of a single token (the **"33% Swap-Out Limit"**). These limits apply not only to transactions where one underlying token is exchanged for another, but also to mints and burns of the pool tokens where the pool token is exchanged for a single underlying token ("**single-**

---

[13] Day Affidavit, paras 75-79, MR vol 1, Tab 2, pp 34-35.
[14] Day Affidavit, para 76, MR vol 1, Tab 2, pp 34-35.

asset mints" and "**single-asset burns**"). In general, these limits are not intended to and do not prevent multiple swaps in a row involving the same token.[15]

ii. Introducing A New Token to the Index Pool

19. Introducing a new token to an index pool requires a series of special steps. When a new token is first added to the pool, its balance will be zero. The AMM function does not work with a balance of zero. So, the index controller assigns a starting balance and weight, the "**Minimum Balance**" and "**Minimum AMM Weight**", to calculate an initial Pool Price (the "**Initialization Price**"). The AMM then allows trades at that price until the new token reaches the Minimum Balance. This process is called "initialization."[16] The trade in which a token first reaches, or exceeds, its Minimum Balance, is its "**Initialization Trade**."[17] By definition, the Initialization Trade is a single trade, and is thus subject to the 50% Swap-In Limit. Before a token reaches its Minimum Balance, the 50% Swap-In Limit is set by reference to the token's Minimum Balance, such that the Initialization Trade cannot be more than 50% of the Minimum Balance.[18] The Attack circumvented this limit, as described below.

20. The Minimum Balance of a new token is the balance that, at current market prices, would represent 1% of the value of the index pool. Therefore, to calculate the Minimum Balance, the index controller must determine the total value of the pool.[19] To reduce transaction costs, the index controller uses a shortcut calculation, a function called TotalPoolValue. It selects a token to use as a reference asset (generally the token with the largest value in the pool).

[15] Day Affidavit, para 143, MR vol 1, Tab 2, pp 54-55.
[16] Day Affidavit, para 85, MR vol 1, Tab 2, pp 37-38.
[17] Day Affidavit, para 87, MR vol 1, Tab 2, p 38.
[18] Day Affidavit, para 158, MR vol 1, Tab 2, p 59.
[19] Day Affidavit, para 88, MR vol 1, Tab 2, p 38.

It then multiplies *that* token's balance by the reciprocal of its AMM Weight. This approximates the total value of the pool, expressed in terms of the reference token.[20] It depends on a reasonable correlation between the AMM Weight of the benchmark token and its actual weight (i.e. Pool Weight). The Minimum Balance is set as the number of the new token that, at current market exchange rates, would purchase 1% of TotalPoolValue.[21]

21. If the market price of the uninitialized new token increases before the Minimum Balance is attained, no one will want to sell the new token into the pool at the under-market Initialization Price. Hence, the index pool allows the Minimum Balance (and Initialization Price) to be updated during initialization, with a function called UpdateMinimumBalance. UpdateMinimumBalance re-runs the TotalPoolValue calculation by recalculating the market value for the reference token based on fresh market price information and its current balance in the pool, then resets the Minimum Balance and Initialization Price of the new token accordingly.[22]

22. When a new token completes initialization (by reaching its Minimum Balance), it is assigned an initial AMM Weight ("**Initial AMM Weight**"). The Initial AMM Weight will equal the Minimum AMM Weight (1%), plus a percentage to the extent the Initialization Trade caused the new token's balance to exceed the Minimum Balance.[23] The index pool gradually

[20] Day Affidavit, para 89, MR vol 1, Tab 2, pp 38-39.
[21] Day Affidavit, para 90, MR vol 1, Tab 2, p 39.
[22] Day Affidavit, para 94, MR vol 1, Tab 2, p 40.
[23] Day Affidavit, para 95, MR vol 1, Tab 2, pp 40-41. So, for example, if the Minimum Balance of SUSHI was 400 and the pool currently had 300 SUSHI tokens, and user swapped in 200 SUSHI, the Initial AMM Weight would be 1.25%, because its current balance would be 1.25 times its Minimum Balance.

moves the AMM Weight for the new token from its Initial AMM Weight to its Index Weight, by a maximum of 1% of the current AMM Weight every thirty minutes.[24]

23. When a new token is initialized and the new token's Initial AMM Weight is set, the AMM Weights of all the other assets must be reduced (the **"Initialization Re-Weighting"**).[25]

C. The Attack

24. The Attack targeted first the DEFI5 index pool (the **"DEFI5 Phase"**) and then the CC10 index pool (the **"CC10 Phase"**). Both attacks occurred on October 14, 2021, within minutes of each other.[26] The Attack was carried out by a user identified only by a wallet address, i.e. the Wallet.[27]

25. The below narrative is lengthy, but, in fact, each attack occurred instantaneously; it was executed as a single transaction by computer code.[28] The attacks were almost identical, and so only the DEFI5 attack is described in detail.[29]

26. At the time of the Attack, the DEFI5 pool's market value ("**NAV**") was approximately $13.4 million.[30] The DEFI5 index was due for a Re-Indexing: a new token, SUSHI (the token for the crypto exchange platform Sushiswap), had increased in market capitalization to the point where it was due to replace one of the existing tokens in the index.[31]

---

[24] Day Affidavit, paras 99-101, MR vol 1, Tab 2, pop 41-42.
[25] Day Affidavit, para 98, MR vol 1, Tab 2, p 41.
[26] Day Affidavit, paras 102-103, MR vol 1, Tab 2, p 43.
[27] Day Affidavit, para 125 (the address is 0xba5ed1488be60ba2facc6b66c6d6f0befba22ebe), MR vol 1, Tab 2, p 50.
[28] Day Affidavit, paras 104-105, MR vol 1, Tab 2, pp 43-44.
[29] Day Affidavit, para 106, MR vol 1, Tab 2, p 44.
[30] Day Affidavit, para 107, MR vol 1, Tab 2, p 44.
[31] Day Affidavit, para 110, MR vol 1, Tab 2, p 45.

27. First, the Attacker triggered a Re-Indexing of the DEFI5 index, which added SUSHI to the index and set an Index Weight for it of 12%.[32] The index controller set a Minimum Balance and Initialization Price for SUSHI using the TotalPoolValue benchmark. In this case, the reference token used by TotalPoolValue was UNI. The TotalPoolValue benchmark worked correctly and set a reasonable Minimum Balance and Initialization Price for SUSHI.[33]

28. The Attacker then borrowed approximately $157 million in tokens through "flash loans", a form of collateral-free borrowing available on the blockchain. The borrowed tokens matched the composition of the DEFI5 pool, i.e. there were approximately $48 million in UNI (the token for another crypto exchange platform, Uniswap) and a combined $109 million in the five non-UNI assets.[34] In a series of swaps, he used the borrowed tokens to purchase 98% of the UNI in the pool, driving down its balance, and massively inflating its Pool Price to about 860 times its market price. The net result of these trades was that the Attacker sold $109 million in borrowed assets to receive only $5.2 million in UNI tokens. There is no economic justification for such a trade: it only makes sense as part of the Attack.[35]

29. Next, the Attacker triggered the UpdateMinimumBalance command, which re-ran the TotalPoolValue calculation. This calculation used the UNI token, multiplying its current balance by the reciprocal of its AMM Weight. The function was intended to estimate the pool's NAV in terms of the UNI token. However, here, the balance of UNI had dropped, while its

---

[32] Day Affidavit, paras 134-135, MR vol 1, Tab 2, p 53.
[33] Day Affidavit, paras 109 and 136, MR vol 1, Tab 2, pp 44-45, 53.
[34] Day Affidavit, paras 138-140, MR vol 1, Tab 2, pp 53-54.
[35] Day Affidavit, paras 141-146, MR vol 1, Tab 2, pp 54-55.

AMM Weight remained constant. Accordingly, TotalPoolValue massively underestimated the pool's NAV, by a factor of roughly 400.[36]

30. The UpdateMinimumBalance function then used this massively underestimated figure to reset the Minimum Balance for SUSHI, meaning that that figure was roughly 400 times too low. That distorted the Initialization Price for SUSHI, meaning that a user could trade $3,200 of SUSHI into the pool and receive tokens worth $1,172,000.[37]

31. The Attacker then used all the UNI tokens that he had (both flash-loaned and purchased) to mint new DEFI5 tokens, approximately $153.8 million worth.[38]

32. If the Attacker had stopped here, distorting the Initialization Price of SUSHI would have had limited effect, since the Initialization Price would only govern until SUSHI reached its Minimum Balance. The Attack succeeded because the Attacker was able to hack the trade volume limit on the Initialization Trade. This allowed him to pour an unlimited amount of SUSHI tokens into the index pool, which overwhelmed the pool and caused its pricing mechanism to go haywire.[39]

33. The Attacker did this by performing a trade that the index pool did not expect: a gift of roughly $2.4 million of flash-loaned SUSHI. There was no legitimate economic justification for this gift. Its purpose could only have been to further manipulate the pool.[40]

---

[36] Day Affidavit, paras 148-152, MR vol 1, Tab 2, pp 56-57.
[37] Day Affidavit, paras 153-154, MR vol 1, Tab 2, pp 57-58.
[38] Day Affidavit, paras 155-157, MR vol 1, Tab 2, pp 58-59.
[39] Day Affidavit, paras 158-160, MR vol 1, Tab 2, pp 59-60.
[40] Day Affidavit, paras 161-162, MR vol 1, Tab 2, p 60.

34. A gift is not subject to the 50% Swap-In Limit, and this gift was massively greater than what the 50% Swap-In Limit would have allowed.[41] The Attacker then triggered a function called "**Gulp**", which forced the index pool to recognise the gift of SUSHI. The Gulp function causes the pool to treat a gift as if it were a trade. Since this trade brought SUSHI above its Minimum Balance, the Gulp function caused the pool to treat the gift as the Initialization Trade for SUSHI. The gift was therefore used by the index pool to set SUSHI's Initial AMM Weight and triggered the Initialization Re-Weighting.[42]

35. As a result of the massive gift of SUSHI, the Initial AMM Weight for SUSHI was set at 87%, far above its Index Weight of 12%. This is the reverse of how things are supposed to work: the Initial AMM Weight is supposed to be *lower* than the Index Weight, such that the index controller gradually *increases* the AMM Weight until it reaches Index Weight.[43]

36. The result of the vastly inflated Initial AMM Weight for SUSHI was vastly *deflated* AMM Weights for the other tokens in the pool. This distorted the rates by which SUSHI and the other tokens could be exchanged for each other, overpricing SUSHI and underpricing all other tokens. It also allowed a user to mint DEFI5 tokens at greatly distorted rates with overpriced SUSHI tokens.[44]

37. Recall that, earlier in the Attack, the Attacker had minted approximately $153.8 million worth of DEFI5 tokens. He now burned those tokens for the underlying tokens, including

---

[41] Day Affidavit, subpara 166(a), MR vol 1, Tab 2, p 61.
[42] Day Affidavit, paras 161-163, MR vol 1, Tab 2, p 60.
[43] Day Affidavit, paras 164-167, MR vol 1, Tab 2, pp 60-62.
[44] Day Affidavit, paras 168-171, MR vol 1, Tab 2, pp 62-63.

SUSHI.[45] He used those SUSHI tokens to mint new DEFI5 tokens, and then immediately burned them for the underlying assets, then repeated this process.[46]

38. In all, the Attack reduced the NAV of the DEFI5 pool from $13.4 million to $900,000. After repaying the flash loans and transaction costs, the Wallet received $11.9 million of underlying assets. Those tokens remain in the Wallet to this day, and can be seen on the blockchain by anyone with an internet connection.[47]

39. Minutes later, the Attacker executed the CC10 Phase, causing direct losses of $4.0 million (with a net recovery to the Wallet of $3.9 million).[48]

40. The DEFI5 and CC10 tokenholders are not the only ones who suffered losses in the Attack. Some users hold those pool tokens through other pools. They saw a proportionate fall in the value of their tokens, and also suffered losses through the arbitrage trading that followed.[49]

D. The Identity of the Attacker

41. In the weeks before the Attack, the plaintiffs had each been contacted on Discord (a social media platform) by a user with the Discord username "UmbralUpsilon." The plaintiffs agreed to pay UmbralUpsilon to develop computer scripts related to the Indexed Finance platform. UmbralUpsilon had asked questions about the re-indexing and re-weighting functions

[45] Day Affidavit, paras 173-174, MR vol 1, Tab 2, p 63.
[46] Day Affidavit, paras 175-178, MR vol 1, Tab 2, pp 63-64.
[47] Day Affidavit, paras 182-183, MR vol 1, Tab 2, pp 65-66.
[48] Day Affidavit, paras 184-188, MR vol 1, Tab 2, pp 67-69.
[49] Day Affidavit, paras 189-192, MR vol 1, Tab 2, pp 69-70.

in the index pools.[50] The series of conversations had ended on October 12, 2021, two days before the Attack.

42. Since these were the exact same functions that the Attack had exploited, the plaintiffs became suspicious. They saw that UmbralUpsilon had changed his Discord username to "Bogholder#1688" and deleted his half of their conversation.[51]

43. The Wallet had received deposits of three Ether tokens (a popular cryptocurrency) to pay the transaction costs of the Attack. The source of these deposits could not be easily traced since the Attacker had run them through a "privacy mixer", Tornado Cash (a service that disguises the flow of funds on the blockchain).[52] However, the plaintiffs received a tip that "BogHolder" was linked to an Ethereum address (the "**AB3 Address**"), which had made deposits to Tornado Cash before the Attack. The plaintiffs cross-referenced incoming and outgoing Tornado Cash transfers within the 24 hours before the Attack, and confirmed that the AB3 Address had made deposits of four Ether that corresponded in time to the deposits to the Wallet.[53] They also confirmed that the AB3 Address had received coding contest rewards on behalf of a user with the Discord username UmbralUpsilon.[54]

44. That user had registered for the contests with a GitHub account, "mtheorylord1", with no other notable activity. However, the plaintiffs found another GitHub account, "mtheorylord", which had been active in 2016. The data associated with that account contained

---

[50] Day Affidavit, para 197, MR vol 1, Tab 2, pp 71-72.
[51] Day Affidavit, para 198, MR vol 1, Tab 2, p 720.
[52] Day Affidavit, paras 206-208, MR vol 1, Tab 2, pp 74-75.
[53] Day Affidavit, paras 203-216, MR vol 1, Tab 2, pp 73-77.
[54] Day Affidavit, paras 216-220, MR vol 1, Tab 2, pp 76-78; Avenir Affidavit paras 2-6, 12-13, 14-17, and 26-28, MR vol 2, Tab 3, pp 343-348, 350.

an email address, [redacted] This email address appears to be the email account of the defendant, Andean Medjedovic, at the [redacted].[55] A Wikipedia user called "mtheorylord" had added the defendant's name to the Wikipedia page for "Reach for the Top", describing "Andean Medjedovic" as a "notable mathematician". That Wikipedia user page has since been deleted.[56]

45. A Google search for the defendant's name revealed a website, https://nontrivial.xyz.[57] It had been deleted when the plaintiffs tried to retrieve it, but the plaintiffs could see a version cached (copied) by Google on October 14, the day of the Attack (indicating that it had been deleted after the Attack).[58] The website disclosed an interest in "cryptocurrency and other decentralized open-source software", and a personal email address, [redacted].[59]

46. The plaintiffs did a reverse IP search on the defendant's personal website, which showed that another website was also hosted by that same IP address: https://urbitstar.xyz. That website had been deleted, but it suggested an interest in a platform called "Urbit."[60] The Urbit Discord chat showed that the user "BogHolder" was listed as "~libmud-bonted" (the name of an Urbit planet).[61] This planet, in turn, is linked through payments to the AB3 Address.[62]

---

[55] Day Affidavit, paras 222-225, MR vol 1, Tab 2, pp 79-80.
[56] Day Affidavit, paras 226-227, MR vol 1, Tab 2, pp 80-81.
[57] Day Affidavit, para 228, MR vol 1, Tab 2, p 81.
[58] Day Affidavit, para 228, MR vol 1, Tab 2, p 81.
[59] Day Affidavit, paras 227-229, MR vol 1, Tab 2, p 81.
[60] Urbit is a decentralized personal server platform or a "peer-to-peer network" that allows each individual user to buy and own a "planet" on the Urbit network. It is described on the website https://urbit.org. Purchasing a "planet" is the equivalent of purchasing a permanent identity or, in other words, a static individualized IP address that allows users to store and run whatever they want on it. See Day Affidavit, para 232, MR vol 1, Tab 2, p 82.
[61] Day Affidavit, para 234, MR vol 1, Tab 2, p 82.
[62] Day Affidavit, paras 232-235, MR vol 1, Tab 2, pp 82-83.

47. One of the co-founders of Indexed Finance, PR0, emailed [redacted] and offered a $50,000 reward for the return of the assets.[63] He received a reply from the email address, asking for the reward to be transferred to an address (the **"E64 Address"**). As mentioned above, prior to the Attack the plaintiffs had paid UmbralUpsilon to develop code related to indexed Finance. At UmbralUpsilon's request, they had sent payment to that same E64 Address.[64] Nobody knew this other than the plaintiffs and UmbralUpsilon.[65]

48. A Twitter account called @ZetaZeroes had, immediately before the Attack, posted the address of the Wallet on a public internet chat. Since the Attack, @ZetaZeroes has taken responsibility on Twitter for the Attack.[66] @ZetaZeroes has also complained about the plaintiffs disclosing information about the defendant, Andean Medjedeovic, in a manner suggesting that @ZetaZeroes is the defendant.[67]

49. The plaintiffs' New York lawyer, Jason Gottlieb, has communicated with a Texas lawyer representing the defendant. The defendant's Texas lawyer did not deny that his client was the Attacker, and stated that his client has no plans to send tokens to the plaintiffs.[68]

50. Mr. Gottlieb also communicated with the defendant's father, who stated, among other things, "what he did, he did to prove [a] point"; "the money's gonna be gone, because he's the only one who knows how to get it". and "he's the only one who knows the code."[69] Although

[63] Day Affidavit, para 236, MR vol 1, Tab 2, pp 83-84.
[64] Day Affidavit, paras 199-200, MR vol 1, Tab 2, pp 72-73.
[65] Day Affidavit, paras 236-237, MR vol 1, Tab 2, pp 83-84.
[66] Day Affidavit, paras 254-258, MR vol 1, Tab 2, p 88.
[67] Day Affidavit, paras 240-264, MR vol 1, Tab 2, pp 85-90.
[68] Day Affidavit, paras 264-266, MR vol 1, Tab 2, p 90.
[69] Day Affidavit, para. 267, MR vol 1, Tab 2, p 91.

the defendant's father stated that the defendant did not live with him, he stated that they had had recent contact. The father insinuated that his son might harm himself.[70]

PART III - STATEMENT OF ISSUES, LAW & AUTHORITIES

51. The issues to be determined in this motion are:

(a) Should the Court grant the requested *Mareva* order?

(b) Should the Court appoint RCGAP as a receiver of property?

A. *Mareva* Order

52. A *Mareva* order prohibits a defendant from disposing or transferring assets to evade judgment.[71] A *Mareva* order is an extraordinary remedy that is an exception to the general rule against execution before judgment.[72] The test for obtaining a *Mareva* order is therefore more onerous than for other injunctive relief. The plaintiff must establish:

(a) a strong *prima facie* case;

(b) that there is a real and genuine risk that the defendant will dissipate assets;

(c) that the balance of conveniences favours granting the order; and

(d) that the plaintiff has provided an undertaking as to damages.[73]

---

[70] Day Affidavit, paras 268-270, MR vol 1, Tab 2, pp 91-92.
[71] *SFC Litigation Trust v. Chan*, 2017 ONSC 1815 para. 38.
[72] *Chitel v. Rothbart* (1982), 1982 CanLII 1956 (ONCA).
[73] *Sibley & Associates LP v Ross,* 2011 ONSC 2951 at para. 11; *SFC Litigation Trust v. Chan*, 2017 ONSC 1815 (Div. Ct.) at para. 60, *per* Pattillo J. (dissenting but not on this point); *Chitel v. Rothbart* (1982), 1982 CanLII 1956 (ON CA); *Aetna Financial Services Ltd. v. Feigelman* [1985] 1 SCR 2 at p. 27.

53. Additionally, in an *ex parte Mareva* motion, the plaintiffs must make full and frank disclosure of all material facts.[74] As with all injunctive relief, the decision to grant the order is within the discretion of the Court.[75]

i. Strong *Prima Facie* Case

54. A strong *prima facie* case exists if there is "a substantial likelihood of success in the action that justifies extraordinary relief at the commencement of the proceeding".[76] This standard is higher than the "serious issue to be tried" standard that applies to most injunctions, due to the drastic nature of the *Mareva* order.[77]

55. This case raises novel factual and legal issues. At its heart, this action is a claim by the plaintiffs (and proposed class members) to unwind a series of transactions that were carried out through "smart contracts." Professor Andrew Luesley of Dalhousie University gives a useful analysis of smart contracts in a recent paper, in which he defines a smart contract as "an agreement in digital form that is self-executing and thus self-enforcing":

> A major difference between a traditional contract and a so-called smart contract, is that contracts create enforceable obligations, whereas smart contract automatically enforce obligations. Compare signing a contract to purchase an item versus purchasing an item from a vending machine. Like the smart contract, the vending machine will automatically complete the transaction by dispensing the item, whereas a paper contract for the sale of an item does not actually force the sale, and thus can be reneged by breaching the contract.[78]

---

[74] Rule 39.01(6) of the *Rules of Civil Procedure*; *Chitel v. Rothbart* (1982), 1982 CanLII 1956 (ONCA).
[75] *SFC Litigation Trust v. Chan*, 2017 ONSC 1815 para. 36.
[76] *R. v. Canadian Broadcasting Corp.*, 2018 SCC 5, at paras. 17-18.
[77] *Cytrynbaum v. Look Communications Inc.,* 2013 ONCA 455, at para. 54.
[78] Andrew Luesley, "Unravelling Smart Contracts: Smart Contracts and the Law of Rescission in Canada", (2019) 19 Asper Review 155(2019) 19 Asper Review 155 at 155-156, BOA Tab 1.

56. The Attack involved a series of trades between the defendant and the index pools carried out through a series of commands executed on the smart contracts of the index pools. While the technology is new, the legal analysis falls within established causes of action. There is a strong *prima facie* case that the transactions involved in the Attack should be set aside and damages awarded. Among other causes of action, the plaintiffs have a strong *prima facie* case for civil fraud, rescission for misrepresentation or mistake, and/or unjust enrichment.

57. **Civil Fraud.** To establish civil fraud, a plaintiff must show that: (a) the defendant made a false representation; (b) the defendant knew the representation was false; (c) the false representation caused the plaintiff to act; and (d) the plaintiff suffered loss as a result.[79]

58. Because of the role of smart contracts, this case does not exactly match the classic paradigm of a fraudulent misrepresentation. All of the steps in the Attack occurred through the instantaneous execution of a series of commands and trades with the index pools' smart contracts. As such, the defendant did not make any misrepresentation directly to any human mind. Nonetheless, the Attack was essentially *computer deception*. In particular, it was market manipulation, which the courts have held constitute an actionable misrepresentation for the purposes of the tort of civil fraud.

59. Market manipulation amounts to a misrepresentation by conduct and/or as a form of active concealment. The tort of civil fraud usually requires a positive misrepresentation, i.e. non-disclosure of a material fact is generally not sufficient. However, non-disclosure has been

---

[79] *Bruno Appliance and Furniture, Inc. v. Hryniak*, 2014 SCC 8, at para. 14.

held to constitute a misrepresentation if the defendant took active steps to conceal the truth.[80] Courts have held that market manipulation is a form of misrepresentation:

> Market manipulation is a form of representation. The very purpose of market manipulation is creating an artificial stock price or trading volume that induces investors to buy or sell the stock in question. It follows that failure to disclose market manipulation can constitute active concealment or non-disclosure of a material fact for the purposes of meeting the fraudulent misrepresentation test.[81]

60. In this case, the defendant used flash loans to purchase almost all of the reference tokens for the TotalPoolValue benchmark (UNI for the DEFI5 pool, and LINK for the CC10) pool). As explained above, his purpose was to distort the TotalPoolValue benchmark. This effectively misrepresented to the index pools that the distorted value for the benchmark fairly represented the value of the assets in the pools. The index pool was effectively a computerized agent for the individual tokenholders (it was authorized to trade their tokens in accordance with its code) and therefore the defendant's misrepresentation to the index pool smart contracts was in effect a misrepresentation to the individual tokenholders. By manipulating the benchmark, the defendant actively concealed the true state of the pool's holdings from the index pools (and therefore from the tokenholders). He then exploited this distorted value to cause the index pools to sell him assets at a fraction of their true value.

61. **Rescission:** although the execution of a smart contract is capable of leading to the formation of a valid legal contract,[82] no valid contract could be formed in the circumstances of

---

[80] *Borelli v. Chan,* 2018 ONSC 1429 (Div. Ct.) at para. 912.
[81] *National Bank Financial Ltd. v. Potter,* 2013 NSSC 248 at para. 679, rev'd in part but on other grounds 2015 NSCA 47.
[82] Luesley, *supra* at 156, BOA Tab 1.

the Attack. The contracts should be rescinded and the defendant required to make restitution to the affected tokenholders.

62. The court may rescind a contract for material misrepresentation, even if innocent[83] or on the basis of unilateral mistake.

63. The common law has long prevented a contracting party from taking advantage of a unilateral mistake by their counterparty. Where there is an obvious error in the terms of an offer, the law does not permit the offeree to "snap up" the offer and enforce the agreement.[84] These principles were applied in the context of a pricing glitch for an online retailer by the Singapore Court of Appeal in a 2005 decision, *Digilandmall.com*.[85] Through a pricing glitch on an online retailer's website, HP LaserJet printers were listed for sale at $66, instead of the correct price of $3,854. The plaintiffs had purchased over 700 printers at the incorrect price and sued to enforce the contract. The court applied the "snapping up" cases and held that there was no valid contract. There was no true meeting of the minds because the plaintiffs were aware of the obvious mistake made by the defendant.[86] Although there do not appear to be any cases applying the "snapping up" cases in the context of smart contracts, academic commentary supports the application of the doctrine in this context.[87]

64. Compared to the Singapore case, this action presents a more compelling case for relief, since here the defendant himself *created* the "glitch" by actively manipulating the index pools.

[83] *Deschenes v. Lalonde*, 2020 ONCA 304 at para. 30 rescission is more readily available in the context of a fraudulent misrepresentation than for negligent or innocent misrepresentation: *Singh v. Trump*, 2016 ONCA 747 at paras. 156-157.
[84] *McMaster University v Wilchar Construction Ltd* [1971] 3 O.R. 801 (Ont. HCJ), citing *Hartog v. Colin & Shields* [1939] 3 All ER 566.
[85] *Chwee Kin Keong v Digilandmall.com Pte Ltd*, [2005] SGCA 2.
[86] *Chwee Kin Keong v Digilandmall.com Pte Ltd*, [2005] SGCA 2 at paras. 92-99.
[87] Luesley, *supra* at 164, BOA Tab 1.

In this case, the net effect of the trades involved in the Attack was that the defendant traded $456,000 of SUSHI tokens for over $16.5 million of other tokens held by the DEFI5 and CC10 index pools.[88] It would have been obvious to the defendant that the only reason the index pools permitted these trades was due to the glitches he had triggered in the index pools' pricing mechanisms. Indeed, the only plausible inference is that this was his very purpose. This Court should not permit the defendant to take advantage of a mistake that he himself deliberately induced.

65. **Unjust Enrichment.** To establish unjust enrichment, the plaintiffs must show that: (a) the defendant was enriched; (b) there was a corresponding deprivation to the plaintiffs; and (c) there was no juristic reason for the enrichment.[89]

66. The defendant enriched himself through the Attack at the direct expense of the DEFI5 and CC10 tokenholders (which include the plaintiffs). The total net assets collected by the defendant were valued at approximately $15.8 million. The DEFI5 and CC10 tokenholders suffered a corresponding loss.[90]

67. There was no juristic reason for this transfer of wealth from the tokenholders to the defendant. The transfer does not represent any legitimate commercial exchange between the tokenholders and the defendant. Instead, the defendant acquired the assets by using computer hacking techniques to manipulate and exploit the computer code controlling the index pools, causing them to sell him assets at a tiny fraction of their true value.

---

[88] Day Affidavit, para 186, MR vol 1, Tab 2, p 67.
[89] *Garland v Consumers' Gas Co.*, 2004 SCC 25.
[90] Day Affidavit, para 186, MR vol 1, Tab 2, p 67.

68. As outlined above, there was no valid contractual basis for the impugned transactions. Further, conduct amounting a breach of the *Criminal Code* will vitiate any juristic reason for a transaction.[91] In this case, the defendant's conduct amounted to fraud, contrary to s. 380(2) of the *Criminal Code* and/or the unauthorized use of a computer service, contrary to s. 342.1.

69. The analysis under s. 380 largely mirrors the discussion of civil fraud above. However, criminal fraud is arguably broader than civil fraud in that it does not require a misrepresentation, but includes other forms of dishonest conduct:

> Fraudulent conduct for the purposes of a fraud prosecution is not limited to deception, such as deception by misrepresentations of fact. Rather, fraud requires proof of "deceit, falsehood or other fraudulent means": s. 380(1). The term "other fraudulent means" encompasses "all other means which can properly be stigmatized as dishonest". … **[T]he fraudulent means "need not involve fraudulent misrepresentation such as is needed to constitute the civil tort of deceit"**.[92]

70. To the extent that criminal fraud is broader than the tort of civil fraud, the defendant's conduct clearly falls within the broader category of prohibited conduct.

71. Section 342.1 of the *Criminal Code* sets out the *Criminal Code*'s prohibition on computer hacking. The provision contains a broad prohibition against "fraudulently and without colour of right…obtain, directly or indirectly, any computer service". "Computer service" is defined broadly to include "data processing and the storage or retrieval of computer data".

72. In this case, the defendant conducted a hack of the trade volume limits on the Initialization Trade for SUSHI. He discovered that the code for the index pool smart contracts

---

[91] E.g. *Garland v Consumers' Gas Co.,* 2004 SCC 25 at para. 48.
[92] *R. v. Riesberry*, 2015 SCC 65 at para 23; c.f. *Adascan v Swad Grain*, 2021 ONSC 210 at para 49, citing *Harland v Francsali* (1993), 13 OR (3d) 103 (Gen. Div.), BOA Tab 2 ("if conduct constitutes fraud under the criminal law it certainly constitutes a wrong for which a civil court can grant relief.").

did not place a limit on the number of mispriced tokens that could be gifted to the pool. By making this gift and then immediately triggering the "Gulp" function, the defendant caused the index pool's pricing mechanism to go haywire. By circumventing the trade volume limit, the defendant fraudulently obtained access to a computer service. This computer hacking was unlawful and vitiates any possible juristic reason for the defendant's enrichment.

ii. Real Risk of Dissipation

73. There is a real and genuine risk that the defendant will dissipate the assets in the Wallet if he is not restrained from doing so. The defendant is a highly adept user of crypto platforms. While transactions on the blockchain are transparent and can be viewed by anyone, the identity of account holders is anonymous by default. The defendant could at any moment transfer the assets from the Wallet to an anonymous account. Worse still, the defendant could use a "privacy mixing" service like Tornado Cash to disguise any such transfers. The defendant is evidently familiar with Tornado Cash, because he used the service to disguise the source of tokens he used to finance the Attack.[93] If the defendant used a privacy mixer to transfer the assets from the Wallet, he would effectively put them beyond the reach of the plaintiffs (and this Court). Indeed, the defendant's father has threatened that the defendant may do exactly this.[94] Further, the defendant has actively deleted other evidence of his involvement in the Attack.[95]

---

[93] Day Affidavit, paras 206-216, MR vol 1, Tab 2, pp 74-77.
[94] Day Affidavit, paras 268-270, MR vol 1, Tab 2, pp 91-92, and Exhibit "42", MR vol 2, p 317.
[95] Day Affidavit at paras. 198 (deletion of Discord chat history), MR vol 1, Tab 2, p 72; 227 (deletion of Wikipedia user account); 228 (removal of information from personal website), MR vol 1, Tab 2, p 81.

74. Moreover, this Court has held that the risk of dissipation can be inferred from the fraudulent nature of a defendant's conduct.[96] As outlined above, the defendant's actions in carrying out the Attack were fraudulent and dishonest.

75. There is no need for the plaintiffs to show that a defendant has assets in Ontario, i.e. Ontario courts have the power to grant worldwide *Mareva* orders against a defendant over whom the court has *in personam* jurisdiction.[97] In any event, it appears that the assets in the Wallet are located within Ontario (to the extent that digital assets can be said to have a physical location). Although the plaintiffs have no direct evidence of the defendant's present whereabouts, circumstantial evidence suggests that he resides in Ontario. The resume posted on his personal website (apparently created in May 2021) states that he is "Living at: Waterloo, ON, Canada since 2017." He grew up in Hamilton, Ontario; he completed a bachelor's degree at the University of Waterloo; and he was, until recently, a master's student at that institution.[98] In October, 2021, his father stated that the defendant does not live with him [redacted] but that they had had recent contact with him.[99] The evidence shows that the defendant is in control of the private key to the digital assets in the Wallet.[100]

iii. Balance of Conveniences Favours Granting the *Mareva* Order

76. The balance of conveniences strongly favours granting the *Mareva* order. The plaintiffs (and members of the proposed class) would be exposed to a significant risk of irreparable harm

---

[96] *Sibley & Associates Lp v Ross*, 2011 ONSC 2951, at para. 64; *Sunwing Airlines Inc v Mora et al*, 2019 ONSC 3917, at paras. 44-47; *Total Traffic Services Inc v Kone,* 2020 ONSC 4402, at paras. 2-4,18-19. [97] *SFC Litigation Trust v. Chan*, 2017 ONSC 1815 para. 38.
[97] *SFC Litigation Trust v. Chan*, 2017 ONSC 1815 para. 38.
[98] The defendant's master's thesis is dated 2021, Exhibit "37" to Day Affidavit, MR vol 2, pp 257-302.
[99] Day Affidavit at, paras. 268-270, MR vol 1, Tab 2, pp 91-92.
[100] Day Affidavit, para 290, MR vol 1, Tab 2, p 97.

if the order is not granted. There is a strong *prima facie* case that they have been the victims of a fraud and have suffered significant losses. Given that the defendant is a 19-year-old who either is (or was until recently) a graduate student, it is very unlikely that he will be able to satisfy a judgment in the amount claimed in the action if the assets in the Wallet are dissipated. Securing these assets is likely the only way to preserve the ability of the tokenholders to obtain compensation for the losses suffered in the Attack.

77. By contrast, the defendant will not suffer any significant hardship or inconvenience if the order is granted. The order is drafted narrowly and only freezes the assets in the Wallet (it does not apply to the defendant's other assets). The misappropriated assets have remained at the Wallet since the date of the Attack and the effect of the *Mareva* order would simply require the misappropriated assets to be preserved pending a return date for the continuation of the injunction until trial. If the defendant is unable to meet living expenses and legal fees without access to those assets, the draft order provides for the usual mechanism for him to apply to the court for relief. Since the assets are readily identifiable online, the plaintiffs are not seeking an asset statement or asset examination in support of the *Mareva* order at this time.

iv. Damages Undertaking

78. The plaintiffs have undertaken to abide by any Order this Court may make concerning damages arising from the granting and enforcement of this Order.[101] The plaintiffs have the financial resources to satisfy any such damages.[102] The fact that the plaintiffs are non-residents with foreign assets does not preclude this Court from accepting their undertaking without the

[101] Day Affidavit at paras 293-296, MR vol 1, Tab 2, pp 97-98.
[102] Day Affidavit at paras. 294-296, MR vol 1, Tab 2, p 98.

need for security.[103] The plaintiffs reside in the United Kingdom and United States, both jurisdictions in which an Ontario judgment could readily be enforced.

v. Full and Frank Disclosure

79. The plaintiffs have provided full and frank disclosure of all the material matters that are within their knowledge in the affidavits filed, as well as identifying arguments the defendant would likely have made if he had been given notice. This includes the following points:

80. **Identity Evidence.** The plaintiffs acknowledge that there are limitations of their evidence regarding the defendant's identity as the individual responsible for the Attack.

81. **Risk of Dissipation.** The defendant has not dissipated the assets in the Wallet since the time of the Attack, which the defendant would likely argue indicates that he does not intend to dissipate the assets in the Wallet.

82. **The "Code is Law" Defence.** The defendant will likely argue that the Attack did not involve any illegal conduct. He did not outright lie or make any positive false statements. He did not carry out a "hack" in the traditional sense of that word, i.e. breaking encryption to gain unauthorized access to a computer system. The defendant will likely argue that all of the trades and commands that he executed were technically permitted to occur under the software of the index pool smart contracts and are therefore legitimate. This argument implies that there are no legal terms that govern the relationship between users of a smart contract, besides the express terms of its computer code. Effectively, the computer code is taken to be the "entire agreement" between users as to how the code will function.[104] As explained in the Day affidavit, this theory

---

[103] *SFC Litigation Trust (Trustee of) v. Chan*, 2017 ONSC 1815 (Div. Ct.) at paras. 50-51.
[104] Luesley, *supra*, at 160, 167, BOA Tab 1.

is known as "Code is Law".[105] It represents a narrow and unrealistic view of the expectations of users on the blockchain.[106] If true, it would mean that the users have implicitly waived all rights they would otherwise have under the common law. This would represent a radical and unjustified departure from the normal rules of private law.

B. Receivership Order

83. This Court has the jurisdiction to appoint a receiver of property to preserve assets on an *ex parte* motion where it is "just or convenient" to do so.[107] The purpose of the receivership in this case is to preserve the assets in the Wallet. The proposed receivership does not contemplate the liquidation or sale of the disputed assets, simply their preservation.

84. Justice Strathy (as he then was) set out the principles governing the appointment of a receiver for the preservation of property as follows:[108]

> (a) The appointment of a receiver to preserve assets is extraordinary relief which prejudges the conduct of a litigant and should be granted sparingly;
>
> (b) There must be strong evidence that the plaintiff's right to recovery is in serious jeopardy.
>
> (c) The appointment of a receiver is very intrusive and should only be used sparingly, with due consideration for the effect on the parties as well as consideration of the conduct of the parties;
>
> (d) The Court must have regard to all the circumstances, but in particular the nature of the property and the rights and interests of all parties in relation thereto.
>
> (e) The test for the appointment of an interlocutory receiver is comparable to the test for interlocutory injunctive relief under *RJR-MacDonald*:

---

[105] Day Affidavit at paras. 284-287, MR vol 1, Tab 2, pp 95-96.
[106] Day Affidavit at paras. 284-287, MR vol 1, Tab 2, pp 95-96.
[107] *Courts of Justice Act,* RSO 1990, c C.43, s. 101; *Rules of Civil Procedure,* RRO 1990, Reg 194, rules 37.07, 45.01, 45.02.
[108] *Anderson v. Hunking*, 2010 ONSC 4008 at para. 15.

(i) Is there a serious issue to be tried?

(ii) Would the moving party suffer irreparable harm?

(iii) Does the balance of convenience favour the relief?

(f) Where the plaintiff's claim is based on fraud, a strong case of fraud, coupled with evidence that the plaintiff's right of recovery is in serious jeopardy, will support the appointment of a receiver of the disputed assets.[109] While proof of fraud is an important consideration, it is not required in all cases.

85. The plaintiffs repeat and rely on their submissions above in respect of the *Mareva* order in support of the appointment of a receiver.

86. The facts of this case make it somewhat unusual and call for special measures beyond the *Mareva* order itself. Due to the decentralized nature of the blockchain, there are no financial institutions or governing authorities which can assist the plaintiffs in enforcing a *Mareva* order. In other words, there is no blockchain equivalent of a bank that can simply freeze the assets in the defendant's accounts. So long as the assets remain in the Wallet, the defendant will be able to control them. This creates a serious risk of dissipation.

87. RCAP is a reputable firm with relevant experience in acting as a receiver over digital assets.[110] Under the terms of the proposed receivership order, the defendant would be required to transfer control of the assets in the Wallet to RCAP, under the direct supervision of RCAP representatives. RCAP would take possession of the disputed assets and would transfer them to a "cold storage wallet", a hardware device that can store tokens. RCAP will securely store the cold storage wallet and maintain control over the assets pending further direction from this Court. The proposed receivership order is limited in scope compared with the Commercial List

---

[109] *Anderson* at para. 15.

[110] Day Affidavit at paras. 277-282, MR vol 1, Tab 2, pp 94-95.

model order: the receiver will have no power or duty to liquidate or manage the assets, simply to take possession of them and preserve them.

PART IV - ORDER REQUESTED

88. The Plaintiffs respectfully request the relief as set out in the draft orders.

ALL OF WHICH IS RESPECTFULLY SUBMITTED this 17th day of December, 2021.

Gerald Chan/Fredrick Schumann/
Stephen Aylward/Alexandra Heine
STOCKWOODS LLP
Barristers

Lawyers for the Moving Parties

SCHEDULE "A"
LIST OF AUTHORITIES

1. *SFC Litigation Trust v. Chan*, 2017 ONSC 1815 at ¶10, 36, 38, 50-51, 60
2. *Chitel v. Rothbart* (1982), 1982 CanLII 1956 (ONCA)
3. *Sibley & Associates LP v Ross,* 2011 ONSC 2951 at ¶11
4. *Aetna Financial Services Ltd. V. Feigelman,* [1985] 1 SCR 2 at p. 27
5. *R. v. Canadian Broadcasting Corp*., 2018 SCC 5, at ¶17, 18
6. *Cytrynbaum v. Look Communications Inc.,* 2013 ONCA 455 at ¶54
7. *Bruno Appliance and Furniture, Inc. v. Hryniak*, 2014 SCC 8 at ¶14
8. *Borelli v. Chan,* 2018 ONSC 1429 (Div. Ct.) at ¶912
9. *National Bank Financial Ltd. v. Potter,* 2013 NSSC 248 at ¶912, rev'd in part but on other grounds 2015 NSCA 47
10. *Deschenes v. Lalonde*, 2020 ONCA 304 at ¶30
11. *Singh v. Trump*, 2016 ONCA 747 at ¶156-157
12. *McMaster University v Wilchar Construction Ltd* [1971] 3 O.R. 801 (Ont. HCJ)
13. *Chwee Kin Keong v Digilandmall.com Pte Ltd*, [2005] SGCA 2 at ¶92-99
14. *Garland v Consumers' Gas Co.,* 2004 SCC 25 at ¶48
15. *R. v. Riesberry*, 2015 SCC 65 at ¶23
16. *Adascan v Swad Grain*, 2021 ONSC 210 at ¶49
17. *Harland v Francsali* (1993), 13 OR (3d) 103 (Gen. Div.)
18. *Sibley & Associates Lp v Ross*, 2011 ONSC 2951 at ¶64
19. *Sunwing Airlines Inc v Mora et al,* 2019 ONSC 3917 at ¶44-47
20. *Total Traffic Services Inc v Kone,* 2020 ONSC 4402 at ¶2-4,18-19
21. *Anderson v. Hunking*, 2010 ONSC 4008 at ¶15

Secondary Source

22. Andrew Luesley, "*Unravelling Smart Contracts: Smart Contracts and the Law of Rescission in Canada*", (2019) 19 Asper Review

SCHEDULE "B"
TEXT OF STATUES, REGULATIONS & BY-LAWS

Criminal Code (R.S.C., 1985, c. C-46)

Unauthorized use of computer

342.1 (1) Everyone is guilty of an indictable offence and liable to imprisonment for a term of not more than 10 years, or is guilty of an offence punishable on summary conviction who, fraudulently and without colour of right,

> **(a)** obtains, directly or indirectly, any computer service;
>
> **(b)** by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system;
>
> **(c)** uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) or under section 430 in relation to computer data or a computer system; or
>
> **(d)** uses, possesses, traffics in or permits another person to have access to a computer password that would enable a person to commit an offence under paragraph (a), (b) or (c).

Definitions

(2) In this section,

> ***computer data*** means representations, including signs, signals or symbols, that are in a form suitable for processing in a computer system; (*données informatiques*)
>
> ***computer password*** means any computer data by which a computer service or computer system is capable of being obtained or used; (*mot de passe*)
>
> ***computer program*** means computer data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function; (*programme d'ordinateur*)
>
> ***computer service*** includes data processing and the storage or retrieval of computer data; (*service d'ordinateur*)
>
> ***computer system*** means a device that, or a group of interconnected or related devices one or more of which,
>
> > **(a)** contains computer programs or other computer data, and
> >
> > **(b)** by means of computer programs,

(i) performs logic and control, and

(ii) may perform any other function; (*ordinateur*)

Data [Repealed, 2014, c. 31, s. 16]

electro-magnetic, acoustic, mechanical or other device means any device or apparatus that is used or is capable of being used to intercept any function of a computer system, but does not include a hearing aid used to correct subnormal hearing of the user to not better than normal hearing; (*dispositif électromagnétique, acoustique, mécanique ou autre*)

function includes logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within a computer system; (*fonction*)

intercept includes listen to or record a function of a computer system, or acquire the substance, meaning or purport thereof; (*intercepter*)

traffic means, in respect of a computer password, to sell, export from or import into Canada, distribute or deal with in any other way. (*trafic*)

Fraud

380 **(1)** Every one who, by deceit, falsehood or other fraudulent means, whether or not it is a false pretence within the meaning of this Act, defrauds the public or any person, whether ascertained or not, of any property, money or valuable security or any service,

…,

Affecting public market

(2) Every one who, by deceit, falsehood or other fraudulent means, whether or not it is a false pretence within the meaning of this Act, with intent to defraud, affects the public market price of stocks, shares, merchandise or anything that is offered for sale to the public is guilty of an indictable offence and liable to imprisonment for a term not exceeding fourteen years.

Courts of Justice Act, R.S.O. 1990, c. C.43

Injunctions and receivers

101 (1) In the Superior Court of Justice, an interlocutory injunction or mandatory order may be granted or a receiver or receiver and manager may be appointed by an interlocutory order, where it appears to a judge of the court to be just or convenient to do so. R.S.O. 1990, c. C.43, s. 101 (1); 1994, c. 12, s. 40; 1996, c. 25, s. 9 (17).

Terms

(2) An order under subsection (1) may include such terms as are considered just. R.S.O. 1990, c. C.43, s. 101 (2).

Courts of Justice Act

R.R.O. 1990, REGULATION 194

RULES OF CIVIL PROCEDURE

Service of Notice
Required as General Rule

37.07 (1) The notice of motion shall be served on any party or other person who will be affected by the order sought, unless these rules provide otherwise. R.R.O. 1990, Reg. 194, r. 37.07 (1); O. Reg. 260/05, s. 9 (1).

Where Not Required

(2) Where the nature of the motion or the circumstances render service of the notice of motion impracticable or unnecessary, the court may make an order without notice. R.R.O. 1990, Reg. 194, r. 37.07 (2).

(3) Where the delay necessary to effect service might entail serious consequences, the court may make an interim order without notice. R.R.O. 1990, Reg. 194, r. 37.07 (3).

(4) Unless the court orders or these rules provide otherwise, an order made without notice to a party or other person affected by the order shall be served on the party or other person, together with a copy of the notice of motion and all affidavits and other documents used at the hearing of the motion. O. Reg. 219/91, s. 3; O. Reg. 260/05, s. 9 (2).

Where Notice Ought to Have Been Served

(5) Where it appears to the court that the notice of motion ought to have been served on a person who has not been served, the court may,

(a) dismiss the motion or dismiss it only against the person who was not served;

(b) adjourn the motion and direct that the notice of motion be served on the person; or

(c) direct that any order made on the motion be served on the person. R.R.O. 1990, Reg. 194, r. 37.07 (5).

Minimum Notice Period

(6) Where a motion is made on notice, the notice of motion shall be served at least seven days before the date on which the motion is to be heard. R.R.O. 1990, Reg. 194, r. 37.07 (6); O. Reg. 171/98, s. 12; O. Reg. 438/08, s. 33.

Evidence by Affidavit
Generally

39.01 (1) Evidence on a motion or application may be given by affidavit unless a statute or these rules provide otherwise. R.R.O. 1990, Reg. 194, r. 39.01 (1).

…

Full and Fair Disclosure on Motion or Application Without Notice

(6) Where a motion or application is made without notice, the moving party or applicant shall make full and fair disclosure of all material facts, and failure to do so is in itself sufficient ground for setting aside any order obtained on the motion or application. R.R.O. 1990, Reg. 194, r. 39.01 (6).

Interim Order for Preservation or Sale

45.01 (1) The court may make an interim order for the custody or preservation of any property in question in a proceeding or relevant to an issue in a proceeding, and for that purpose may authorize entry on or into any property in the possession of a party or of a person not a party. R.R.O. 1990, Reg. 194, r. 45.01 (1).

(2) Where the property is of a perishable nature or likely to deteriorate or for any other reason ought to be sold, the court may order its sale in such manner and on such terms as are just. R.R.O. 1990, Reg. 194, r. 45.01 (2).

Specific Fund

45.02 Where the right of a party to a specific fund is in question, the court may order the fund to be paid into court or otherwise secured on such terms as are just. R.R.O. 1990, Reg. 194, r. 45.02.

DILLON KELLAR et al and ANDEAN MEDJEDOVIC
Plaintiffs Defendant

Court File No. CV-21-00673984-00CP

ONTARIO
SUPERIOR COURT OF JUSTICE

Proceeding commenced at TORONTO

FACTUM OF THE MOVING PLAINTIFFS

STOCKWOODS LLP
Barristers
Toronto-Dominion Centre
TD North Tower, Box 140
77 King Street West, Suite 4130
Toronto ON M5K 1H1

Gerald Chan (54548T)
Tel: 416-593-1617 / GeraldC@stockwoods.ca

Fredrick Schumann (59377L)
Tel: 416-593-2490 / FredrickS@stockwoods.ca

Stephen Aylward (66556E)
Tel: 416-593-2496 / stephena@stockwoods.ca

Alexandra Heine (83514R)
Tel: 416-593-1669 / AlexandraH@stockwoods.ca

Tel: 416-593-7200
Fax: 416-593-9345

Lawyers for the Plaintiffs

Court File No. CV-21-00673984-00CP

ONTARIO
SUPERIOR COURT OF JUSTICE

B E T W E E N:

DILLON KELLAR and LAURENCE DAY

Plaintiffs

and

ANDEAN MEDJEDOVIC

Defendant

Proceeding under the *Class Proceedings Act, 1992,* SO 1992, c 6

MOTION RECORD OF THE MOVING PLAINTIFFS
(Urgent *Mareva* and Receivership Orders)

VOLUME 1

December 17, 2021

STOCKWOODS LLP
Barristers
Toronto-Dominion Centre
TD North Tower, Box 140
77 King Street West, Suite 4130
Toronto ON M5K 1H1

Gerald Chan (54548T)
Tel: 416-593-1617
GeraldC@stockwoods.ca

Fredrick Schumann (59377L)
Tel: 416-593-2490
FredrickS@stockwoods.ca

Stephen Aylward (66556E)
Tel: 416-593-2496
stephena@stockwoods.ca

Alexandra Heine (83514R)
Tel: 416-593-1669
AlexandraH@stockwoods.ca

Tel: 416-593-7200
Fax: 416-593-9345

Lawyers for the Plaintiffs/Moving Parties

TO: [redacted]

TO: **RAYMOND CHABOT ADMINISTRATEUR PROVISOIRE INC.**
Tour de la Banque Nationale 600,
rue De La Gauchetière Ouest Bureau 2000
Montréal, QC H3B 4L8

Emmanuel Phaneuf, M.Sc., CIRP, LIT
Tel: 514-393-4826
phaneuf.emmanuel@rcgt.com

Proposed Receiver

I N D E X

Court File No. CV-21-00673984-00CP

ONTARIO
SUPERIOR COURT OF JUSTICE

B E T W E E N:

DILLON KELLAR and LAURENCE DAY

Plaintiffs/Moving Parties

and

ANDEAN MEDJEDOVIC

Defendant/Responding Party

NOTICE OF MOTION

The Plaintiffs will make a motion to a Judge on Tuesday, December 21, 2021 at 10:00 a.m., or soon after that time as the motion can be heard at 361 University Avenue, Toronto, Ontario.

PROPOSED METHOD OF HEARING: The motion is to be heard

[ ] In writing under subrule 37.12.1(1) because it is made without notice;

[ ] In writing as an opposed motion under subrule 37.12.1(4);

[ ] In person;

[ ] By telephone conference;

[X] By video conference.

THE MOTION IS FOR

i. An interim and interlocutory *Mareva* order freezing the defendant's assets, including the digital assets held in the Wallet (capitalized terms defined below);

ii. An interim and interlocutory order appointing a receiver for the preservation of the digital assets held in the Wallet;

iii. An Order abridging the time for service and filing of the Motion Record, Factum and Brief of Authorities, if necessary;

iv. The costs of this motion; and,

v. Such further and other relief as to this Honourable Court may deem just.

THE GROUNDS FOR THE MOTION ARE

Overview

(b) On October 14, 2021, the defendant, Andean Medjedovic (**"Andean"**), launched a sophisticated cyber-attack (the **"Attack"**) against Indexed Finance, a decentralized financial platform for cryptocurrencies and other digital assets. As a result of the Attack, Andean routed net assets of approximately $15.8 million in crypto assets from two of Indexed Finance's index pools to a "wallet" (account) on the Ethereum blockchain with public address: 0xba5ed1488be60ba2facc6b66c6d6f0befba22ebe (the **"Wallet"**).

(c) To achieve this, Andean used computer hacking techniques to bypass Indexed Finance's trading controls. He executed a series of trades, using approximately $159 million in borrowed assets, that he knew would distort the algorithm used by Indexed Finance to set trading prices. This allowed Andean to purchase those assets at artificially deflated prices, thus acquiring assets representing over 90% of the value of the affected pools at a tiny fraction of their true value.

The Parties

(d) The defendant, Andean, is a 19-year-old mathematics prodigy who has completed a master's degree in mathematics at the University of Waterloo. He is a resident of Ontario.

(e) The plaintiff, Dillon Kellar is a co-founder of Indexed Finance and a resident of the City of [redacted].

(f) The plaintiff, Laurence Day is a full-time contributor to Indexed Finance, where his responsibilities include communications, technical writing, and research. He is a resident of the City of Leeds in the United Kingdom.

(g) Indexed Finance is a project focused on the development of passive portfolio management strategies for digital assets on the Ethereum blockchain. Indexed Finance is an unincorporated association of its users, or “tokenholders.” It is a “decentralized autonomous organization” (or “**DAO**”), a common governance model in the crypto world. Indexed Finance has no physical offices and no centralized location.

Background

(h) Index pools are the blockchain’s equivalent of index funds. They allow users to purchase a digital “token” that represents a pool of digital assets, allowing users to gain diversification through exposure to a broader index of digital assets at a low cost. Index pools are "non-custodial", meaning that the underlying assets are owned by its users (and not by Indexed Finance).

(i) The Attack targeted two index pools:

- **DEFI5:** the "DeFi Top 5 Tokens Index" (or **"DEFI5"**) focuses on large cap decentralized finance protocols across the Ethereum network;

- **CC10:** the "Cryptocurrency Top 10 Tokens Index" (or **"CC10"**) covers the most popular medium to large-cap cryptocurrencies on the Ethereum network.

(j) Index pools are like exchange-traded index funds (**"ETFs"**) in traditional finance. Like a share of an ETF, each token of an index pool represents a fractional stake in a set of underlying assets. Like the shares of an ETF, index pool tokens are traded on an exchange. Like an ETF, the trading price for an index pool token is regulated so that it tracks the net asset value (**"NAV"**) of its underlying assets. Like an ETF, the actual trading price of an index pool token may diverge from its NAV. When this occurs, arbitrage traders can exploit the divergence and earn a profit, at the expense of the pool's tokenholders. Index pools use a complex mechanism to ensure that the pool token's trading price matches its NAV. Unlike an ETF, however, an index pool allows users to issue and redeem their own pool tokens directly from the index pool in exchange for the index token's trading price.

(k) Adding a new token to the pool is akin to adding a new stock to the bundle of stocks included in an index ETF. When a new token is added to one of Indexed Finance pools, the index pool recalculates the trading price for pool tokens using a benchmark called

"TotalPoolValue" which is used to approximate the index pool's NAV (the **"Benchmark"**). The index pool sets a trade volume limit that restricts the number of new pool tokens that can be issued at the new trading price to a maximum of 1.5% of the Benchmark's value.

The Attack

(l) The Attack used market manipulation and computer hacking techniques to deliberately trigger a malfunction in the pricing mechanism for the DEFI5 and CC10 index pools. The malfunction caused the index pools to set a trading price for the DEFI5 and CC10 pool tokens at a tiny fraction of their NAV. The Attack then purchased assets at the depressed trading prices, i.e. to exploit the pricing glitch that the attacker himself had created.

(m) The Attack involved the deployment of customized computer code developed by Andean, involving dozens of trades and hundreds of commands. It occurred over just a few minutes, first targeting the DEFI5 index pool and then the CC10 index pool. While the mechanics of the Attack were highly complex, the plan of the Attack involved three basic components. For the DEFI5 phase of the Attack:

i. **Benchmark Manipulation:** Andean used over $150 million in borrowed assets (more than 10 times DEFI5's NAV) to execute a series of trades designed to manipulate the Benchmark by temporarily distorting the price of its reference asset (the asset price by which the Benchmark is set).

ii. **Hacking the Trade Volume Limits:** by manipulating the Benchmark, Andean caused the DEFI5 index pool to set an artificially low price for the DEFI5 pool token relative to its NAV. Due to the index pool's trade volume limit, Andean should only have been able buy a limited number of pool tokens at prices influenced by the Benchmark manipulation (to a maximum of 1.5% of the Benchmark's value). However, Andean devised a hack by which he disabled the trade volume limit, permitting him to issue himself an enormous number of pool tokens at manipulated prices.

iii. **"Arbitrage" Trades:** the combined effect of manipulating the Benchmark manipulation and circumventing the volume limit was that the DEFI5 index pool set a price for issuing new pool tokens that was vastly below their NAV. Andean executed trades by issuing new pool tokens at the price that his actions had deflated, then immediately redeeming the pool token into its underlying assets. Andean repeated this pattern until he had drained over 90% of DEFI5's NAV.

(n) Andean repeated the above process on the CC10 index pool, with similar results.

(o) Andean funded and coordinated the Attack through the Wallet. He also routed the assets removed from the pools in the Attack to the Wallet.

(p) Andean sought to conceal his identity by running the cryptocurrency used to pay the transaction costs for the Attack through a sophisticated "privacy mixer" called Tornado Cash.

Strong Prima Facie Case of Liability

(q) Andean has been unjustly enriched as a result of the Attack at the expense of the DEFI5 and CC10 tokenholders. There is no juristic reason for Andean's enrichment. The Attack involved conduct that is prohibited by provisions of the *Criminal Code* relating to computer hacking (s. 342.1) and fraud (s. 380(2)).

(r) To the extent that Andean asserts that the juristic reason for his enrichment is a contract or contracts between or among Andean and any tokenholder, any such contracts would be void *ab initio*, or voidable, because of:

i. Fundamental misrepresentation;

ii. Mistake;

iii. Unconscionability; and/or

iv. Fraud or illegality.

(s) Further, Andean violated the duty of honest performance in respect of any such contracts.

(t) Andean's conduct constitutes civil fraud on the holders of DEFI5 and CC10 tokens. In the Attack, he knowingly made a false representation by manipulating the value of the Benchmark. By manipulating the Benchmark, Andean induced the DEFI5 and CC10 index pools – the contents of which were owned by the tokenholders – to sell him the pools' underlying assets at dramatically deflated prices, causing them to suffer significant losses.

(u) In taking the digital assets and storing them in his own Wallet, Andean interfered with the tokenholders' immediate right of possession over the digital assets and is liable in conversion.

Strong *Prima Facie* Case for Proprietary Remedy and Damages

(v) The digital assets stored in the Wallet are the rightful property of the tokenholders and a constructive trust should be recognized or imposed over the Wallet.

(w) The holders of DEFI5 and CC10 tokens suffered direct losses of approximately $12.5 million and $4.0 million, respectively. Furthermore, additional losses were suffered by token holders who held their tokens indirectly, i.e. who owned tokens through other "pools" (the equivalent of a "fund of funds"). The effect of the Attack on the NAV of the DEFI5 and CC10 tokens caused severe disruptions in the prices of any pool token on the blockchain that held DEFI5 and CC10 tokens. In the immediate aftermath of the Attack, these disruptions caused massive and predictable losses to arbitrage traders. The Plaintiffs continue to investigate the quantum of these losses but estimate that they exceed $10 million.

(x) Andean was, at all times, aware that his conduct would harm the tokenholders. His conduct was high-handed, oppressive, harsh, vindicative, reprehensible, malicious, and in disregard of the rights of the DEFI5 and CC10 tokenholders.

Urgent Injunctive Relief is Appropriate

(y) There is a strong *prima facie* case that the assets held in the Wallet are the rightful property of the tokenholders of the DEFI5 and CC10 index pools.

(z) The assets held in the Wallet are at imminent risk of dissipation. The Attack employed a sophisticated "privacy mixer" program called "Tornado Cash" designed to conceal the source of assets transferred into the Wallet that were used to finance the Attack. Andean could dissipate the assets by using Tornado Cash at any time. If he did so, the assets would be put beyond the reach of this Court.

(aa) Further, Andean has deleted evidence of his involvement in the Attack.

(bb) The balance of convenience strongly favours granting a *Mareva* order freezing the defendant's assets and preserving the assets in the Wallet pending trial;

(cc) The moving parties have given an undertaking to pay any damages that the defendant may incur if they are not successful at trial;

(dd) Section 101 of the *Courts of Justice Act*;

(ee) Rules 16.04, 40.01, 45.01, 45.02 of the *Rules of Civil Procedure*;

(ff) Such further and other grounds as the lawyers may advise

.

THE FOLLOWING DOCUMENTARY EVIDENCE will be used at the hearing of the motion:

i. The Affidavit of Dr. Laurence Day, sworn December 9, 2021;

ii. The Affidavit of Adam Avenir, sworn December 6, 2021; and

iii. Such further and other evidence as the lawyers may advise and this Honourable Court may permit.

December 17, 2021

STOCKWOODS LLP
Barristers
Toronto-Dominion Centre
TD North Tower, Box 140
77 King Street West, Suite 4130
Toronto ON M5K 1H1

Gerald Chan (54548T)
Tel: 416-593-1617
GeraldC@stockwoods.ca

Fredrick Schumann (59377L)
Tel: 416-593-2490
FredrickS@stockwoods.ca

Stephen Aylward (66556E)
Tel: 416-593-2496
stephena@stockwoods.ca

Alexandra Heine (83514R)
Tel: 416-593-1669
AlexandraH@stockwoods.ca

Tel: 416-593-7200
Fax: 416-593-9345

Lawyers for the Plaintiffs/Moving Parties

TO: **GOWLING WLG (CANADA) LLP**
Barristers and Solicitors
1 First Canadian Place
100 King Street West
Suite 1600
Toronto ON M5X 1G5

Duncan C. Boswell
Tel: 416-862-4466
duncan.boswell@gowlingwlg.com

Usman M. Sheikh
Tel: 416-862-3627
usman.sheikh@gowlingwlg.com

Tel: 416-862-7525
Fax: 416-862-7661

Lawyers for the Defendant

TO: **RAYMOND CHABOT ADMINISTRATEUR PROVISOIRE INC.**
Tour de la Banque Nationale 600,
rue De La Gauchetière Ouest Bureau 2000
Montréal, QC H3B 4L8

Emmanuel Phaneuf, M.Sc., CIRP, LIT
Tel: 514-393-4826
phaneuf.emmanuel@rcgt.com

Proposed Receiver

Court File No.

ONTARIO
SUPERIOR COURT OF JUSTICE

B E T W E E N:

DILLON KELLAR and LAURENCE DAY

Plaintiffs

and

ANDEAN MEDJEDOVIC

Defendant

AFFIDAVIT OF DR. LAURENCE DAY

I, Laurence Day, of the Town of Otley, in the Metropolitan City of Leeds, in the County of West Yorkshire, in the United Kingdom, MAKE OATH AND SAY:

1. I am one of the Plaintiffs in this proceeding, and, as such, have knowledge of the matters contained in this Affidavit. Where my knowledge is based on information and belief, I indicate the source of my information and I believe it to be true.

2. The factual matters discussed in this affidavit are technical and complex. I have organized this affidavit into five parts to assist the reader.

3. In Part I, I provide a general overview of the issues. In Part II, I provide some general background to the Ethereum blockchain and the nature of index pools. In Part III, I set out the details of the Attack (as defined below). In Part IV, I set out the evidence that shows that the person

responsible for the Attack is the defendant, Andean Medjedovic. In Part V, I address ancillary matters related to the relief sought on this motion.

PART I - OVERVIEW

4. Indexed Finance is a decentralized financial platform for cryptocurrencies and other digital assets. On October 14, 2021, the defendant, Indexed Finance suffered a sophisticated cyber-attack (the **"Attack"**). The user who carried out the Attack (the **"Attacker"**) inflicted losses of $16.5 million[1] in losses on index pools overseen by Indexed Finance. The Attacker routed net assets worth approximately $15.8 million from the index pools to his account (or "wallet") on the Ethereum blockchain.

5. To achieve this, the Attacker used computer hacking techniques to bypass Indexed Finance's trading controls. He executed a series of trades, using approximately $159 million in borrowed assets, that he knew would distort the algorithm used by Indexed Finance to set trading prices. This allowed the Attacker to purchase those assets at artificially deflated prices, thus acquiring assets representing almost all the value of the affected pools.

6. Index pools allow users to purchase a digital "token" that represents a pool of digital assets, allowing users to gain diversification through exposure to a broader index of digital assets at a low cost. Index pools are "non-custodial", meaning that the underlying assets of Indexed Finance's pools are owned by its users (and not by Indexed Finance).

---

[1] All dollar amounts are in USD, the conventional reference currency for digital assets. All USD amounts are calculated using market pricing information quoted by Etherscan, an online tool that uses price aggregators to quote prices in USD for various digital assets. The prices quoted by Etherscan are daily averages and so are less precise than other available pricing information. However, using the Etherscan values allows for consistency to the logs of the transactions discussed in this affidavit.

7. The Attack targeted two index pools:

- **DEFI5:** the "DeFi Top 5 Tokens Index" (or **"DEFI5"**) focuses on large cap decentralized finance protocols across the Ethereum network;

- **CC10:** the "Cryptocurrency Top 10 Tokens Index" (or **"CC10"**) covers the most popular medium to large-cap cryptocurrencies on the Ethereum network.

8. Index pools are like exchange-traded index funds (**"ETFs"**) in traditional finance. Like a share of an ETF, each token of an index pool represents a fractional stake in a set of underlying assets. Unlike an ETF, however, an index pool allows users to issue and redeem their own pool tokens directly from the index pool in exchange for the pool token's trading price. Like the shares of an ETF, index pool tokens are traded on an exchange. Like an ETF, the trading price for an index pool token is regulated so that it tracks the net asset value (**"NAV"**) of its underlying assets. Like an ETF, the actual trading price of an index pool token may diverge from its NAV. When this occurs, arbitrage traders will exploit the divergence and earn a profit, at the expense of the pool's tokenholders. Index pools use a complex mechanism to ensure that the pool token's trading price tracks its NAV.

9. Adding a new token to the pool is akin to adding a new stock to the bundle of stocks included in an ETF. When a new token is added to one of Indexed Finance pools, the index pool recalculates the trading price for pool tokens using a benchmark called "TotalPoolValue" which is used to approximate the index pool's NAV. The index pool sets a trade volume limit that restricts the number of new pool tokens that can be issued at the new trading price to a maximum of 1.5% of TotalPoolValue.

Summary of the Attack

10. The Attack used market manipulation and computer hacking techniques to trigger a glitch in the pricing mechanism for the DEFI5 and CC10 index pools. The glitch caused the index pools to set a trading price for the DEFI5 and CC10 pool tokens at a tiny fraction of their NAV. The Attacker then purchased assets at the depressed trading prices, i.e. to exploit the pricing glitch that he himself had created.

11. The Attack involved the deployment of customized computer code, involving dozens of trades and hundreds of commands. It involved two instantaneous interactions separated by two minutes, the first targeting the DEFI5 index pool and the second targeting the CC10 index pool. While the mechanics of the Attack were highly complex, the plan of the Attack involved three basic components. For the DEFI5 Attack:

(a) **Benchmark Manipulation:** the Attacker used over $150 million in borrowed assets (more than 10 times DEFI5's NAV) to execute a series of trades designed to manipulate the TotalPoolValue benchmark by temporarily distorting the price of its reference asset (the asset price by which the benchmark is set).

(b) **Hacking the Trade Volume Limits:** by manipulating the Benchmark, the Attacker caused the DEFI5 index pool to set an artificially low price for the DEFI5 pool token relative to its NAV. Due to the index pool's trade volume limit, the Attacker should only have been able buy a limited number of pool tokens at prices influenced by the benchmark manipulation (to a maximum of 1.5% of TotalPoolValue). However, the Attacker devised a hack by which he disabled the trade volume limit, permitting him to issue himself an enormous number of pool tokens at manipulated prices.

(c) **"Arbitrage" Trades:** the combined effect of manipulating the TotalPoolValue benchmark and circumventing the volume limit was that the DEFI5 index pool set a price for issuing new pool tokens that was vastly below their NAV. The Attacker executed trades by issuing new pool tokens at the price that his actions had deflated, then immediately redeeming the pool token into its underlying assets. The Attacker repeated this pattern until he had drained 93% of DEFI5's NAV.

12. The Attack repeated the above process on the CC10 index pool, with similar results.

PART II - BACKGROUND

Personal Background

13. I am currently a full-time contributor to Indexed Finance, where my responsibilities include communications, technical writing, and research. I have contributed full-time to Indexed Finance since April 2021, prior to which I was a functional programmer employed by Plow Technologies (an American firm in the oil and gas sector), a financial risk reporting analyst at Standard Chartered Bank in Singapore, and a software compilation researcher at Intel Labs in the United States. I hold a BSc Jt Hons in mathematics and computer science and a PhD in computer science from the University of Nottingham, as well as a Master's degree in financial engineering from WorldQuant University.

14. Dillon Kellar is one of three co-founders of Indexed Finance, along with Samuel Gosling and an anonymous co-founder known as "PR0". [2] Dillon is involved in developing the platform's code, writing smart contracts (*i.e.,* computer scripts), and project management. Dillon has been

---

[2] PR0's identity is known to me through my work for Indexed Finance. He has asked that his name not be made public.

involved in the cryptocurrency space since 2013, working as a consultant and software developer since early 2019. He founded several ventures prior to Indexed Finance, including ZKC (a consultancy), Hypervisor Labs (developing an Ethereum-based blockchain called Interstate Network), and Tiramisu (another blockchain).

15. Dillon is a resident of the [redacted], [redacted]. He is a co-plaintiff with me in this action.

16. Indexed Finance is a project focused on the development of passive portfolio management strategies for digital assets on the Ethereum blockchain. Further information about the nature of the Ethereum blockchain and of Indexed Finance's business is set out in detail below.

17. Indexed Finance is an unincorporated association of its users, or "tokenholders." It is a "decentralized autonomous organization" (or "**DAO**"), a common governance model in the crypto world. The relationship between tokenholders is governed by computer code. The code can be changed only through a governance vote taken by the holders of the Indexed Finance governance token (NDX). There are currently over 5,000 tokenholders, who live around the world.[3] I own approximately 1% of the NDX tokens and Dillon owns 4%. The NDX tokens are traded on crypto markets. The total value of all NDX tokens in circulation is approximately $3.6 million at current prices (the prices of digital assets are highly volatile and so this value is subject to significant fluctuations).

---

[3] This figure is based on the number of "wallets" that hold the NDX token. Some individuals may hold NDX tokens across multiple wallets. Conversely, some wallets may hold NDX tokens on behalf of multiple individuals. Because the identity of a wallet holder is kept anonymous, there is no reliable way to estimate the number individuals who hold the NDX token.

18. Indexed Finance's target user demographic is new users seeking an accessible way to own a diversified portfolio of crypto assets. Most of its users have modest portfolio sizes. For example, for the DEFI5 index pool, at the time of the Attack there were 1,214 unique wallets holding at least 1 DEFI5 token, with a median portfolio value of about 29 DEFI5 tokens (worth roughly $2,600).

19. Indexed Finance does not have any physical offices and is not located in any single geographical location. As is common in the blockchain world, many of the tokenholders are anonymous and known only by their usernames or their account numbers (which are referred to as "addresses" or "wallets").

Basics of Blockchain and Ethereum

20. A blockchain is a digital ledger existing in a distributed database (*i.e.,* a database in which data is stored across different physical locations) using strong cryptography to secure transaction records and verify transfers of ownership. A "permissionless" or "public" blockchain is a universally accessible, decentralized database, stored on any number of computers, anywhere around the world. There is no central server that oversees and maintains the network. It is a "peer-to-peer" network (as opposed to a "server-client" network, such as Google, Facebook, or Amazon).

21. A blockchain serves as a ledger of digital assets. The value of digital assets is represented in the form of "tokens". Tokens are held by individual users in digital "wallets", each of which has a public key (a public account number or address) and a private key, which allows the user to access those assets. Digital assets can be traded for each other, and for government issued currencies such as USD and CAD, on crypto exchanges. There is an active market in these tokens.

22. The largest and best-known digital asset (and token) is Bitcoin (BTC). The Bitcoin blockchain is the original blockchain, which was established in 2009. The present matter relates

to a separate blockchain, Ethereum, which was established in 2015. Ethereum is a programmable, permissionless blockchain platform that allows users to build software to execute blockchain transactions on the Ethereum network. The native token of the Ethereum blockchain is "Ether" (ETH). That is, ETH is to the Ethereum blockchain what BTC is to the Bitcoin blockchain.

23. Software on the Ethereum platform is built via "smart contracts." Smart contracts are self-executing computer programs stored on a blockchain that function in a conditional/deterministic manner (e.g., "if x happens, then y will automatically follow"). There is no human discretion involved in this process — the terms on which a smart contract operates are determined entirely by its code. The Attack exploited aspects of the computer code used in the smart contracts that govern Indexed Finance's index pools.[4]

24. While blockchain is best known for its association with cryptocurrencies, the Ethereum network has evolved to offer a wide array of financial services, including lending facilities and investment products for digital assets. This allows the kinds of financial transactions that, in the world of traditional finance, would be handled by intermediaries such as financial institutions to occur on a peer-to-peer basis. This decentralized ecosystem of financial services is known as "decentralized finance" or "DeFi" (in contrast with traditional finance, or "TradFi").

Indexed Finance

25. Indexed Finance is a DeFi project on the Ethereum blockchain. Indexed Finance is focused on the development of passive portfolio management strategies for digital assets on the Ethereum

[4] While there are multiple smart contracts involved in the Indexed Finance platform, the two that were exploited in the Attack were the "index controller" (which controls the index and sets weights for indexed assets within the index pool) and the index pool's trading mechanism. Each of these is discussed in greater detail below.

network. It oversees “index pools”, which essentially operate as the DeFi equivalent of index funds. As with traditional index funds, Indexed Finance’s index pools are designed to appeal to users who are seeking diversification, through a broad exposure to the market, at a low cost.

26. The Indexed Finance software was developed by Dillon, building on pre-existing open-source code.

27. Cyber-attacks and exploits are common in the blockchain environment. Because systems run entirely on computer code, without human intervention or discretion, inadvertent errors or weaknesses in a system’s code leave that system vulnerable to exploitation. Most exploits occur shortly after a new platform is launched. Before Indexed Finance was launched, its source code was subject to extensive security audits by two leading Ethereum auditors. The protocol operated from December 2020 up to the date of the Attack (October 14, 2021), without any material problems. Users grew confident in the security of the Indexed Finance platform. By the time of the Attack, Indexed Finance had $34 million in “total value locked”, the equivalent of “assets under management” in the TradFi world.

Index Funds vs. Index Pools

28. Index pools use blockchain technology to decentralize and automate functions typically performed by a fund manager for traditional index funds. To understand the functioning of index pools, it is first necessary to review the mechanics of traditional index funds.

Index Funds

29. A traditional index fund tracks the performance of an “index”, an aggregate measurement of the performance of a pool of assets. For example, the S&P 500 *index* is a broad-based market

index that tracks the value of the 500 largest companies traded on US stock exchanges. An S&P 500 index *fund* is a fund comprising the stocks of the companies listed in the S&P 500 index, such that the performance of the index fund tracks the performance of the index.

30. An index fund is divided into "shares" which are offered to investors. This allows an investor to gain diversification through exposure to the performance of the index. It would be prohibitively expensive for most retail investors to replicate the index, e.g., by purchasing shares of each of the 500 companies on the S&P 500. An index fund allows many investors to pool their resources to buy the shares, then issue one share of the index fund to each of the investors.

31. The term "weight" has two distinct meanings, one in relation to the index itself, and the other in relation to an index fund. (Below, I introduce a third meaning of "weight", this one specifically in relation to the code of an index pool.) In relation to an *index*, an asset's "weight" means that asset's value as a percentage of the total value of the index. In relation to an index *fund*, an asset's "weight" means the value of the holdings of the fund in that asset as a percentage of the total holdings of the fund.

32. No index fund can perfectly match the performance of its target index. The performance of the index is a mathematical ideal based solely on the prices of the underlying assets. An index fund is a real-world approximation of that theoretical ideal. The performance of an index fund will differ from the performance of the index. This difference is called "tracking error." Tracking error occurs because of factors such as transaction costs, management fees, and differences between the weight of assets in the index fund and their weight in the index itself.

33. The last "tracking error" factor referred to above warrants more explanation. Generally, the weight of an asset in an index (**"Index Weight"**) depends on some variable such as market

capitalization, and so the Index Weight of the indexed assets fluctuates in real time with the market prices of those assets. The weight of the asset in an index fund cannot keep pace with those fluctuations: a fund manager cannot buy and sell assets as quickly as market prices change. This creates a lag between the weight of an asset in the index and its weight in the index fund. This difference in weights, in turn, leads to tracking error. As explained below, Indexed Finance uses index pools to minimize tracking error.

34. There are two types of index funds: mutual funds and exchange-traded funds (**"ETFs"**). A mutual fund is managed by a fund manager. To buy into the fund, an investor must buy shares from the fund manager. To exit the fund, an investor "redeems" their shares by selling them back to the fund manager. The price at which the shares are traded is determined by the net asset value (**"NAV"**) of the fund, which means the value of the underlying assets (put simply, a fund's NAV is the "sum of its parts"). The price of a mutual fund share is recalculated at periodic intervals to equal the NAV per share. Between recalculations, as market prices fluctuate, the NAV per share may diverge from the price per share.

35. ETFs are a more recent innovation that automate certain functions of the fund manager in a mutual fund. Rather than buying shares from, and selling shares to, a fund manager, investors buy and sell shares of an ETF by trading with each other on an exchange. As a result, index ETFs generally have lower management fees and higher liquidity than index mutual funds.

36. In contrast to a mutual fund, the price per ETF share is set by market forces. The price of an ETF share generally tracks the ETF's NAV per share, but there may be temporary divergences between market price and NAV per share. In such a situation, the ETF shares are said to be "mispriced." Mispricing is generally minor because, when it occurs, arbitrage traders will enter

the market to even out the price discrepancy. For example, if an ETF is trading below its NAV per share, the ETF shares are undervalued compared to its underlying assets. An arbitrage trader will purchase the undervalued asset (the ETF), expecting to earn a profit by selling it when the ETF's market price rises towards to its NAV per share.[5]

37. To reduce tracking error and arbitrage opportunities, the total number of shares in an ETF, called its "supply", must be actively managed. The supply must be adjusted to manage the ETF's trading price and keep it in line with its NAV. Otherwise, market forces could drive the share price away from its NAV per share. For example, if interest rates fall, demand for equities (including equity index ETFs) will increase. If the ETF's supply remains constant, the increased demand will bid up the trading price of the ETF's shares, which could cause the trading price to diverge from its NAV. In that scenario, arbitrage traders would enter the market and earn a profit at the expense of the ETF's shareholders (by short selling the ETF). In an ETF, the supply of fund shares is managed by financial institutions that monitor the ETF's market price and issue or redeem ETF shares to maintain parity between the fund's NAV per share and its market price. Managing supply in this way may also be necessary to maintain liquidity, i.e. to ensure that investors can always purchase shares of the ETF.

Index Pools

38. Index pools are the DeFi equivalent of index funds. Index pools allow a user to purchase a token that represents a pool of digital assets. By owning a token, a user has a proprietary claim on a proportionate share of the underlying assets in the index pool.

---

[5] This is an oversimplification. The detailed mechanics of ETF arbitrage are not relevant here.

39. At the time of the Attack, Indexed Finance offered six distinct index pools. Each index pool is based on a separate index of digital assets. The Attack successfully targeted two of the six pools: DEFI5 and CC10.

40. Holdings in an index pool are represented by a token, e.g., there are DEFI5 tokens and CC10 tokens. These tokens are the equivalent of "shares" in an index fund. The index pool tokens represent fractional ownership of the digital assets held in each index pool. Like index funds, index pools are fully backed by these underlying assets. In other words, the index pool always holds "deposits" of sufficient underlying assets such that it could redeem 100% of the outstanding pool tokens.

41. The most obvious difference between Indexed Finance's index pools and an S&P 500 index fund is that its index pools hold crypto assets, whereas an S&P 500 index fund holds shares in corporations. But this is only a superficial difference. While most index pools focus on crypto assets, mutual funds or ETFs can (and do) hold crypto assets (there are several crypto ETFs currently trading on the TSX), and a DeFi index pool could theoretically be used to track the value of non-crypto assets.

42. The real difference between index pools and index funds is not their underlying assets, but how those assets are managed. Index pools are the next step in the progression that began with the move from mutual funds to ETFs. Just as ETFs automate certain functions that a fund manager performs for a mutual fund, index pools further automate and decentralize the functions that a financial institution perform for an ETF. In doing so, index pools aim to reduce management fees and reduce tracking error.

43. Like ETF shares, index pool tokens are traded on exchanges. Like ETF shares, the market price of these pool tokens generally tracks their NAV. Unlike ETFs, which are traded on traditional securities exchanges such as the TSX and the NYSE, index pool tokens are traded on crypto exchanges along with other digital assets. In the crypto world, there are both centralized crypto exchanges, such as Coinbase, which operate analogously to traditional exchanges, and decentralized exchanges, such as Uniswap, which operate on a peer-to-peer basis. Index pool tokens are traded on decentralized exchanges.

44. Three functions that are centralized for an ETF are decentralized in an index pool: pool re-balancing, custodianship of the underlying assets, and control of the supply of pool tokens.

45. **Pool Re-Balancing:** in a traditional index fund, a fund manager buys and sells amounts of the underlying assets so that the weights of the assets in the fund match their weights in the index. Index pools do not depend on a fund manager or other intermediary for this function. Instead, index pools automate the re-balancing process by allowing arbitrage traders to trade with the pool directly. The index pool incentivizes trades that move the fund towards parity with the index. The profits of the arbitrage traders are essentially a fee paid by tokenholders for the service of re-balancing the pool without the need for an intermediary. The process by which this occurs is central to the issues in this case and is discussed in detail below.

46. **Custodianship of Underlying Assets:** in an index fund, investors effectively pool their money to buy underlying assets and share in the returns. For this to work, a trusted financial institution (a “custodian”) holds the underlying assets. The costs of this service are passed on to the index fund’s shareholders in the form of management fees.

47. This “custodian” function is unnecessary on the blockchain because the distributed ledger securely and transparently tracks the location of the underlying assets. The underlying tokens are “deposited’ with the index pool’s smart contract in the sense that the underlying tokens are sent from a user’s “digital wallet” to a blockchain address associated with the index pool smart contract. The smart contract then executes trades in the underlying tokens on behalf of the tokenholders. The index pool smart contract has no power to do anything with the tokens other than execute trades in accordance with its underlying software. The security of the ledger is guaranteed by the integrity of the Ethereum blockchain itself.

48. **Control of Pool Token Supply:** as explained above, the proper functioning of a traditional index fund requires a financial institution to actively manage the supply of fund shares, which increases management fees. In an index pool, users can create (“mint”) and redeem (“burn”) their own index pool tokens by trading (“swapping”) them for a proportionate amount of the underlying assets.

49. A user “mints” new pool tokens by providing underlying assets to the pool. As stated above, in the case of Indexed Finance, the underlying assets are tokens representing cryptocurrencies and other digital assets. “Minting” can be done either by providing all the underlying assets in exchange for an index pool token (an “all-asset mint”), or by providing a single asset held within the pool (a “single-asset mint”). An all-asset mint is functionally equivalent to an individual index fund investor buying shares of each company on the S&P 500 and trading them in for new shares of an S&P 500 index fund.

50. A user “burns” a pool token by reversing the trade, swapping the pool token back into the pool in exchange for a proportionate share of the underlying assets (an “all-asset burn”). It is also

possible to burn pool tokens into a single underlying asset (a "single asset burn"). The mechanics of single asset mints and burns are relevant to the Attack and are discussed further below.

51. Allowing fund participants to create and destroy their own fund shares would be wildly impractical in the world of traditional finance. It is made possible by special features of the DeFi ecosystem. For example, digital assets are divisible. As noted above, it would be prohibitively expensive for a single investor to buy shares in each company on the S&P 500. But on the blockchain, a single investor can trade fractional amounts of any asset, the equivalent of a single investor buying 0.0001 shares of each company on the S&P 500. Moreover, the distributed ledger on the blockchain means there is a permanent and real-time record accurately showing who owns which pool tokens. Trades in digital assets are settled instantaneously, whereas traditional trades in securities only settle days after the trade first clears.

52. As with all transactions with Indexed Finance index pools, "minting" and "burning" tokens is permissionless. This means that a user on the Ethereum blockchain can execute these functions at any time without prior authorization or approval from Indexed Finance. Indexed Finance imposes fees for these transactions, which range from 0% to 2.5% depending on the precise trading strategy employed (there are no fees for an "all-asset mint").[6]

53. For Indexed Finance's index pools, there is no limit to the number of new pool tokens that a user can create using an "all asset mint." For an index pool of two equally weighted underlying tokens, ETH and BTC, if a user deposited $100 billion of each token, they would be issued pool tokens worth $200 billion. For an "all-asset burn", the only limit is the number of tokens in the

[6] A portion of these fees is retained by Indexed Finance and a portion is returned to other tokenholders of the index pool to offset "impermanent loss" (a trading loss caused by the mechanics of index pool trading, the details of which are not relevant here).

pool (a user cannot redeem more tokens than are in the pool). As discussed below, index pools do place limits on the volume of trades in which a single underlying asset is swapped with a pool token.

Index Composition

54. Indexed Finance itself created the indices that are tracked by its index pools, including the DEFI5 and CC10 indices that the Attack targeted. This differs from most index funds, which follow pre-existing market indices, such as the S&P 500.

55. To create an index, Indexed Finance must determine its *composition*, which means the specific tokens to be included and their relative Index Weights. Index composition is regulated by an "index controller." The index controller is a smart contract that sets Index Weights, using a formula that adjusts for market capitalization.

Selecting Index Tokens

56. To determine which tokens should be included in the index, the index controller runs a filter on a list of candidate tokens and selects the tokens that are ranked highest. For example, the DEFI5 index controller selects the five tokens from the list of candidates that have the largest diluted market capitalization (according to market pricing information from Uniswap). The list of candidate tokens is overseen by the community of Indexed Finance token holders, who add or remove tokens from the candidate list for an index pool through a voting process.

57. Large fluctuations in token value may require a change to the tokens in the index (a **"Re-Indexing"**). The equivalent for the S&P 500 would be when an indexed company falls greatly in

value and drops out of the list of the 500 largest companies (e.g. Enron), to be replaced by another company that now belongs in that list.

58. Indexed Finance does not centrally initiate the Re-Indexing process. Instead, the index controller permits a Re-Indexing to be triggered periodically (about once a month). Any user can trigger a Re-Indexing. Executing commands on the Ethereum blockchain requires a user to pay transaction fees using ETH (known as "gas"). Rather than executing the Re-Indexing function automatically (and having to pay the gas), the index controller leaves it to individual users to trigger a Re-Indexing by running the command.

59. When a Re-Indexing is triggered, the index controller runs a script to determine which of the candidate tokens (including the ones currently in the index) are ranked highest. If a token in the index has dropped below another candidate (because it has decreased in value or the other has increased in value), it will be replaced in the index by the other token.

Index Weighting

60. The index controller also assigns an Index Weight for each of the indexed tokens.

61. The simplest way to set Index Weights would be by market capitalization, i.e. the weight of each asset in the index would be the ratio between its market capitalization and the total market capitalization of all the indexed assets. The S&P 500 is an example of an index that is weighted by market capitalization: the weight of each stock in the index is the ratio between its market capitalization and the total market capitalization of all the companies in the index.[7]

[7] Technically, by "free float capitalization" but the distinction is irrelevant here.

62. However, weighting by market capitalization has drawbacks where the underlying assets vary widely in their market capitalization, as crypto assets do. If an index were weighted purely by market capitalization, the performance of the "largest" tokens would dominate the performance of the index, thus diluting the benefits of diversification.

63. To mitigate this effect, for the DEFI5 and CC10 indices, the index controller sets Index Weights by using a square root of market capitalization function (the **"Square Root Market Cap Function"**). The Square Root Market Cap Function sets each asset's Index Weight by dividing the square root of its market capitalization by the sum of the square roots of all indexed assets' market capitalizations. This function still weights assets with larger market capitalization more heavily, but less so than would be the case if market capitalization itself were used.[8]

64. Because the market capitalizations of the indexed assets fluctuate, it is necessary to periodically re-run the Square Root Market Cap Function to re-calculate their Index Weights. Because running commands on the Ethereum blockchain requires a user to pay ETH as "gas", running the Square Root Market Cap Function continuously would be costly. Like the Re-Indexing function, the index controller allows users to trigger a re-weighting function (**"Re-Weighting"**). The Re-Weighting function causes the index controller to recalculate the Index Weights using the Square Root Market Cap Function.

[8] In a simple index pool consisting of asset X (value $100) and asset Y (value $25), in a purely market cap-weighted index, asset X would have a weight of 100/125 = 80% of the fund's total value. If the pool instead used the square root of market cap (10 for asset X, 5 for asset Y), asset X's weight would be 10/15 = 66.7%.

65. The Re-Weighting function may be triggered at any time after one week has passed since the previous Re-Weighting or Re-Indexing. A Re-Indexing may be executed at any time after one week has passed after three Re-Weightings.

Index Pool Composition

66. The previous section described the process for determining the composition of an Indexed Finance *index*, meaning which assets are in the index, and their Index Weights. This section describes the process for determining the composition of an Indexed Finance *index pool*, meaning which assets are held in the pool, and their weights in the pool.

67. As in the relationship between a stock market index and an index fund, the index serves as a theoretical ideal. The index pool is designed to replicate the performance of the index as accurately as possible, i.e., to minimize tracking error. The specific assets in the index pool will generally match the assets in the index. The only exception to this occurs when there is a Re-Indexing. When an asset is removed from the index, it is not immediately removed from the index pool. Instead, it is gradually phased out.

68. The weight of a token in a pool (**"Pool Weight"**) means the value of the pool's holdings of that token, divided by the value of the total holdings of the pool. The aim of the index pool is for the Pool Weight of each token to match as closely as possible its Index Weight. However, this is not always the case, and a mechanism is needed to adjust the amounts of each token that the pool holds (called their "**balances**") to maintain parity between each token's Pool Weight and its Index Weight. This process is called "re-balancing". Indexed Finance re-balances its index pools very differently from traditional index funds. Understanding this process is fundamental to understanding the Attack, which is discussed in detail in the next section.

Index Pool Re-Balancing

69. Re-balancing is necessary in three scenarios:

(a) **Re-Indexing:** when a Re-Indexing occurs, and an old token is replaced by a new token, the pool must acquire the new token and sell the old token.

(b) **Re-Weighting:** when the Index Weights change, the pool must acquire tokens whose Index Weights have increased and sell tokens whose Index Weights have decreased.

(c) **Maintenance Re-Balancing:** even as the composition of the index remains constant, the Pool Weights of the tokens will vary with market prices. For an index that is weighted purely by market capitalization (as is the S&P 500), these price changes would cause equivalent changes in the Index Weights, and so no re-balancing would be necessary. But for indices that are weighted in another manner, changes in market prices will cause the Pool Weights to diverge from their Index Weights. Where the market price of a token has increased relative to the others in the pool, the pool will need to divest that token and acquire more of the other tokens to align Pool Weights with Index Weights.

70. For a traditional index fund, the fund manager re-balances the index fund by periodically buying and selling the underlying assets. Indexed Finance does not employ a fund manager to centrally re-balance its index pools. Instead, Indexed Finance has decentralized this process. It does so by effectively inverting the model used by traditional index funds. Instead of actively buying and selling tokens, the index pool creates an incentive structure for arbitrage traders to do

the re-balancing themselves. Whereas a fund manager changes the “balances” of fund assets directly, index pools use price signals to indirectly change balances.

71. An index pool sets a price at which it is willing to buy or sell each token in the pool (the “**Pool Price**”). Since an index pool allows users to trade directly with the pool, users can buy or sell any token in the index pool by trading (swapping) it for another token held in the pool. Those trades will occur at the Pool Price. (This “price” is in reality a series of exchange rates at which the index pool will swap one asset into the other pool assets.) The index pool sets Pool Prices to incentivize trades that will help re-balance its holdings.

72. In other words, unlike fund managers, who adjust the *balances* of fund assets, index pools adjust the *prices* at which the pool is willing to buy or sell assets, which indirectly results in the balances moving to the desired level, and thus bringing Pool Weights in line with Index Weights.

73. The mechanics of the Pool Price are described below. Essentially, however, when the balance of a token is too low, such that its Pool Weight is less than its Index Weight, the pool will incentivize traders to swap it into the pool, by setting a Pool Price that exceeds the token’s market price. Conversely, when the balance of a token is too high, such that its Pool Weight exceeds its Index Weight, the Pool Price will incentivize traders to swap it out of the pool, by setting a Pool Price that is less than its market price. As these trades occur, they will move the balance of the token such that its Pool Weight approaches its Index Weight. If the Pool Weight and Index Weight are equal, then the Pool Price will equal the market price, and the opportunity for arbitrage will no longer exist.

74. Re-balancing in the traditional way (e.g. by buying and selling assets centrally) requires frequent trading on the open market. This would involve significant transaction costs on the

Ethereum blockchain and would require a level of centralized control that is contrary to the way Indexed Finance operates. Decentralizing the re-balancing process avoids management fees and permits re-balancing to occur in real time, which minimizes tracking error.

The Automated Market-Maker Function

75. Re-balancing in this way requires a mechanism by which the index pool can determine the appropriate Pool Price. Indexed Finance sets its Pool Prices with an “Automated Market-Maker” function (“**AMM**”). An AMM sets the exchange rates (i.e. Pool Prices) by which tokens within a pool can be freely traded, one with one another.

76. The AMM uses a mathematical model to set prices for tokens in terms of one another. The details of this formula are not relevant to the issues in this proceeding. However, three features of the AMM are relevant here:

(a) **Supply and Demand:** the Pool Price follows a logic of supply and demand based on the assets held in the pool. As traders buy more of a token, its Pool Price increases (i.e., it requires more of other tokens to be exchanged to acquire that token). As traders sell that token into the pool, its Pool Price decreases.

(b) **Pool Price Determined by Weights and Balances:** at pool inception, the AMM sets a Pool Price for each token that is equivalent to its market price. However, after that point, the Pool Price does not depend on market prices. Instead, it is determined exclusively as a function of the notional weights of the tokens (their “**AMM Weights**”) and balances. A token’s AMM Weight typically equals its Index Weight, subject to some important exceptions, which are described below. By setting the AMM Weight to equal the Index Weight, the index controller creates a price incentive structure that will move Pool Weights towards the Index Weights. After the index controller sets AMM Weights, the Pool Price is purely a function of token balances.

(c) **Pool Price Is Non-Linear:** the AMM's pricing formula is a non-linear function. As the balance of a token decreases, its Pool Price increases exponentially (and as its balance increases, its Pool Price decreases exponentially). The AMM does not allow the balance of any token to go to zero, because, as the final tokens are purchased, the Pool Price rises to infinity.

77. In the previous section, I described the index pool as setting a Pool Price for each token as part of the re-balancing process. To be more precise, the index pool does not directly set the Pool Price. Rather, the index pool's index controller sets the AMM Weight for each token. Because Pool Price is just an exchange rate that is purely a function of the tokens' relative AMM Weights and balances, by setting the AMM Weights for the tokens, one effectively sets its "price."

78. In a perfectly efficient market, Pool Prices and market prices would always be the same. While no market is perfectly efficient, there is a high volume of trading on the Ethereum blockchain and active arbitrage traders mean that Pool Prices are generally kept in line with market prices.

79. While trading with an index pool is permissionless, Indexed Finance sets swap fees of 2%, which is relatively high by DeFi standards (lower swap fees are used where the purpose of the AMM is to boost token liquidity, another common application of AMMs). This minimizes "noise trading" because an arbitrage trade will only be profitable where the returns exceed the swap fee.

Single Asset Mints and Burns

80. The AMM also allows users themselves to mint and burn index pool tokens (i.e. the tokens representing a stake in the index pool itself, such as DEFI5 and CC10 tokens). The simplest way to do this is the "all-asset mint" or "all-asset burn", where, respectively, the user creates or redeems pool tokens in exchange for each of the underlying tokens, in ratios that correspond to their weights. However, some users will not have, or want to acquire, all the underlying tokens; they may prefer to swap pool tokens for a single underlying token. Hence, the AMM allows users to exchange pool tokens for any one of the underlying tokens.

81. How many underlying tokens are required to "mint" a single pool token is calculated based on the notional amount of the underlying token that would be required to purchase all the other tokens in proportion to their Pool Weight. This would be like a mutual fund investor selling 17 shares of Microsoft in exchange for one newly issued share of an S&P 500 index fund.[9] Conversely, a user can "burn" a pool token by selling it for a single token held in the pool (i.e. like selling one share of the S&P 500 index fund for 17 Microsoft shares).

82. As noted above, the index pools do not place any limits on all-asset mints. All-asset burns are limited only by the number of underlying tokens in the pool. But the index pool does place limits on the volume of "single asset mints" and "single asset burns". For a single-asset mint, the index pool will only permit a user to swap in up to 50% of the pool's balance of a single token in a single swap (the **"50% Swap-In Limit"**). For a single-asset burn, the index pool will only allow a user to swap-out up to one-third of the pool's balance of a single token (the **"33% Swap-Out**

[9] Microsoft's current market capitalization is about $2.5 trillion out of a total market cap of all S&P 500 companies of about $40 trillion, or 6%. 100/6 = 16.67, i.e. ~17 shares of Microsoft are equivalent to one share in the S&P 500.

Limit"). Both limits apply to all swaps with the index pool (not just minting and burning). The limits are designed to limit price distortions in the pool that would result from massive inflows or outflows of a single token. As explained below, the Attacker circumvented these limits in the Attack.

83. The AMM is used in single-asset mints and single-asset burns to quote the price (i.e. the exchange rate) at which the pool token can be traded for other tokens. Rather than consulting market prices, Indexed Finance uses the Pool Prices. As such, like the swaps described above, Pool Prices incentivize single-asset mints and single-asset burns that re-balance the pool.

Adding a New Token to an Index Pool

Minimum Balance and Minimum Weight

84. As explained above, a pool has its own Pool Price for each underlying token. This harnesses arbitrage trading to ensure that Pool Weights match Index Weights. The AMM sets Pool Prices based on AMM Weights (generally equal to Index Weights), independently of market prices. Market values are used at pool inception (since the initial weights and balances of indexed tokens must be set to match their market value). After the pool goes live, there is generally no further need for the AMM to consult external markets. However, there is one occasion when the AMM must consult market prices directly: when the index adds a new token because of a Re-Indexing. In that case, the AMM needs market prices to determine the initial Pool Price for the new token.

85. When a new token is first added to the pool, its balance will be zero. The Pool Price function does not work with a balance of zero. It is therefore necessary for the index controller to use a starting balance and weight, called the "**Minimum Balance**" and "**Minimum AMM**

Weight", to calculate an initial Pool Price (the "**Initialization Price**"). The AMM then allows trades at that price until the new token reaches the Minimum Balance. This process is called "initialization."

86. Recall that, usually, the AMM Weight equals the Index Weight. If the index controller simply used the new token's Index Weight as the AMM Weight, the Initialization Price would be greatly inflated, given the low balance of the new token that is being phased into the pool. Instead, the index controller sets a Minimum AMM Weight of 1% for that purpose. The Minimum Balance is the balance that would result in a Pool Weight of 1% *at current market prices*.

87. Until the balance of the new token reaches the Minimum Balance, the index pool only allows traders to swap the new token *into* the pool (it cannot be swapped out) and offers a slight premium to traders to incentivize them to do so.[10] After the Minimum Balance is reached, the new token is "initialized", and it can be both bought and sold like all the other tokens. The trade in which a token first reaches, or exceeds, its Minimum Balance, is its "**Initialization Trade**."

Setting the Minimum Balance

88. Recall that the Minimum Balance of a new token is the balance that, at current market prices, would represent 1% of the value of the index pool. Therefore, to calculate the Minimum Balance, the index controller must determine the total value of the pool.

89. The pool's total value could be calculated by multiplying each token's balance by its market price and adding the results. However, there is a transaction cost to looking up external

---

[10] This is an example of the "weight adjustment" variety of decentralized re-balancing through the AMM discussed in the previous section.

pricing information on the Ethereum blockchain. To minimize those transaction costs, the index controller uses a shortcut, a benchmark called TotalPoolValue. Rather than directly measuring the total value of the pool (i.e. the pool NAV), the index pool estimates the pool NAV indirectly by using the TotalPoolValue benchmark. TotalPoolValue is calculated by a function that selects a token to use as a reference asset (generally the token with the largest value in the pool). The function then multiplies *that* token's balance by the reciprocal of its AMM Weight. This approximates the total value of the pool, expressed in terms of the benchmark token.

90. For example, if the selected reference token for the pool was ETH, and if the pool had 10 ETH, at an AMM Weight of 10%, TotalPoolValue would be calculated as 100 ETH. To calculate the Minimum Balance for a new token, the index controller would take 1% of 100 ETH, i.e. 1 ETH. If the new token to be added was SUSHI,[11] and SUSHI was trading on Uniswap at 400 SUSHI:1 ETH, then the Minimum Balance would be 400 SUSHI tokens. The Initialization Price for SUSHI tokens will be set accordingly. So, for instance, if a user swaps in 200 SUSHI tokens via a Single Asset Mint, they will receive pool tokens representing 0.5% of the total pool value.

91. Until the token's Minimum Balance has been reached, the Initialization Price governs. This is effectively a standing order from the pool to buy the new token at the Initialization Price (since, until the Minimum Balance is reached, the AMM does not permit users to swap the new token out).

92. This standing order is limited by the 50% Single-Asset Swap-In Limit. As noted above, that limit prevents a user from swapping in more than 50% of a pool's existing balance in a single

[11] SUSHI is the token of the Sushiswap protocol, which is a decentralized crypto exchange (like Uniswap).

swap. Until the new token is Initialized, 50% Single Asset Swap-In Limit is set using the Minimum Balance, not the new token's actual balance (which, of course, begins at zero). So, in the example above, where the Minimum Balance of the new token SUSHI was 400, any user could swap in up to 200 SUSHI tokens at the Initialization Price of 400 SUSHI : 1 ETH.

93. Sometimes, the Initialization Price must be updated before a token is initialized. If the market price of the uninitialized new token increases before the Minimum Balance is attained, no one will want to sell the new token into the pool at the under-market Initialization Price. If no one sells the token into the pool, the new token will never reach its Minimum Balance. The index controller uses another function, 'UpdateMinimumBalance' to correct this problem by recalculating the Minimum Balance and, hence, the Initialization Price.

94. The 'UpdateMinimumBalance' function re-runs the TotalPoolValue calculation by recalculating the market value for the reference token based on fresh market price information and its current balance in the pool, then resets the Minimum Balance and Initialization Price of the new token accordingly. In the example above, if the market price of SUSHI had increased from 400 SUSHI : 1 ETH to 300 SUSHI : 1 ETH and the value of the pool's existing assets remained constant, the Initialization Price would be updated accordingly, and the Minimum Balance would be updated from 400 to 300 SUSHI tokens.

Moving From Initial AMM Weight to Index Weight

Initial AMM Weight

95. When a new token completes initialization (by reaching its Minimum Balance), it is assigned an initial weight ("**Initial AMM Weight**"). The Initial AMM Weight will either equal or

exceed the Minimum AMM Weight (1%) depending on whether the Initialization Trade put the new token's balance at or above its Minimum Balance.

96. So, for example, if the Minimum Balance of SUSHI is 400 and the pool currently has 300 SUSHI tokens, a user can swap in 200 SUSHI (the maximum permitted under the 50% Swap-In Limit). The index controller would then set an Initial AMM Weight for SUSHI of 1.25%, because its current balance would be 1.25 times its Minimum Balance.

97. If, however, the user only swapped in 100 SUSHI tokens, the resulting balance would be 400 SUSHI, exactly equalling the Minimum Balance. There, the Initial AMM Weight would equal the Minimum AMM Weight, 1%.

98. When a new token is initialized and the new token's Initial AMM Weight is set, the AMM Weights of all the other assets must be reduced (the **"Initialization Re-Weighting"**).

99. The Index Weight for a new token will almost always be higher than its Initial AMM Weight. The index pool gradually moves the AMM Weight for the new token from its Initial AMM Weight to its Index Weight. The new token's AMM Weight will rise by a maximum of 1% of its current AMM Weight every thirty minutes until the Index Weight is achieved.

100. For example, assume that the Square Root Market Cap Function calculated an Index Weight for SUSHI of 10%. It is then initialized such that its Initial AMM Weight is 1.25%. The index pool would then gradually increase SUSHI's AMM Weight from 1.25% to 10%.

101. Gradually phasing in the Index Weight is necessary. If the index pool suddenly used the *Index Weight* as its AMM Weight, the Pool Price would suddenly jump from the Initialization Price. In the example above, the same 400 SUSHI tokens that represented 1.25% of the pool's total

value would instantly be deemed by the index pool AMM to now be worth 10% of the pool's value. The SUSHI tokens would be greatly overpriced, and all other pool tokens greatly underpriced. This would be too strong and drastic an arbitrage incentive and would cause price volatility and losses to tokenholders.

PART III – THE ATTACK

Background of the Attack

102. The Attack targeted first the DEFI5 index pool (the **"DEFI5 Phase"**) and then the CC10 index pool (the **"CC10 Phase"**). The transactions were almost identical and exploited the same aspects of the code of each index pool. Each phase of the Attack was carried out in a single "transaction" on the Ethereum blockchain. A "transaction" on the blockchain is a cryptographically signed instruction from an account that changes the state of the blockchain. A single "transaction" may contain multiple trades and commands. In this case, each transaction involved in the Attack was really a series of multiple trades and other commands that were all carried out instantaneously.

103. Both attacks occurred on October 14, 2021, within minutes of each other:

(a) The DEFI5 Phase took place at 6:37:43 pm (UTC). The Attacker removed $12.5 million in tokens, or 93% of the pool's NAV.

(b) The CC10 Phase took place two minutes later, at 6:39:49 pm (UTC). The Attacker removed $4.0 million in tokens, or 98% of the pool's NAV.

104. It is worth emphasizing that the steps involved in each of these transactions were instantaneous. I have summarized below a long series of commands that constituted the DEFI5 Phase of the Attack. These commands were executed by computer code, such that there was no temporal gap between the steps. When the Attack was initiated, all the steps occurred at once (one transaction for the DEFI5 Phase and one for the CC10 Phase).

105. Each phase of the Attack was implemented through the deployment of a dedicated "smart contract". Each contract had been programmed by the Attacker in advance and deployed onto the Ethereum blockchain prior to the Attack. The smart contract for each phase of the Attack contained all of the necessary commands. At the time of the Attack, the Attacker triggered each smart contract, which unleashed the commands that make up the Attack.

106. Since the DEFI5 and CC10 Phases were materially identical, in the analysis below, I describe the DEFI5 Phase in greater detail. I then briefly summarize the CC10 Phase.

The DEFI5 Phase

107. At the time of the Attack, there were 151,038.45 DEFI5 tokens in circulation. The pool's NAV was approximately $13.4 million (each DEFI5 token was worth approximately $88.51). At **Exhibit "1"**, I have set out tables with additional detail regarding the DEFI5 Attack. These tables are listed broken into separate Appendices (Appendix A1, Appendix A2, etc.) and I refer to them by these numbers below. The list of tokens held by the DEFI5 index pool, their balances, and approximate values immediately before the Attack is set out in Appendix A1.

108. The DEFI5 index pool held the following tokens: UNI, AAVE, CRV, COMP, MKR, and SNX. The pool held six assets, rather than its target of five, as SNX was in the process of being phased out because of a recent Re-Indexing. The nature of these tokens is not relevant to understanding the Attack. For completeness, I have included them in a Glossary appended to this affidavit.

109. Immediately prior to the Attack, the largest token in the DEFI5 index pool — and the benchmark token used to calculate TotalPoolValue — was UNI. The pool had a UNI balance of

203,318.87 tokens. On the open market, UNI was trading at $26.29, so the market value of the UNI held in the pool was approximately $5.3 million. UNI's Pool Weight (and Index Weight) was approximately 40%, i.e. UNI tokens made up about 40% of the DEFI5 index pool's NAV.

110. At the time of the Attack, the DEFI5 index was due for a Re-Indexing. A new token, SUSHI, had increased in market capitalization to the point where it was due to replace one of the existing tokens in the index.

The Plan of the Attack

111. The objective of the Attack was to manipulate the Pool Prices for the tokens held in the pool. This permitted the Attacker to mint new pool tokens at an artificially deflated price. The Attack used computer hacking and market manipulation techniques to exploit the index controller's process for adding a new underlying token to the pool, specifically how it set the Initialization Price for new tokens and how the pool resets the prices of other tokens at the time of the Initialization Re-Weighting. The artificially deflated Pool Prices for the tokens in the DEFI5 pool allowed the Attacker to acquire the pool's underlying tokens for a small fraction of their true value.

112. Individual steps in the Attack appear to be illogical when viewed in isolation. Several steps of the Attack involve the Attacker deliberately incurring millions of dollars in losses. Doing so can only be understood as part of a broader scheme to manipulate the index controller and pools.

113. The Attack involved dozens of trades and hundreds of commands. However, the plan of Attack involved three basic components:

1) **Manipulating the TotalPoolValue benchmark** used to set the Initialization Price for the new token, SUSHI;

2) **Hacking the index pool's trade volume** limits to permit an unlimited number of new tokens to be added into the pool in the Initialization Trade for SUSHI, thereby distorting the Initialization Re-Weighting (and ultimately the Pool Prices for all tokens in the pool).

3) **Minting new pool tokens** at the deflated prices and immediately burning them back into their underlying tokens, thereby sapping the pool of more than 90% of its value.

114. **1) Manipulating TotalPoolValue:** as explained above, when a new token is added to an index pool, the index controller calculates its Minimum Balance, which is the number of those tokens that would represent 1% of the total NAV of the pool.

115. As also explained above, to reduce transaction costs, the index controller does not measure pool NAV directly, but rather models it with the TotalPoolValue benchmark. The function used to calculate TotalPoolValue estimates the pool's NAV by extrapolating from the value of a single reference token based on its Pool Price. At the time of the Attack, the reference token was UNI.

116. However, the TotalPoolValue calculation will inaccurately approximate the pool NAV to the extent that the Pool Price of the benchmark token does not match its market price. The Attacker exploited this mechanism by using over $100 million in borrowed tokens to buy up almost all the UNI in the pool. Greatly reducing the balance of UNI caused the Pool Price of UNI to skyrocket, to the point that the Pool Price for UNI was over 860 times its market price. The Attacker then triggered the UpdateMinimumBalance function, which used the manipulated Pool Price of UNI to calculate the TotalPoolValue and set the Minimum Balance for SUSHI. This caused the TotalPoolValue benchmark to vastly underestimate the pool's actual NAV and thus the amount of SUSHI worth 1% of the pool's assets.

117. Further, TotalPoolValue is calculated when the Minimum Balance is set, not at the time of the Initialization Trade. However, that value is reused at the time of the Initialization Trade, in the Initialization Re-Weighting (in which the index pool resets the Index Weights for all assets, which consequently affects their AMM Weights and Pool Prices). If pool NAV changes between when TotalPoolValue is calculated and the Initialization Trade, this will also cause a discrepancy between TotalPoolValue and the pool's NAV at the time of the Initialization Re-Weighting.[12]

118. Having distorted the TotalPoolValue benchmark, the Attacker then reversed his initial trade by swapping UNI back into the pool. In other words, the Pool Price of UNI was distorted temporarily, for just long enough to set a distorted value for TotalPoolValue. The effect of this was that the index controller set an artificially inflated price for the Initialization Trade for SUSHI tokens.

119. **2) Hacking Trade Volume Limits:** as explained above, TotalPoolValue is used to calculate the Initialization Price for a new token. The index pool attempts to set the Initialization Price for the new token at a level that will not alter the Pool Prices of its other assets. However, when the TotalPoolValue benchmark is off kilter, this will distort the Initialization Price of the new token, which in turn will affect the Initialization Re-Weighting, and therefore the Pool Prices for other assets. The extent of the impact is determined by two factors: (i) the *extent* of the mispricing of the new token; and (ii) the *volume* of mispriced tokens traded into the pool:

[12] This does not apply only to chronological "time', but also to the sequence of steps within a single transaction. The mismatch between TotalPoolVaue and pool NAV in this case arose due to a mismatch between TotalPoolValue as set at an earlier sequence in the Attack transaction and the pool NAV later in the sequence of the same transaction.

(a) **Extent of Mispricing:** the extent of the mispricing of the new token is the difference between its Initialization Price and its market price at the time of the Initialization Trade. This divergence is a direct function of the difference between TotalPoolValue and the pool's actual NAV at the time of the Initialization Trade. The greater the error in the TotalPoolValue benchmark, the greater the error in pricing the new token.

(b) **Volume of Initialization Trade:** the impact of the mispricing on the Pool Prices also depends on the volume of new tokens introduced into the pool at the incorrect price. If only a small number of tokens are added to the pool, there will be only a minimal impact on the Pool Prices of other tokens. The index pool sets a trade volume limit that restricts the volume of an Initialization Trade to a maximum of 50% of the Minimum Balance of the initialized token (which is worth 0.5% of the TotalPoolValue). This limit should have contained the damage to the Pool Prices arising from the Attacker's manipulation of TotalPoolValue.

120. The Attacker devised a hack by which he could disable this trade volume limit. The index pool's volume limit on the Initialization Trade only applied to an actual trade—where a user sells the new token in exchange for either pool tokens (DEFI5) or tokens that are currently held within the pool. But the Attacker found a way to circumvent this limit by means of a *gift*. On the blockchain, users occasionally transfer tokens to the wrong address by mistake. When an index pool receives such a transfer, the index pool does not recognize it, and so the Pool Prices are not adjusted in response to the new balance. The code for index pools contains a function that allows the AMM to treat such a "gift" as if it were a trade with no output (called the **"Gulp"** function). The Gulp function updates the pool's internal records to accommodate the new balance. By making

a gift of an uninitialized token and immediately triggering the Gulp function, a user can theoretically "gift" an unlimited number of tokens into the pool.

121. The Attack exploited this aspect of the index controller's code. After the Attacker had successfully distorted the TotalPoolValue benchmark and thus the Minimum Balance of SUSHI, he executed a "gift" of over $2 million of mispriced SUSHI tokens to the DEFI5 pool. He then immediately triggered the Gulp function, which caused the index pool to treat the "gift" as if it were the Initialization Trade for SUSHI tokens. As such, the gift was a Trojan horse. It swamped the pool with overpriced SUSHI tokens. The large volume of mispriced SUSHI tokens caused the Initialization Re-Weighting to go haywire, setting AMM Weights for pool assets that were far lower than their Index Weights. This in turn caused their Pool Prices to decrease.

122. **3) Minting and Burning New Pool Tokens:** the net result of this activity was that the Attacker tricked the index pool into setting an artificially low Pool Price. Having done so, the Attacker simply minted new pool tokens at the deflated prices and immediately redeemed ("burned") those pool tokens for the underlying assets. He repeated this process until he had drained 93% of the value from the DEFI5 index pool.

Step-By-Step Breakdown

123. The previous section provided an overview of the Attack. This section provides a detailed step-by-step analysis of the steps corresponding to each of the three main components identified above.

124. Because of the transparent nature of blockchain transactions, the details of the trades and other commands involved in the Attack are publicly available. Dillon and I have used freely

available tools such as Etherscan to reconstruct the steps in the Attack. Etherscan is a tool that allows users to review the details of blockchain transactions. Etherscan does not display the underlying source code for the smart contracts deployed in the Attack. However, it does display all of the effects of the transaction, i.e. the trades involved in the Attack. Etherscan has a webpage for the transaction involved in the DEFI5 Phase that sets out the movement of all tokens involved in the DEFI5 Phase, as well as an "event log" that records all trades and commands involved in the transaction.[13] This is the raw data that Dillon and I used to reconstruct the Attack. In this form, the data is difficult to interpret. To simplify matters, I have compiled a transaction log for the DEFI5 Phase that sets out the relevant trades and commands and links them to their respective entries in the Etherscan event log (the **"DEFI5 Transaction Log"**). The Transaction Log is attached as **Exhibit "2"**. There are over 200 entries in the DEFI5 Transaction Log. Below, I provide an interpretation of those events in a narrative form that describes each step in the DEFI5 Phase of the Attack.

125. Etherscan shows that the Attack was carried out by a user identified only by a wallet address, 0xba5ed1488be60ba2facc6b66c6d6f0befba22ebe (the "**Attacker's Wallet**"). As I explain below in Part IV, I believe that this wallet is controlled by the defendant Andean Medjedovic, and furthermore was controlled by him during the Attack. The DEFI5 Transaction Log records the transactions involving the Attacker's Wallet that comprise the Attack.

126. The Attacker's Wallet was a new account created before the Attack. It had no transaction history until the morning of the Attack on October 14, 2021, when it became active at around 4:27

[13] https://etherscan.io/tx/0x44aad3b853866468161735496a5d9cc961ce5aa872924c5d78673076b1cd95aa (note: this page annotates the Attacker's Wallet as "Indexed Finance Exploiter". This annotation was made by Etherscan itself based on publicly available information about the Attack. Neither I nor Dillon, nor to my knowledge anyone else involved in Indexed Finance requested that this annotation be added.

am (UTC). The Attacker laid the preparatory work in the hours leading up to the Attack. In order to finance the DEFI5 Phase, the Attacker had to transfer ETH to the Attacker's Wallet. The Attacker's Wallet received transfers of ETH in three transactions between 6:02 am and 4:42 pm UTC). At 4:03 pm (UTC), the smart contract that facilitated the DEFI5 Phase of the Attack (the **"DEFI5 Attack Contract"**) was deployed. Once the smart contract was deployed, it was available to be triggered at any time. The transaction for the DEFI5 Phase of the Attack consisted of the Attacker's Wallet triggering the DEFI5 Attack Contract, which carried out a series of trades and commands culminating in most of the value in the DEFI5 pool being routed to the Attacker's Wallet.

Manipulating the TotalPoolValue Benchmark (Steps 1-5)

Step 1: Trigger Re-Indexing

127. Beginning in February 2021, the Indexed Finance community began to discuss adding a new token to the candidate lists for the DEFI5 (and CC10) index pools. These discussions occurred mainly on Indexed Finance's Discord server. Discord is a social media and instant messaging platform that serves as one of the main hubs for community discussion regarding Indexed Finance. Our Discord server can be accessed by any member of the public.

128. Recall that, as outlined above, adding a new token *from* a candidate list to an index happens automatically when a user triggers a Re-Indexing by the index controller. But adding a new token *to* the candidate list requires a governance vote by NDX tokenholders.

129. The proposed new token was SUSHI, which, as mentioned above, is the token for the Sushiswap exchange platform. SUSHI was rapidly growing in size and popularity at the time and was deemed a good fit for inclusion in the candidates list.

130. In August 2021, I officially proposed adding SUSHI to the candidate list for DEFI5 and CC10. The NDX tokenholders that voted unanimously approved the addition, and SUSHI was added to the candidate lists on August 31, 2021. The vote was held on the blockchain and so the result of the vote was visible to the public.

131. At that time, SUSHI's market capitalization was not high enough to be added from the candidate list to the index for DEFI5. However, a user could determine when SUSHI would be due to be added by monitoring its market capitalization and comparing it to the market capitalizations of the tokens in the index. Once SUSHI's market capitalization exceeded the market capitalization of at least one token in the index, the user would know that that token would be removed, and SUSHI would be added in the next Re-Indexing.

132. By October 14, the date of the Attack, SUSHI had already been added to the CC10 index by a Re-Indexing that took place shortly after the vote mentioned above. It had not yet been added to the DEFI5 index, but its market capitalization had grown such that it was due to be added as soon as the Re-Indexing function was triggered.

133. As noted above, any user can trigger a Re-Indexing one week after three Re-Weightings (which occur up to once a week). DEFI5 had a third Re-Weighting on October 7, 2021 and had been eligible for a Re-Indexing for about six hours when the Attack began.

134. The first command executed by the DEFI5 Attack Contract triggered a Re-Indexing of the DEFI5 index. The Re-Indexing added SUSHI to the index.

135. The Re-Indexing also involved setting SUSHI's Index Weight. The Square Root Market Cap Function calculated SUSHI's Index Weight as approximately 12%.

136. As explained above, once a new token is added to an index, the index controller sets a Minimum Balance and Initialization Price for the new token using the TotalPoolValue benchmark. In this case, TotalPoolValue was calculated using the UNI token to estimate the pool's NAV.

137. At this stage, TotalPoolValue was estimated fairly, resulting in a reasonable Minimum Balance for SUSHI of 11,926 SUSHI tokens, worth about $128,000 on the market.[14] In other words, the DEFI5 index pool would accept 11,926 SUSHI tokens in exchange for issuing (i.e. minting) new DEFI5 pool tokens representing 1% of the pool's NAV.

Step 2: Flash Loans

138. The Attack required a massive volume of trades to sufficiently distort the prices set by the index pool. To achieve the required volumes, the Attacker made use of flash loans, a service available in decentralized finance that provides instantaneous access to capital.

139. Flash loans permit any user to borrow extremely large quantities of tokens from a decentralized exchange. The user is not required to post any collateral. However, the borrowed tokens must be repaid (plus interest) as part of the same blockchain "transaction" in which they

---

[14] This implies a pool value of $12.8 million. As outlined above, the total value at the instant before the Attack was actually $13.4 million. The difference arises because the formula used to calculate TotalPoolValue uses time-weighted average prices (TWAPs), whereas the $13.4 million is based on daily price information quoted by Etherscan. The volatility of prices for digital assets can result in significant differences between these values.

are borrowed. If a trading strategy is unable to repay the loan, the strategy fails, and the transaction is reverted (i.e. none of the state changes of that transaction take effect).

140. The Attacker took out flash loans worth approximately $157 million[15] in the form of a basket of tokens that matched the composition of the DEFI5 index pool, i.e. approximately $48 million in UNI and a combined $109 million in AAVE, CRV, COMP, MKR, and SNX (the five non-UNI assets). The details of the assets flash loaned by the Attacker are set out in **Appendix A2**. The flash loans were routed to the DEFI5 Attack Contract.

Step 3: Use leverage to distort the Pool Price of UNI

141. Next, the Attacker purchased almost all the UNI from the DEFI5 index pool. He did this by swapping into the pool the flash-borrowed $109 million in non-UNI tokens and receiving in exchange UNI tokens from the pool.

142. This was an enormous volume of trading: the non-UNI assets that the Attacker traded into the pool were worth about eight times the pool's initial NAV of $13.4 million. As I explain in more detail below, the volume of this trade greatly distorted the Pool Price of UNI, and, in turn, the TotalPoolValue benchmark.

143. As explained above, the index pool limits the maximum volume of a single asset swap (the 50% Swap-In Limit and the 33% Swap-Out Limit). However, the code does not prohibit a user from stacking multiple swaps. There is nothing inherently improper in bypassing the trade volume limits in this way (as compared with the hack of the trade volume limit for the Initialization Trade, discussed at step 6 below). Indexed Finance's documentation recognizes that this is possible, with

[15] An additional $2 million in SUSHI was borrowed in Step 6, as discussed below.

one passage stating that the trade volume limit "only applies to an individual call [trade] to the contract and can be bypassed with multiple calls." An excerpt of this statement is attached as **Exhibit "3"**.

144. As a result, the Attacker was able to use dozens of trades to purchase 198,540.04 UNI, out of the original balance of 203,318.87 UNI, i.e. about 98% of the pool's UNI.

145. As explained above, as the balance of a given token decreases, its Pool Price increases in a non-linear way, requiring ever-increasing amounts of the other tokens to purchase that token. This occurred here, as the Attacker purchased UNI, to an extreme degree. As he purchased more and more UNI from the pool, the Pool Price of UNI increased far in excess of its market price. For the $109 million in non-UNI assets that he swapped into the pool, he received only 198,540.04 UNI (worth about $5.2 million). By the final swap of the series, the Pool Price was $22,645.08 per UNI token.[16] Market pricing data shows that UNI was trading at $26.29 per token at the time. In other words, in the final swap, the Attacker was deliberately paying over 860 times the UNI market price.

146. There is no economic justification to sell $109 million in borrowed assets to receive only $5.2 million in UNI tokens. Such a trade only makes sense as part of a broader Attack.

Step 4: Exploit the Inflated UNI Price to Manipulate the TotalPoolValue Benchmark

147. Having purchased almost all the UNI from the DEFI5 pool, the Attacker had inflated the Pool Price for UNI to over 860 times its market price.

[16] 143,052.10 SNX for 62.67 UNI, or 2,282.77 SNX per UNI. SNX was trading at $9.92 per token.

148. The Attacker then ran the UpdateMinimumBalance command on the index controller. Recall that this function causes the index controller to recalculate the Minimum Balance for a new token that is being added to the pool (in this case SUSHI).

149. The UpdateMinimumBalance function triggers a recalculation of the TotalPoolValue benchmark. As explained above, the formula used to calculate TotalPoolValue multiplies the UNI token's balance by the reciprocal of its AMM Weight to estimate the pool's NAV in terms of UNI. For example, if UNI's AMM Weight was 40%, and the balance of UNI in the pool was 200,000, the pool's NAV would be extrapolated as 500,000 UNI. The index controller then multiplies this value by the market price of UNI to obtain the TotalPoolValue. Using the previous extrapolated NAV of 500,000 UNI, if UNI had a market price of $25 per token, the TotalPoolValue would be calculated as $12,500,000.[17]

150. Critically, the TotalPoolValue benchmark uses the UNI token's *market* price, not its Pool Price. Generally, a token's Pool Price will be closely aligned with its market price, because any misalignment will create an arbitrage opportunity. In this case, the Attacker caused an instantaneous "spike" in the Pool Price of UNI. Before arbitrage traders could intervene, and while UNI's Pool Price was still wildly above its market price, he ran the UpdateMinimumBalance function.

151. The AMM Weight for UNI remained 40%, while the balance of UNI had declined by 98%. Because the formula for TotalPoolValue uses UNI's AMM Weight of 40% (not its actual weight by market value, i.e. its Pool Weight) to estimate the pool's total value in terms of UNI, and

[17] In actual fact, TotalPoolValue is quoted in ETH, not USD. I have used USD to simplify for the purposes of the example.

because the TotalPoolValue benchmark multiplies this by its market price, this created a mismatch between TotalPoolValue and the pool's actual NAV at the time the 'MinimumBalanceUpdate' function was triggered, as follows:

(a) **TotalPoolValue**: 203,319 UNI tokens (starting balance) - 198,540 (removed by Attacker) = 4,779 remaining UNI tokens * 100%/40% (reciprocal of AMM Weight) = 11,947.5 UNI (extrapolated value of pool in UNI). 11,947.5 * $26.29 (market price of UNI) = **$314.100** (i.e. TotalPoolValue estimates the pool NAV to be $314,100).

(b) **Actual DEFI5 Pool NAV**: $13.4 million (starting pool NAV) - $5.2 million (UNI swapped out)) + $109 million in flash loaned assets swapped into the pool (see step 3) = **$117.2 million**

152. In short, the formula used to extrapolate the pool's NAV from the value of a single reference token malfunctioned and caused the index controller to calculate TotalPoolValue as a quarter of 1% of the pool's actual NAV, i.e. the benchmark was off by a factor of roughly 400.

153. The UpdateMininumBalance function then updated the Minimum Balance of SUSHI tokens required to make up 1% of the pool's NAV using the wildly distorted TotalPoolValue benchmark. The Minimum Balance of SUSHI was updated from 11,926 to 299 (i.e. roughly $3,200)[18]. Recall that the Minimum Balance for a token is supposed to approximate 1% of pool NAV. But, here, the value of the Minimum Balance for SUSHI *decreased* from $128,000 to $3,200 even though the actual pool NAV had *increased* from $13.4 million to $117.2 million. Rather than

[18] $3200 is the value using Etherscan prices. 1% of $314,100 is $3,141. The discrepancy reflects a difference in the methodology used to quote a USD price (TotalPoolValue uses market price information from Uniswap).

approximating 1% of pool NAV, the updated Minimum Balance for SUSHI was 0.0025 percent – roughly 400 times too low.

154. In turn, this manipulated the Initialization Price for SUSHI. Recall that the Initialization Price is the Pool Price for a new token up to and including the Initialization Trade. The Initialization Price is supposed to represent the value in other tokens that would correspond to 1% of the pool's NAV. In the Attack, because of the artificially low Minimum Balance for SUSHI, $3,200 in SUSHI tokens could be used to mint new DEFI5 pool tokens worth 1% of the pool's actual NAV. This meant that a user could trade $3,200 of SUSHI into the pool and receive pool tokens with underlying assets worth $1,172,000. That is, the index pool was greatly overestimating the price of SUSHI relative to the other pool assets.

Step 5: Reverse the UNI Swap-Out and Mint DEFI5 Tokens

155. Having manipulated the TotalPoolValue benchmark (and thus the Initialization Price for SUSHI), the Attacker swapped all his UNI tokens back into the pool to mint new DEFI5 tokens. This included the $5.2 million in UNI that he had swapped out of the pool (step 3) plus the $48 million in UNI he had previously flash loaned (step 2). With these proceeds, he was able to mint approximately 1.4 million new DEFI5 tokens. The NAV of the new DEFI5 tokens corresponded to the value of the assets swapped into the pool minus the swap fees, i.e. $157 million less swap fees of 2% on the initial swap-in of $109 million in flash borrowed assets (step 3) and the $53.2 million in UNI (step 5), i.e. 2% of $162.2 million = $3.2 million; $157 million - $3.2 million = $153.8 million worth of new DEFI5 tokens. In other words, at this point in the transaction, the Attacker had turned $157 million in borrowed assets into $153.8 million in new DEFI5 tokens.

156. The details of this trade are set out in **Appendix A3**.

157. This minting of 1.4 million new DEFI5 tokens drastically inflated the total number of DEFI5 tokens in circulation by a factor of 10x (from 151,000 to 1.5 million). The significance of minting these DEFI5 tokens becomes apparent in step 7, below.

Hacking the Trade Volume Limit on the SUSHI Initialization Trade (Step 6)

Step 6: Contaminate the AMM With the Distorted Valuation

158. Up to this point, the Attacker had manipulated the TotalPoolValue and thereby set an artificially inflated Initialization Price for SUSHI tokens. But the Initialization Price is only used by the index pool for a specific purpose, namely for trades until the new token reaches its Minimum Balance. Recall that the Initialization Trade is the trade that brings the new token to or above its Minimum Balance. But the Initialization Trade is, by definition, a single trade. As such, it is subject to the 50% Swap-In Limit. Before a token reaches its Minimum Balance, the index controller sets the 50% Swap-In Limit by reference to the token's Minimum Balance, which corresponds to the token's Minimum Weight, i.e. 1%. In other words, the 50% Swap-In Limit restricts the Initialization Trade to a maximum of 50% of the Minimum Balance of the new token.

159. Had the Attacker stopped at this point, he could have deposited 450 SUSHI over three distinct swaps (with just under 150 SUSHI in each) to mint new DEFI5 pool tokens worth up to 1.5% of the pool's NAV.[19] However, the gains from such a trade would not have offset the losses suffered on the swap fees and the overall trading strategy would have been unprofitable.

[19] By swapping in SUSHI in three swaps: two trades to bring the balance to just below the Minimum Balance (0.99999999%), and a third trade (the Initialization Trade) to bring it to 1.49999999%.

160. The Attack succeeded because the Attacker was able to hack the trade volume limit on the Initialization Trade. This allowed him to pour an unlimited amount of SUSHI tokens into the index pool, which overwhelmed the pool and caused its pricing mechanism to go haywire.

161. The Attacker did this by performing a trade that the index pool did not expect: a gift.

162. The Attacker entered another flash loan, this time for 220,000 SUSHI tokens (roughly $2.4 million). He deposited all the flash loaned SUSHI tokens into the DEFI5 pool. This was effectively a gift of the borrowed SUSHI tokens. There was no legitimate economic justification for this gift: its purpose could only have been to further manipulate the index controller. The Attacker lost another $2.4 million on this step, bringing his cumulative losses on steps 1-6 to $5.7 million. Those losses were only offset by the subsequent profits that the Attacker was able to make by exploiting the pricing glitch he had created.

163. Immediately after gifting this SUSHI to the index pool, the Attacker triggered the Gulp function. Gulp performs internal accounting updates within the pool based on the tokens it currently holds. This forced the index pool to recognise that the amount of SUSHI it held was in excess of its Minimum Balance, thus triggering the Initialization Re-Weighting. The Gulp function is intended to be used on the rare occasion that someone accidentally sends tokens to the pool, to allow the pool to integrate those tokens into the AMM by treating the transfer as if it were a swap. The Gulp function was not intended to be used in the manner that the Attacker used it here.

164. As explained above, the Initial AMM Weight of a new token is set to equal 1% plus the percentage by which the balance of the token exceeds the Minimum Balance in the Initialization Trade. In this case, the Minimum Balance of SUSHI was 299. Adding 220,000 tokens completely

swamped the pool with SUSHI, tricking the index pool into setting a wildly inflated Initial AMM Weight for SUSHI of 87%.

165. Recall that, when SUSHI was added to the DEFI5 index, the index controller used the Square Root Market Cap Function to calculate its Index Weight as approximately 12%. The combined effect of the "gift" of SUSHI and triggering the Gulp function was to set SUSHI's Initial AMM Weight well *above* its Index Weight. This is the reverse of how things are supposed to work: the Initial AMM Weight is supposed to be lower than the Index Weight, and the index controller gradually increases the AMM Weight until it reaches Index Weight.

166. Making a gift of $2.4 million of SUSHI exploited the index pool's code in three separate ways:

(a) ***First,*** the 50% Swap-In Limit prevents a user from swapping in more than 50% of the Minimum Balance in a new token. In other words, the index pool protocol would not have allowed the Attacker to swap in more than 300*0.5 = 150 SUSHI tokens in a single swap. However, the protocol contained no rule against making a *gift* in excess of the 50% limit. Understandably, the protocol was simply not expecting a gift of $2.4 million.

(b) ***Second***, the Initialization Re-Weighting function implicitly assumes that the balance of new tokens traded in the Initialization Trade will be less than the balance that would hit the new token's Index Weight. In other words, Initial AMM Weight is not capped so as not to exceed the new token's Index Weight. If such a limit had been in effect, SUSHI's Initial AMM Weight would have been set to its Index Weight, i.e. 12%, rather than 87%. Ordinarily, the Initial AMM Weight would implicitly be limited, since the 50%

Swap-In Limit would itself prevent such a large Initialization Trade. The Attacker circumvented this implicit limit by making a gift.

(c) ***Third*,** the trade used the index pools' own security features against it. The index pool sets a 1% per 30 minutes limit so that a token's AMM Weight moves gradually from its Initial AMM Weight to its Index Weight. In this case, because the Initial AMM Weight was set so far above the Index Weight, the 1% limit actually *prevented* the pool from correcting the error in the Initial AMM Weight.

167. The distorted Initial AMM Weight meant that the index pool saw $2.4 million in SUSHI as worth 87% of the pool. That would imply a pool NAV of around $2.75 million ($2.4 million/87% = $2,758,620). But, of course, the real pool NAV was much greater than this, at around $172.8 million.[20] The net result of this trade is that SUSHI was vastly overvalued by the pool and was now freely tradable against the other assets in the pool.

168. As noted above, the index pool assigns new weights to all assets in the pool following the Initialization Trade, i.e. the Initialization Re-Weighting. Adding a new token to the pool, with its own AMM Weight, requires the AMM Weights of the other tokens to be adjusted downwards so that the sum remains 100%.

169. However, the greatly excessive Initial AMM Weight of SUSHI (87%) meant that the AMM Weights of the other tokens plummeted. For example, UNI's AMM Weight decreased from 40% to about 5% (40% of the remaining 13%).

[20] The DEFI5 pool's starting value was $13.4 million + $157 million flash loaned assets (step 2) + $2.4 million flash loaned SUSHI (step 6) = $172.8 million.

170. Since the Pool Prices of the tokens are functions of their AMM Weights, the inflated AMM Weight for SUSHI and the deflated AMM Weights for other tokens distorted the rates by which they could be exchanged for one another. Essentially, the index pool was overpricing SUSHI and underpricing all other tokens.

171. The distorted prices meant that a user could mint new DEI5 tokens using the overpriced SUSHI tokens, which would permit the user to obtain the full value of the pool's underlying assets at a small fraction of their market price.

Minting and Burning DEFI5 Pool Tokens at Distorted Prices (Steps 7-11)

172. Having successfully manipulated the TotalPoolValue benchmark and hacked the trade volume limit on the Initialization Trade, the Attacker had thrown the DEFI5 index pools' Pool Prices into chaos.

Step 7: Burn DEFI5 Tokens to Collect Underlying Assets

173. Next, the Attacker burned the 1.4 million DEFI5 tokens that he had minted using UNI (step 5) and obtained the underlying tokens. At this point, the Attacker had recovered most of the value of the borrowed tokens ($155 million of the $159 million initially borrowed). A breakdown of the tokens received by the Attacker is set out in **Appendix A4**.

174. The tokens returned to the Attacker in the burn included 197,555 tokens of SUSHI (worth approximately $2.1 million). This SUSHI became the ammunition for the next phase of the Attack.

Step 8: Use SUSHI To Mint New DEFI5 At Distorted Prices

175. The Attacker then immediately recycled these SUSHI tokens, swapping his 197,555 SUSHI tokens back into the DEFI5 pool to mint new DEFI5 tokens. Due to the 50% Swap-In

Limit, he had to use a ramping series of six trades, increasing the volume of SUSHI swapped in by 50% with each trade. In total, the Attacker swapped 197,555 SUSHI tokens (market value $2,124,567.64) and received 1,012,219.94 DEFI5 tokens. Additional details of these trades are set out in **Appendix A5**.

Step 9: Burn DEFI5 tokens and receive a disproportionate amount of underlying assets

176. At this stage, the Attacker burned all 1,012,219.94 DEFI5 tokens, obtaining underlying tokens worth roughly $16.9 million (as compared with the $2.1 million worth of SUSHI he paid for them). Additional details of the tokens received are set out in **Appendix A6**.

177. The underlying tokens received again included SUSHI tokens (189,340 tokens).

Step 10: Rinse and repeat

178. The Attacker then repeated steps 8-9 by recycling the SUSHI he obtained by burning DEFI5 tokens at step 9. The Attacker used his 189,340 SUSHI tokens (roughly $2.0 million) to mint new DEFI5, which he immediately burned for tokens worth roughly $3.9 million.

179. Additional details regarding these trades are set out in **Appendix A7** and **Appendix A8**.

Step 11: Cash Out

180. At this point, the Attacker cashed out. He first used the proceeds of his trades to repay the $159 million in flash-loaned tokens plus fees.

181. The rest of the tokens from the trades were then transferred to the Attacker's Wallet. As of the time of the Attack, the total net assets received by the Attacker had a value of roughly $11.9 million (89% of the pool's pre-Attack NAV of $13.4 million). A breakdown of the tokens

routed to the Attacker's Wallet is set out in **Appendix A9**. The total pool NAV of the DEFI5 Pool after the Attack was less than $1 million, as set out in **Appendix A10**. Comparing Appendix A1 and Appendix A10 gives a "before" and "after" snapshot of total pool NAV, showing that the Attack reduced pool NAV by $12.5 million. Note that this means the total value obtained by the Attacker ($11.9 million) was less than the total loss suffered by the DEFI5 pool ($12.5 million). The difference is due to significant transaction costs the Attacker was required to pay, namely re-paying the flash loans with interest.

182. Post-Attack, the balances of all pool tokens had decreased, except that there remained an additional $430,000 in SUSHI tokens (left behind by the Attacker). Excluding the value of these SUSHI tokens, the loss to the DEFI5 pool would have been increased by $430,000, so roughly $12.9 million. In other words, on a net basis the effect of the Attack was that the Attacker was able to trade $430,000 of SUSHI tokens for $12.9 million worth of tokens held by the DEFI5 pool.

183. Those tokens remain in that Attacker's Wallet to this day. Due to the transparent nature of the blockchain, anyone with an internet connection can enter the public address for the Attacker's Wallet and see the tokens.[21] A print-out of this web address is attached as **Exhibit "4"**.

Summary

Step	Description	Ref	Transaction Log Entry
	Pre-Attack Balance ("Before")	A1	

[21] https://etherscan.io/address/0xba5ed1488be60ba2facc6b66c6d6f0befba22ebe.

Manipulate the TotalPoolValue Benchmark			
1	Trigger re-indexing to add SUSHI to DEFI5 index		1--2
2	Add leverage by borrowing $157 million in flash loans	A2	3--8
3	Purchase 98% of the UNI in DEFI5 using $109 million of borrowed tokens, causing the AMM to assign a massively inflated Pool Price to UNI		9--76
4	Exploit the inflated UNI Pool Price by causing the index controller to set a value for the TotalPoolValue benchmark far below the pool's NAV, and thus an inflated Initialization Price for SUSHI		77
5	Use $53 million in UNI ($48 million flash loaned in step 2 + $5.2 million swapped out in step 3) to mint 1.4 million DEFI5 tokens	A3	78--122
Hack the Trade Volume Limit on the Initialization Trade			
6	Circumvent the trade volume limit on the Initialization Trade by making a "gift" of $2.4 million of SUSHI and executing the "Gulp" function, causing the price glitch for the Initialization Price of SUSHI to affect the prices of all other assets		123--126
Minting and Burning DEFI5 Tokens at Deflated Minting Price			
7	Burn 1.4 million of DEFI5 minted in Step 5 for $155 million, including $2.1 million of SUSHI	A4	127--136
8	Use $2.1 million of SUSHI to mint more DEFI5	A5	137--154
9	Burn DEFI5 for $16.9 million, including $2 million of SUSHI	A6	155--164
10	Repeat steps 8-9 with $2.0 million of SUSHI, burning for $3.9 million	A7/A8	166--189
11	Cash out net gain of $12 million	A9	199--207
	Post-Attack Balance ("After")	A10	

The CC10 Phase

184. The format of the CC10 Phase of the Attack followed the same strategy as the DEFI5 Phase. The individual steps were substantially similar. Step 1 was not necessary because SUSHI had already been added to the CC10 index by a previous Re-Indexing, though SUSHI had not yet reached its Minimum Balance (and so had not been Initialized). For the CC10 pool, LINK (rather than UNI) was the reference token used to calculate the TotalPoolValue benchmark.

185. The NAV of the CC10 index pool immediately before the Attack was approximately $4.1 million. Immediately after the Attack, the CC10 pool's value was about $100,000, i.e. about 98% of the pool's value was lost. The net assets routed to the Attacker's Wallet (after repaying flash loans with interest and transaction fees) was $3.9 million. Post-Attack, the balances of all pool tokens had decreased, except that there remained an additional $26,000 in SUSHI tokens. In other words, on a net basis the Attacker effectively traded $26,000 of SUSHI tokens for $4.0 million worth of tokens held by the CC10 pool.

186. Taken together, the combined impact of the DEFI5 Phase and the CC10 Phase a direct loss of $16.5 million in value, of which $15.8 million remained in the Attacker's Wallet at the conclusion of the Attack. On a net basis, the Attacker had effectively traded $456,000 of SUSHI tokens for $16.9 million of other tokens held by the DEFI5 and CC10 pools.

187. As with the DEFI5 Phase, there is an Etherscan webpage for the CC10 Phase that lists all of the trades and commands involved in the CC10 Phase.[22] I have compiled a series of Appendices (Appendix B1, Appendix B2, etc.) that summarize the key events in the CC10 Phase. The

[22] https://etherscan.io/tx/0xbde4521c5ac08d0033019993b0e7e1d29b1457e80e7743d318a3c27649ca4417

Appendices are attached as **Exhibit "5"**. I have compiled a transaction log for the CC10 Phase of the Attack (the **"CC10 Transaction Log"**). The CC10 Transaction Log is attached as **Exhibit "6"**.

188. The CC10 Phase is summarized below:

Summary

Step	Description	Ref	Transaction Log Entry
	Pre-Attack Balance ("Before")	B1	
Manipulate the TotalPoolValue Benchmark			
1	Add leverage by borrowing $37 million in flash loans	B2	1--10
2	Purchase 99% of the LINK in CC10 using $29 million ofborrowed tokens, causing the AMM to assign a massively inflated Pool Price to LINK		11--334
3	Exploit the inflated LINK Pool Price by causing the index controller to set a value for the TotalPoolValue benchmark far below the pool's NAV, and thus an inflated Initialization Price for SUSHI		335
4	Use $9.3 million in LINK ($8.4 million flash loaned in step 1 + $0.9 million swapped out in step 3) to mint 521,000 CC10 tokens	B3	336--407
Hack the Trade Volume Limit on the Initialization Trade			
5	Circumvent the trade volume limit on the Initialization Trade by making a "gift" of $172,000 of SUSHI and executing the "Gulp" function, causing the price glitch for the Initialization Price of SUSHI to affect the prices of all other assets		408--411
Minting and Burning CC10 Tokens at Deflated Minting Price			
6	Burn 521,000 CC10 minted in Step 4 for $36 million, including $175,000 of SUSHI	B4	412--425
7	Use $175,000 of SUSHI to mint more CC10	B5	426--443

8	Burn CC10 for $4.3 million, including $173,000 of SUSHI	B6	444--457
9	Repeat steps 7-8 with $173,000 of SUSHI, burning for $677,000	B7/B8	458--489
10	Cash out net gain of $3.8 million	B9	504--516
	Post-Attack Balance (“After”)	B10	

Collateral Damage to Indirect Tokenholders

189. Just as Indexed Finance creates index pools that hold underlying tokens, other pools can own the index pool tokens themselves (DEFI5 and CC10) as underlying assets. Accordingly, some users hold their tokens of DEFI5 and CC10 through these other pools. These fall into two categories:

(a) **The “Future of Finance Fund” (FFF):** another index pool operated by Indexed Finance as a “fund of funds”, with weights for DEFI5 and CC10 of 25% and 12%, respectively.

(b) **Liquidity pools:** there were a number of liquidity pools on platforms such as Uniswap to promote liquidity of the DEFI5 and CC10 tokens. For example, there was a Uniswap liquidity pool token for DEFI5 that was equally weighted between DEFI5 and ETH (DEFI5:ETH LP) and a similar token for CC10 (CC10:ETH LP).

190. These pools operate in a manner similar to the index pools described above. They use AMM models to set internal prices for each asset in terms of the other. Tokenholders have a proportionate claim on the underlying pool tokens.

191. The holders of these tokens suffered losses in two stages:

(a) In the Attack itself, a holder of a pool containing 50% DEFI saw 46.5% (i.e. 50% of 93%) of the value of their pool token evaporate.

(b) In the immediate aftermath of the Attack, the market price of the DEFI5 and CC10 tokens instantaneously dropped, because they contained far fewer assets. However, for tokens of DEFI5 and CC10 held in liquidity pools, the AMM for those liquidity pools continued to assign a price for those tokens based on its own internal pricing model (i.e. these pools have their own AMMs). This created an enormous divergence between the Pool Price (which remained at pre-Attack levels) and the market price (which had collapsed). Arbitrage traders immediately went into action and minted new DEFI5 tokens (very cheaply) which they then sold into the liquidity pools that had not yet priced in the change. As a result these pools lost almost all of their value.

192. We are continuing to investigate the full extent of the damage caused to liquidity pool tokenholders. However, we estimate that this loss is likely more than $10 million. I learned of the Attack shortly after it happened, when another Indexed Finance community member messaged me with a screenshot of some of the trades. The Attack came as a total shock to me and the entire Indexed Finance community. In the immediate aftermath of the Attack, Dillon and I worked with Indexed Finance stakeholders to reconstruct what had happened and to try to identify who was responsible. Within about eight hours of the Attack, Dillon had identified the vulnerability in the re-indexing and re-weighting functions that had been exploited by the Attacker. We posted a "post-mortem" online to explain to the community what had happened. I have attached a copy of the post-mortem as **Exhibit "7"**.

193. The more difficult task was to identify the Attacker.

PART IV – IDENTITY OF THE ATTACKER

Post-Attack Investigation

194. As explained above, transactions on the Ethereum blockchain are publicly visible. Using publicly available services such as Etherscan, it is possible to trace tokens as they move between public addresses on the blockchain. However, there is no way to ascertain the identity of an account holder from their public address. Unlike a traditional financial institution, there are no know-your-client (KYC) obligations on the blockchain and no central server to maintain such records.[23] The blockchain does not record the internet protocol (IP) address[24] of its users and so there is no way to determine the IP address from which the Attack was launched.

195. As a result, it can be extremely difficult to tie a blockchain user to a human being in the real world. For this reason, those responsible for many crypto hacks and frauds are never found.

196. In this case, however, the Attacker left enough traceable clues that we have a high level of confidence that Andean is the Attacker.

Suspicious Pre-Attack Interactions with "UmbralUpsilon" aka "BogHolder"

197. The night of the Attack, I recalled that, between September 11, 2021, and October 12, 2021, Dillon and I had had a series of conversations on Discord with a user with the Discord username "UmbralUpsilon." That user had contacted Dillon and I, asking us questions that over the course

---

[23] There are some DeFi institutions with KYC requirements, but the attacker's account is not associated with any of those platforms.

[24] An IP address is a unique address that identifies a computer or a local network.

of several weeks evolved into discussions about the re-indexing and re-weighting functions in the index pools. This was the exact mechanism that the Attacker later exploited.

198. I opened my Discord account to review our chat history and discovered that "UmbralUpsilon" had changed his Discord username to "BogHolder#1688" ("**BogHolder**") and deleted his half of our conversation.[25] I notified Dillon, who checked his own chat history and found that "UmbralUpsilon" had deleted his half of their conversation as well. While Discord does not expressly show when the chats were deleted, my most recent exchange with "UmbralUpsilon" had been on October 12, meaning that the chats had been deleted at most two days prior to the Attack, or in the hours immediately afterwards.

199. "UmbralUpsilon" had expressed interest in providing technological support to the index pools.[26] He had wanted to create an "arbitrage bot" for the pools. An arbitrage bot is a computer script that automates the arbitrage performed on the index pools. As explained above, arbitrage is essential to the proper functioning of the AMM.[27]

200. Since an arbitrage bot would add value to the index pools, Dillon had offered "UmbralUpsilon" $4,000 worth of tokens to develop the bot, with half up front as an incentive. He had agreed and had told Dillon to transfer the tokens to the Ethereum address 0xb7e77cdAf7EBF76dB72571f2D6E43aA5e84a5E64 (the "**E64 Address**"). As far as I know,

[25] Discord allows either party to a chat to delete the messages they authored, not just from their own device but from the Discord server, thus removing the ability of other participants to view those messages.

[26] This is not unusual. One of the benefits of DeFi protocols running on underlying open-source code is that anyone can view it and propose changes to it.

[27] As explained above, arbitrage imposes price discipline on the internal market created within the index pool and ensures that the prices of assets within an index track their market price. Automating this function through a bot would add value to the pools by making the arbitrage process more efficient and reliable, which would ultimately reduce tracking error.

the only people who knew this address were myself, Dillon, and "UmbralUpsilon." As I explain later, after the Attack, Andean's personal email address, [redacted] gave this same address as a destination for payment, which suggested that he was "UmbralUpsilon".

201. In the Discord chats, we had answered UmbralUpsilon's questions in the spirit of community-building and fostering interest in the Indexed Finance platform. Since every component of the index pools is open source, no aspect of the code is confidential.

202. Because "UmbralUpsilon" aka "BogHolder" had deleted his half of our conversations, Dillon and I have lost access to the text of his specific inquiries. However, each of us still has our half of the conversation, i.e., our responses to his questions. I have attached a print-out of my responses to "UmbralUpsilon" aka "BogHolder" as **Exhibit "8"**. I have attached a print-out of Dillon's responses as **Exhibit "9"**.

Connecting "BogHolder" to the Attacker's Wallet

The Attacker's Wallet

203. We began to look at whether the "BogHolder" account was connected to the Attacker's Wallet, the address that had financed the Attack and still held the proceeds. To determine if "BogHolder" was the Attacker, we had to work backwards.

204. Although there is no way to confirm exactly when the Attacker's Wallet was created, it had no transaction history until the morning of the Attack on October 14, 2021, when it became active at around 4:27 am UTC.

205. There was only one clue linking the Attacker's Wallet to any other account. When the Attack began, there was a balance of roughly 3 ETH (roughly $11,000) in the Attacker's Wallet. These ETH tokens were used to pay transaction costs (called "gas') for the transactions on the blockchain that made up the Attack.[28]

Attacker Attempts to Conceals Source of Tokens in Attacker's Wallet

206. The ETH used to fund the Attack entered the Attacker's Wallet in the hours leading up to the Attack in three separate deposits, each of 1 ETH. Each deposit originated from an account associated with "Tornado Cash".

207. Tornado Cash is a "privacy mixer", which is a service designed to disguise the movement of tokens through the Ethereum blockchain. While blockchain account holders are anonymous, all the transactions associated with any given account are public. This creates a digital "paper trail" that can reveal information about an account holder's identity. A user can create a new account without any transaction history but would still have to fund the new account. If they simply transferred tokens from their original account to the new account, the blockchain would record the transfer and the new account could easily be traced back to the original account.

208. A privacy mixer, such as Tornado Cash, breaks the link between the originating account address and the recipient account address, making it difficult for others to track the user's

[28] To initiate a transaction on the blockchain, a user must pay fees ("gas") to cover the significant costs associated with validating the transaction. The "gas" required to pay for transactions on the Ethereum blockchain is "ether" (ETH), which, as noted above, is the native token of the Ethereum blockchain. Although the Attacker was able to borrow all the assets that he traded in the Attack, he still needed to pay for the transactions with ETH. Because of the sophistication of the Attack, it required a significant amount of processing power, and therefore a significant amount of ETH.

transactions. A user deposits tokens into Tornado Cash's shared pool of mixed ETH. The user then provides a secret direction to Tornado Cash about where to send the same amount of ETH.

209. The tokens received by the Attacker's Wallet must have been deposited into Tornado Cash earlier. We therefore tried to find corresponding deposits to Tornado Cash.

"BogHolder" Linked to Tornado Cash Deposits

210. We posted an update to the Attack post-mortem on October 15, 2021. We included our suspicions about "BogHolder" in that post. I have attached a copy of this updated post as **Exhibit "10"**.

211. A few hours later, we received a tip from a Discord user, "hickuphh3". He told us that "BogHolder" was active on Code Arena,[29] which is a "white-hat" or "ethical security hacker" community of auditors. Code Arena runs competitions where wardens (participants) search for weaknesses in smart contracts for decentralized protocols. "hickuphh3" told us that the Discord user "BogHolder" had recently won rewards in two Code Arena competitions — participating in them under the warden name "tensors" — and that those rewards had been paid to the address 0x3c86b2b86f0a4b180802026cb1d0d73f80200ab3 (the "**AB3 Address**"). The tipster further noted that the AB3 Address had made deposits to Tornado Cash shortly before the Attack. I have attached a copy of the message from the Discord user "hickuphh3" as **Exhibit "11"**. We set about trying to confirm this information.

212. First, using Etherscan, we confirmed that the AB3 Address had made four separate deposits in the amount of 1 ETH each to Tornado Cash in the hours leading up to the Attack. The

[29] Code Arena is sometimes written as "Code423n4", or "C4" for short.

times of the deposits corresponded roughly with the times of the deposits from Tornado Cash to the Attacker's Wallet. Each transaction occurred on October 14, 2021. The timing of the deposits and withdrawals into and out of Tornado Cash was as follows (all times in UTC):

AB3 Address → Tornado Cash	**Tornado Cash → Attacker's Wallet**
02:13:54 am	06:02:52 am
08:42:09 am	02:56:28 pm
01:40:10 pm	04:42:06 pm
05:58:46 pm	n/a

213. I have attached a copy of a transaction record showing the four deposits of 1 ETH into and three withdrawals of 1 ETH out of Tornado Cash as **Exhibit "12"**.

214. We reviewed the transaction data for all deposits to Tornado Cash in the 24 hours prior to the Attack. Only four users had made at least three deposits of 1 ETH each. Of these four, only two had made deposits within the time windows corresponding to the withdrawals from Tornado Cash to the Attacker's Wallet.

215. If the Attacker had deposited tokens into Tornado Cash within 24 hours of the Attack using a single account, then the AB3 Address would be one of only two accounts that could have funded the Attacker's Wallet. The other candidate's address deposited 7 ETH into Tornado Cash in that time window. Although neither account is a perfect match to the 3 ETH received by the Attacker's Wallet, the AB3 Address is a closer match.

216. While I consider these to be reasonable assumptions (that the Attacker used a single account to make deposits within 24 hours of the Attack), I acknowledge that there are other possibilities. It is possible that the Tornado Cash deposits could have originated from a source

other than the AB3 Address. As well as the four "candidates" above, there were another 30 accounts that had made at least three deposits of 1 ETH in the seven days prior to the Attack. It is also possible that a user could have made deposits into Tornado Cash from multiple accounts. Still, based on the circumstances surrounding the Tornado Cash deposits, we were confident that the ETH used to fund the Attack came from the AB3 Address.

217. Next, we tried to confirm the link between "BogHolder" and the AB3 Address. Using Etherscan, we confirmed that the AB3 Address had in fact received rewards from Code Arena. When Code Arena pays out its competitors, it uses something called a "multisig wallet", which is a wallet that can only transfer tokens when multiple pre-assigned signatories provide confirmation. The multisig wallet address used by Code Arena to pay out its competitors is 0xc2bc2f890067c511215f9463a064221577a53e10 (the "**Code Arena Address**"). I have attached a copy of the Code Arena page that provides the multisig Code Arena Address to its contestants as **Exhibit "13"**.

218. Using Etherscan, we saw that the AB3 Address had received tokens from the Code Arena Address on several occasions, which confirmed the tip we had received from "hickuphh3" that the AB3 Address belonged to someone who had won rewards in Code Arena competitions. I have attached a copy of the Etherscan results, showing the payments from the Code Arena Address to the AB3 Address, as **Exhibit "14"**.

219. To confirm the username associated with these payments, we contacted Code Arena and connected with an organizer whose username is "sockdrawermoney". "sockdrawermoney" later identified himself as Adam Avenir, of Richland, Washington. I understand that Adam is swearing his own affidavit in support of this motion.

220. Adam confirmed that there was a Code Arena warden named “tensors” who was associated with the Discord user “BogHolder”, and whose rewards from Code Arena competitions had been sent to the AB3 Address. Later, we learned from Adam that the Code Arena warden “tensors” also previously went by the Discord username “UmbralUpsilon”. I understand that Adam will be swearing an affidavit in this proceeding explaining the relation between “UmbralUpsilon”, “tensors” and “BogHolder”.

221. We independently confirmed that the warden “tensors” was the same individual as the Discord user “BogHolder”. On Code Arena, users who participate in competitions as wardens select a handle by which they are known. A warden with the handle “tensors” had participated in a competition in August 2021, in which he had placed fourth and had won an award of about $8,000 in tokens. There were two different versions of the Code Arena announcement listing the winners of the competition: the version on the Code Arena website listed users by their warden handle, while the version in the Code Arena Discord chat listed users by their Discord username. The fourth-place winner’s Discord username that was tagged on that list was “BogHolder#1688”, the same Discord user account we suspected of involvement (rather than someone else using the pseudonym “BogHolder”). This version in the Code Arena Discord chat was provided to us by “hickuphh3”. I understand from speaking to Adam that the Discord list with the results no longer displays “BogHolder” as the fourth-place winner because the associated Discord account has since been deleted. The list now displays “Deleted User” as the fourth-place winner. However, we were able to screenshot the original message from “hickuphh3” listing “BogHolder” before anything

was deleted.[30] I have attached a copy of both versions of the list of award winners from the August 2021 Code Arena competition as **Exhibit "15"**.

Identifying "BogHolder"

222. At this point in our investigation, we had connected "BogHolder" to the AB3 Address, and the AB3 Address to the Attacker's Wallet. Next, we tried to determine the identity and whereabouts of "BogHolder".

223. "hickuphh3" pointed out that the Code Arena warden "tensors" aka "BogHolder" had registered for the Code Arena competitions using a GitHub account with the username "mtheorylord1." GitHub is an online collaboration platform for software developers. We were able to confirm this because, when a GitHub user wants to be approved as a warden in the Code Arena competitions, they must add a profile to the Code Arena GitHub "repository"[31] for wardens. That repository can be viewed by anyone. The repository showed that the Code Arena warden with the handle "tensors" had registered with the "mtheorylord1" GitHub account. I have attached a copy of this webpage as **Exhibit "16"**.

---

[30] If the username associated with a Discord account is changed after a post is made that "tags" them in it, that post will be updated to reflect the new username: i.e. if six months ago you were "tagged" in a Discord post under the name "xyz" and subsequently changed your name to "abc", that post would retroactively update to refer to you as "abc".

As a result, the fact that Discord automatically updated the Code Arena post which – by the time it was shown to us - stated that "BogHolder" had won a prize (where the name 'tensors' was shown on the *website* version of the post) allowed us to confirm that the two usernames referred to the same person. Code Arena would not 'tag' someone that had not won a prize, and if that user was not on Discord or was otherwise unknown to them, it is likely that they would have simply written the warden name, rather than 'tagging' a Discord user.

[31] A "repository" is a location on GitHub's server where users can store all their files and their files' revision histories and share those files with other users.

224. Although the GitHub account "mtheorylord1" did not have any other notable activity, a broader search of GitHub revealed an almost identical username, "mtheorylord", which had been active on GitHub in 2016.

225. By using GitHub's version control software, we cloned (copied) the only repository that "mtheorylord" created to a local computer drive. GitHub has this function to allow users to collaborate on projects. By doing this, and inspecting the only update that he had made, we could see that the email address associated with the account was [redacted]. [redacted]. I have attached a copy of this GitHub page showing the data collected from copying "mtheorylord"'s repository as **Exhibit "17"**.

226. A more general internet search of the username "mtheorylord" revealed a Wikipedia account with that username. In 2016, that Wikipedia account made an edit to the Wikipedia page for "Reach for the Top", a Canadian academic quiz competition for high school students. In the edit, "mtheorylord" added "Andean Medjedovic, notable mathematician" to the list of gameshow alumni.[32] "mtheorylord" also added the name of a school, "Hamilton-Wentworth district, Westmount Secondary School, Hamilton, Ontario" to the list of "National Champions" for the year 2015-2016. A screenshot of the record of these edits to the Wikipedia page is attached as **Exhibit "18"**. This, combined with the email address in the GitHub repository, suggested that

[32] We were able to see this because Wikipedia is a wiki, meaning that anyone can edit any page on the website to add information. When edits are made to a Wikipedia page, they are time stamped and associated with a user. Anyone can then see the users who made edits to the page and the time the edits were made by clicking on the "history" tab, which is at the top of every Wikipedia page.

"mtheorylord" was someone named Andean Medjedovic, who attended high school in Hamilton, Ontario in 2015-2016.

227. The Wikipedia account for "mtheorylord" was deleted at some point after November 3, 2021. This has removed the user page for the account, but all historical edits that "mtheorylord" made to various Wikipedia pages have remained intact.

228. A Google search of the name "Andean Medjedovic" revealed a personal website (https://nontrivial.xyz). This website was last "cached" (stored) by Google on 03:18pm (UTC) on October 14, 2021. By the time we searched for the website after the Attack, it had been deleted. This suggested that Andean's personal website was taken down immediately prior to or immediately after the Attack. I have attached a copy of the time and date of Google's cache of the website as **Exhibit "19"**.

229. While the website was taken down, I was able to view the personal website because Google had cached it and the cache was still publicly accessible. On the website, Andean described himself as a Master's student in pure mathematics at the University of Waterloo, with an interest in "cryptocurrency and other decentralized open-source software." I have attached a print-out of the cached webpage as **Exhibit "20"**.

230. The cache of Andean's personal website included personal contact information for him, including a personal email address: [redacted]

231. Sometime after the Attack, the website was put back up, with the information about cryptocurrency removed. The website also contained a resume, whose metadata indicates was created in May 2021, that indicated that Andean was enrolled in a Master's program at the

University of Waterloo for the years 2020-2021. The resume also listed Andean's interests as "cryptocurrency and trading" and indicated that he was born on November 28, 2002, meaning he was 18 years old at the time of the Attack and recently turned 19 (a point I return to below). I have attached a print-out of the post-Attack website as **Exhibit "21"**.

Additional Connections Between Andean and "BogHolder"

232. We then performed a reverse IP address search on Andean's personal website, nontrivial.xyz. A reverse IP address search is a tool that looks up information associated with a given IP address. The reverse IP address search of Andean's personal website showed that another website was also hosted by that same IP address: https://urbitstar.xyz. That website had been deleted, but the name indicated to us that Andean might have had an interest in a platform called "Urbit." I have attached a print-out of the reverse IP address search as **Exhibit "22"**.

233. Urbit is a decentralized personal server platform or a "peer-to-peer network" that allows each individual user to buy and own a "planet" on the Urbit network. It is described on the website https://urbit.org. Purchasing a "planet" is the equivalent of purchasing a permanent identity or, in other words, a static individualized IP address that allows users to store and run whatever they want on it.

234. By searching through the Urbit Discord chat (dedicated to discussing the Urbit platform), we discovered that the user "tensors" aka "BogHolder" is listed as "~libmud-bonted" (the name of an Urbit planet). I have attached a copy of the Urbit Discord chat as **Exhibit "23"**.

235. By using Etherscan, we determined that the "~libmud-bonted" planet is linked to the AB3 Address. Specifically:

(a) We traced the “~libmud-bonted” planet and saw that it was owned by the Ethereum address 0xFC99e43b8D4aA2E87726c10f19785616907e5FC7 (the “**FC7 Address**”).

(b) We investigated the FC7 Address’s history and saw that the “~libmud-bonted” planet was transferred to it on June 13, 2020, by the Ethereum address 0x8421Ee8986a6517196B1F9521D117f9565c068e4 (the “**8E4 Address**”).

(c) When we looked at the transaction history associated with the 8E4 Address, we saw that, on December 27, 2020, it had transferred tokens to the Ethereum Address 0x7bE53cAC08462853476E26Cc242f502293E52e97 (the “**E97 Address**”).

(d) We looked at the transaction history associated with the E97 Address and saw that, on January 10, 2021, it had transferred funds to the AB3 Address.

I have attached a copy of the Etherscan results linking “~libmud-bonted" to the AB3 Address as **Exhibit “24”**.

Direct Communications with Andean After the Attack

236. Having traced the Attack back to the various pseudonyms described, and having traced some of those pseudonyms back to Andean, one of Indexed Finance’s co-founders, pseudonym “PR0”, sent an email to the address in the cached version of Andean’s website, [redacted] PR0 offered Andean a $50,000 payment to return the tokens and stated that he would do his best to get the Indexed team not to press criminal charges. Neither Dillon nor I saw the email before PR0 sent it to Andean. PR0 sent Dillon and I the native .eml file of his email exchange, whose metadata confirms that the response was sent from

[redacted] I have attached a copy of PR0's email to Andean, and Andean's reply, as **Exhibit "25"**.

237. Less than one hour later, Andean agreed to the terms set out in PR0's email and asked PR0 to send the money. He did not deny responsibility for the Attack and directed that the $50,000 payment to the E64 Address, the same address to which "UmbralUpsilon" had told Dillon to send money for the arbitrage bot services. Dillon has informed me that he had never shared the message in which "BogHolder" requested payment for the arbitrage bot to be paid to the E64 Address with anyone other than me (in the context of our investigation), prior to PR0 receiving the email above. I had also never shared this information with anyone before that date.

238. Andean never returned the tokens, and so PR0 did not transfer the $50,000 bounty to the E64 Address.

239. On October 16, 2021, shortly after PR0's email exchange with Andean, Dillon attempted to call Andean to discuss the Attack. Andean did not pick up the call and Dillon has informed me that he left a voicemail asking Andean to call him back. Thereafter, Dillon exchanged a few text messages with Andean in which he mentioned that he saw that Andean had put his personal website back up on the Internet, which included a copy of his resume with his age. Dillon notified Andean that our lawyer would be contacting Andean's university and local law enforcement the next morning. Andean responded that the website was out of date, as it did not have information about his Masters' degree uploaded. He then wrote "[b]est of luck." A copy of this text message exchange is attached as **Exhibit "26"**.

ZetaZeroes and the Ultimatum

240. On October 15, 2021, we received a tip from a white-hat security researcher who was following the developments of the Attack. The researcher told us that, immediately before the Attack, a Twitter account with the name @ZetaZeroes had posted the address of the Attacker's Wallet on a Gitter chat called "Kovan Testnet/faucet".

241. Gitter is an online chat and networking platform that is used in the DeFi world. The Gitter chat thread called "Kovan Testnet/faucet" is about the Kovan faucet, which is a service that distributes free ETH on the Kovan test network to users for performing small tasks. Users go on the Gitter chat to post their wallet addresses to request ETH from this faucet.

242. We were able to confirm this tip. Since the "Kovan Testnet/faucet" chat is public, we saw that, on October 14, 2021 (the day of the Attack), at 05:24am, the Twitter account @ZetaZeroes had posted the address of the Attacker's Wallet to request free ETH from the Kovan faucet. I have attached as **Exhibit "27"** a copy of the Kovan Testnet/faucet Gitter chat showing @ZetaZeroes posting the Attacker's Wallet.

243. In the Attack, thousands of tokenholders all over the world had collectively lost millions of dollars. We felt an obligation to them to be transparent about our efforts to learn who was behind the Attack.

244. We believed that the best way to recover the funds was to offer a "white-hat bounty" — a consensual payment for the return of the funds that would allow Andean to characterize the Attack, retrospectively, as an identification of a way in which Indexed's system could be exploited.

245. On October 15, 2021, around 06:58am (UTC), I sent a message to the Twitter account @ZetaZeroes on Gitter, extending to him the white-hat bounty offer. I did not get a response. I have attached a copy of my Gitter message to @ZetaZeroes as **Exhibit "28"**.

246. Later that day, around 04:38pm (UTC), I posted an update on Twitter first identifying "BogHolder" as a suspect and explaining that we extended an offer to the Attacker that he could keep 10% of the assets if he returned the remaining 90%. I have attached a copy of the first update as **Exhibit "29"**.

247. On October 16, 2021, around 05:34am (UTC), I posted another update stating that we had connected the Attacker to the "tensors" Code Arena warden identity, and that the 10% white-hat bounty was still available, but placed a deadline of 17:00 UTC on October 17, 2021, for funds to be returned, failing which we would report the incident to law enforcement. I have attached a copy of this update as **Exhibit "30"**.

248. Later that day, around 01:54pm (UTC) when we were confident that Andean was the Attacker, and having had no word from him, we posted another update, stating that the Attacker had been identified by name and profession, and issuing an ultimatum that he was now expected to return all funds by midnight Eastern Time on October 17, 2021, failing which we would release what we had discovered and report him to law enforcement. I have attached a copy of this posting as **Exhibit "31"**.

249. Shortly after posting the final update, Dillon tweeted that he knew the identity of the Attacker. I have attached a copy of Dillon's tweets as **Exhibit "32"**.

250. We did not know Andean's age at the time. Because we knew he was a Master's student, we believed that he was older than he is. Before we learned Andean's true age, Dillon posted a tweet in which he stated Andean's first name and university. He did so to try to contact Andean in order to discuss returning the assets. Later, when we learned Andean's age, Dillon deleted the tweet. Since then, Dillon has posted two tweets imploring his Twitter followers – and the wider public - not to harass Andean or his family. I have attached a copy of Dillon's latter two tweets as **Exhibit "33"**.

251. Twenty minutes before the ultimatum deadline, Andean's personal website was put back online with the references to cryptocurrency stripped out. This is when we learned of Andean's true age, because the website contained a resume which, as noted at para. 229 of this Affidavit, stated the owner of the website's date of birth is 28 November, 2002, indicating that at the time he was 18 years old at the time of the Attack. I have attached a copy of his resume as **Exhibit "34"**.

252. Given Andean's age, we put on hold our plan to report him to law enforcement if he failed to return the assets.

253. On October 19, 2021, around 04:48pm (UTC), Dillon released a third update on Twitter, with all of the details connecting Andean to the Attack, without explicitly naming him. Dillon also redacted some of the information, like the personal email address [redacted] which we believed to belong to Andean. He did, however, include mention of "mtheorylord"'s connection with the email address [redacted] I have attached a copy of this update as **Exhibit "35".**

The Twitter Account @ZetaZeroes Confesses to the Attack

254. As explained above, on October 15, 2021, we learned that a Twitter account named @ZetaZeroes had posted the address of the Attacker's Wallet on the "Kovan Testnet/faucet" Gitter chat.

255. The @ZetaZeroes Twitter account did not post any tweets until October 16, 2021, when Dillon tweeted that he knew the identity of the Attacker.

256. On October 16, 2021, at 10:11pm (ET) (October 17, 2021, at 3:11am (UTC)), @ZetaZeroes began tweeting about how "doxxing"[33] teenagers is an "incredibly gauche move", no matter how many university degrees a teenager has in "advanced analytic arbitrage actions."

257. In another tweet on October 16, 2021, at 10:16pm (ET) (October 17, 2021, at 3:16am *(UTC)), @ZetaZeroes admitted to being behind the Attack and receiving $16 million worth of tokens. He wrote:

> There were frontrunners that copied my FFF pool arbitrage taking $5M from what I feel like is rightfully my balance. Should've been my $21M arbitrage instead of $16M. Such is crypto. Don't Kvetch about it too much. Git gud at the game or go home."

258. On October 21, 2021, @ZetaZeroes published another tweet thanking his supporters and asking them to recommend him the "most elite crypto lawyers" to help him, saying he "will need an entire team".

259. I have attached a copy of @ZetaZeroes' tweets as **Exhibit "36"**.[34]

[33] "Doxxing" is the act of revealing private information about an individual on the Internet.
[34] The profile may be found at https://twitter.com/zetazeroes?lang=en

The Twitter Account @ZetaZeroes is Linked to Andean

260. In the tweet asking for support, @ZetaZeroes stated that one way people could contact him is by using "my doxxed email", which we interpreted as a reference to the email address [redacted] In other words, this comment seemed to tacitly admit that Andean Medjedovic was @ZetaZeroes.

261. I note that the name @ZetaZeroes corresponds to one of Andean's research interests. In Andean's Masters' thesis, he discusses the Riemann zeta function. I have attached a copy of the relevant excerpts from Andean's Masters' thesis paper as **Exhibit "37"**. The Wikipedia page for the Riemann hypothesis states that it is a "conjecture that the Riemann **zeta** function has its **zeros** only at the negative even integers and complex numbers with real part ½" that "[m]any consider … to be the most important unresolved problem in pure mathematics" (emphasis added). I have attached a copy of this page as **Exhibit "38"**.

262. As well, the name @ZetaZeroes suggests another connection between that account, Andean, and the username "mtheorylord." We found that a StackExchange user with the username "mtheorylord" (the same username as the GitHub and Wikipedia accounts described at paras. 222-227) had made a post approximately five years ago on a StackExchange questions board entitled "Testing Zeros Of The Riemann Hypothesis". I have attached a copy of this StackExchange post as **Exhibit "39"**.

263. I note that there are other Internet users on unrelated websites with the username "Zeta Zeroes" who are not linked to Andean. The concept of "zeta zeroes" is not unfamiliar to individuals with a background in pure mathematics.

264. However, many of the other usernames that came up in our investigation are also references to concepts in mathematics (or, in the case of "mtheorylord", theoretical physics[35]):

(a) "Umbral" is a term used in mathematics to mean "shadowy" or "mysterious", i.e., "umbral function" or "umbral calculus";

(b) Upsilon is a Greek letter [υ], used in physics to represent the mass-to-light ratio;

(c) M-theory is a theory in physics that unifies all consistent versions of superstring theory;

(d) A tensor is an algebraic object that describes a multilinear relationship between sets of algebraic objects related to a vector space.

Communications Between Jason Gottlieb and Andean's Lawyer, Andrew Lin

265. On October 17, 2021, Jason Gottlieb, our New York lawyer, sent an email to Andean's personal email address asking him to return the tokens.

266. On October 25, 2021, Jason Gottlieb received an email from Andrew Lin, an attorney in Texas, saying that his firm represents "Mr. Medjedovic" and asking all further correspondence to be directed to his firm.

---

35 I note that in mtheorylord's Wikipedia UserTalk page, which is a an administration page where editors can discuss improvements to articles or other Wikipedia page, mtheorylord described himself as an expert in mathematics, as well as theoretical physics. I have attached a copy of this UserTalk page as Exhibit "40".

267. Mr. Gottlieb and Mr. Lin exchanged further emails in which Mr. Gottlieb asked Mr. Lin "[i]s your client going to return the money?" Mr. Lin did not deny that his client had the assets from the Attack. Rather, he responded:

> "We dispute your characterization that those two statements are the same; the terms "return," "funds," and "money" result in a loaded question.
>
> To speed things along, my client currently has no plans to send ERC20 tokens[36] to an address of your choosing."

The email exchange between Mr. Gottlieb and Mr. Lin is attached as **Exhibit "41"**.

Communications Between Jason Gottlieb and Andean's Father

268. On October 18, 2021, Mr. Gottlieb called Andean's father, [redacted], and left a voicemail asking him or his lawyer to call him back. Andean's father called Mr. Gottlieb back that same day and said he had no knowledge of the Attack. He told Mr. Gottlieb that he would try to reach out to Andean, stating that he did not live with him.

269. On October 21, 2021, Andean's father called Mr. Gottlieb back twice and left two voicemails. In the first voicemail, he said he had been in contact with Andean. In the second voicemail, he stated that "what he did, he did to prove [a] point" and "I'm just telling you now as a parent, if this child — and he did before — loses his nerve, he may commit something that you're all gonna regret. The money's gonna be gone, because he's the only one who knows how to get it and you will not get anything, and I will not have my child". A transcription of these voice mail messages along with an audio recording is attached as **Exhibit "42"**.

[36] ERC20 is a standard for tokens on the Ethereum blockchain. All the underlying tokens held by DEFI5 and CC10 (i.e. the tokens that the Attack had removed) are ERC20 tokens.

270. Mr. Gottlieb called Andean's father back a few hours later and they had a lengthy conversation. Mr. Gottlieb has informed me of the details of their conversation. Mr. Medjedovic denied that Andean had hacked anything or had done anything wrong, and asserted that the Indexed Finance smart contracts had a "hole" in them. He complained that Andean had been harassed as a result of his personal information being made public, and warned Mr. Gottlieb that if further pressure was placed on Andean, he could not predict what would happen, and intimated that Andean might do something to the tokens or even that he might harm himself.

PART V – OTHER MATTERS

Standing

271. Dillon and I are co-plaintiffs in a proposed class action against Andean on behalf of the tokenholders who suffered losses as a result of the Attack.

272. At the time of the Attack, I held about $57 in DEFI tokens. I did not hold any CC10 tokens. I also held tokens in a DEFI5 liquidity pool (and a fractional amount of FFF tokens).

273. Dillon held approximately $25 worth of DEFI5 tokens and $276 worth of CC10. He did not hold any liquidity pool tokens or FFF tokens.

274. Between the two of us, we belong to the classes of tokenholders who have suffered losses as a result of the Attack, including $16.5 million in direct losses to DEFI5 and CC10 tokenholders, and an estimated additional $10 million in indirect losses to liquidity pool and FFF tokenholders.

Urgency and Risk of Dissipation

275. The balances of the tokens in the Attacker's Wallet remain the same as they were following the Attack. However, the prices of digital assets are notoriously volatile, and so the actual value of the assets has fluctuated considerably since that time.

276. Dillon and I are concerned that the assets held in the Wallet are at imminent risk of dissipation. As explained above, it appears that Andean is familiar with techniques to disguise the flow of funds on the blockchain. It appears that he used the Tornado Cash privacy mixer in an attempt to disguise the source of the tokens used to fund the Attack. Andean could easily use this technology to dissipate the assets held on the Attacker's Wallet. If the assets are dissipated to an unknown address on the blockchain, they will effectively be placed beyond the reach of any court

and there will be no way to recover the assets. Further, as explained above, Andean has attempted to delete evidence of his involvement in the Attack (including by deleting content from his personal webpage and deleting his Discord chat history).

Receivership Order

277. In traditional finance, customers generally hold their assets at financial institutions. Due to the decentralized nature of the blockchain, there is no central authority with the power to control digital assets. As a result, the disputed assets in this case cannot be secured by securing the cooperation of a financial institution.

278. As a result, Dillon and I are seeking a receivership order to preserve the disputed assets.

279. Due to the unusual nature of crypto assets, there are special technical requirements to ensure that the assets are secured. Every crypto wallet is associated with a public address and a private key. In order to control the Attacker's Wallet, Andean must have the private key, which is essentially a 64-character password (like a PIN for personal banking, but more complex).

280. While the tokens remain in the Attacker's Wallet, they cannot be secured. Even if Andean provided us with the private key, it would be possible that he kept a backup copy that would allow him to continue to exercise control over the assets.

281. In order to secure the assets, it is necessary that they be transferred to a new wallet.

282. Raymond Chabot Administrateur Provisoire Inc. (**"RCAP"**) has agreed to be named as a receiver of property to preserve the disputed assets. While appointing a receiver in the context of a dispute over crypto assets remains novel, RCAP has previously been appointed receiver over

crypto assets in a litigation matter in Quebec involving the Autorité des marchés financiers.[37] In order to ensure that the assets are secured, Andean should be required to transfer the tokens from the Attacker's Wallet to the address for a wallet controlled by RCAP. This process should take place in a controlled environment, where Andean is under the supervision of RCAP representatives to ensure that he does not dissipate the assets.

Once RCAP take possession of the assets, they have agreed to transfer the assets onto a hardware wallet (or wallets), which can be stored securely (for example, in a security deposit box). There are other alternative solutions to preserving the assets, but Dillon and I believe this approach strikes the best balance between minimizing cost and ensuring security. A memo prepared by RCAP outlining their proposed involvement is attached as **Exhibit "43"**.

Full and Frank Disclosure

283. I understand that as the moving party in an *ex parte* proceeding, I am required to make full and frank disclosure by openly acknowledging any potential weaknesses in the case. Below, I address several such matters.

The "Code Is Law" Defence

284. I anticipate that Andean may assert as a defence the idea that "code is law." This phrase has circulated in the cryptocurrency space. Generally, it means that, something is legal as long as it is technically possible on the software platform in question. "Code is law" proponents believe that, if something is technically possible under the software, it is (or should be) also legal; there are no applicable legal norms beyond what the software technically permits.

285. Applied to index pools, "code is law" might be taken to mean that, if a transaction is technically possible under the code governing the index pool — even because of a bug, exploit, or glitch — it is also legal.

286. This theory would imply that the users of an index pool have no legally meaningful expectations or intentions about how the index pool will operate, beyond the technical function of its code. In other words, "code is law" implies that the users of an index pool should reasonably be aware of all of the technically possible ways in which the code could operate, and that, when they use the platform they assume the risk of all of those potential events.

287. I do not accept "code is law". I consider it to be a fringe and unworkable view of the crypto environment. However, I acknowledge that there are users who subscribe to his view and I expect that Andean will raise it as a defence in this proceeding.

Evidence of Identity Is Circumstantial

288. In Part IV, I set out the key evidence connecting Andean to the Attack. While I believe the case that Andean is the Attacker is very strong, as a matter of full and frank disclosure, I must acknowledge that the case is largely circumstantial.

Risk of Dissipation

289. The Attack took place on October 14. The Attacker has not moved the assets since that date, i.e. they remain on the Attacker's Wallet today. As explained above, Dillon and I have made public posts regarding our investigation into this matter, which has included publishing information from which Andean could be (and it seems was in fact) identified by other users. Dillon, Pr0, and our lawyer, Mr. Gottlieb, have all communicated directly with Andean and/or his

father. Despite all of these steps, the Attacker has apparently taken no further steps to secure the assets. In light of this, it might be argued that the risk of dissipation at this stage is limited.

290. It is true that this is some evidence that Andean will not dissipate the assets. However, if he were to do so, the assets could never be retrieved and the tokenholders will never be compensated for their losses.

291. Based on the contact information we have for Andean, Dillon and I believe that he currently resides in Ontario. Dillon and I hired a private investigator to try and locate Andean. The investigator conducted private surveillance at the Medjedovic family home [redacted] The investigators observed a young man who appeared to be living at this address, but could not confirm if it was Andean (it may have been his brother). It is possible that he is still residing with his parents, though his father denied that in his conversation with Mr. Gottlieb.

292. Andean grew up in Hamilton and our most recent information about his whereabouts is that he was pursuing a Masters' degree at the University of Waterloo. We are not aware of any information to suggest that he resides outside of Ontario. However, we do not know with certainty where he was at the time of the Attack or where he is at present.

Damages Undertaking

293. I hereby give an undertaking to abide by any order this Court may make concerning damages arising from the granting and enforcement of the relief sought on this motion. I understand that if the action against Andean is ultimately dismissed and the injunctive relief causes him to suffer damages, that I will be responsible to compensate him for such losses. Dillon has also authorized me to make this undertaking on his behalf.

294. I do not anticipate that there will be any immediate damages from the issuance of the relief sought on this motion. As noted above, the stolen assets have remained at the same location since the date of the Attack. The effect of the order would simply require the assets to be preserved pending a return date for the continuation of the injunction.

295. However, cryptocurrencies and other digital assets are notoriously volatile. If the stolen assets were to decline dramatically in value, a *Mareva* order would prevent Andean from liquidating his position.

296. [redacted]. We anticipate that we would be able to satisfy any judgement awarding damages to Andean as a result of the relief sought on this motion.

Manner of Service

297. As indicated above, Dillon and I do not know Andean's current physical whereabouts, which will make it impossible to effect personal service on him. As indicated above, Andean's resume lists his personal email address is [redacted] and he corresponded with PR0 from this address. In addition to the resume posted on his personal website, he also posted a "course listing" listing the courses he had taken at the University of Waterloo. This document listed his university email address as [redacted] A copy of this course listing is attached as **Exhibit "44"**.

298. Andean's school email address was [redacted] (though it is unclear if that address remains active). Finally, the @ZetaZeroes account tweeted on October 21, 2021 that

members of the public can contact him (i.e. the Attacker, whom we believe to be Andean) at [redacted] This tweet is included with the tweets found at Exhibit "36".

299. Accordingly, we have requested that we be permitted to serve Andean by emailing these various email addresses, along with the email address of Andy Lin, the Texas lawyer who informed our New York lawyer that he represented Andean.

SWORN by Laurence Day of the Town of Otley, in the United Kingdom, before me at the City of Toronto on December 9, 2021 in accordance with O. Reg. 431/20, Administering Oath or Declaration Remotely.

Stephen Aylward

Stephen Aylward
(LSO#66556E)
Commissioner for Taking Affidavits
(or as may be)

DocuSigned by:

3B4DAD6190D8424...

LAURENCE DAY

Token Glossary

INDEXED FINANCE

CC10	One of the index tokens maintained by the Indexed Finance protocol. Designed to track the market performance of ten protocols on Ethereum, weighted by the square root of fully diluted market capitalisation.
DEFI5	One of the index tokens maintained by the Indexed Finance protocol. Designed to track the market performance of five decentralised finance protocols on Ethereum, weighted by the square root of fully diluted market capitalisation.
DEGEN	One of the index tokens maintained by the Indexed Finance protocol. Designed to track the market performance of ten protocols judged as being higher risk/reward on Ethereum, weighted by the square root of circulating market capitalisation.
FFF	One of the index tokens maintained by the Indexed Finance protocol. A meta-index (fund of funds) containing fixed percentages of both Ether and Bitcoin, alongside the DEFI5, CC10 and DEGEN index tokens weighted by the square root of fully diluted market capitalisation.
LPs	Liquidity Pool tokens. A catch-all category of tokens across decentralised finance that are designed to hold certain underlying assets in a given ratio, enabling swaps from one underlying asset to another. An example of a 'classic' LP is the Uniswap ETH-DEFI5 token, which represents a claim on equal amounts of both ETH and DEFI5 in the Uniswap automated market maker protocol. The index tokens provided by Indexed Finance - such as DEFI5 and CC10 - are also LPs mechanically.
NDX	The native token for the Indexed Finance protocol/DAO, used to propose and vote on upgrades to the protocol and usage of the DAO treasury. Indexed Finance is a protocol for passive portfolio management.

Token Glossary

ATTACKED INDEX POOLS

#DEFI5	
AAVE	The native token of the Aave protocol. Aave maintains a system of pools enabling borrowing and lending markets
COMP	The native token for the Compound protocol. Compound maintains a system of pools enabling borrowing and lending markets.
CRV	The native token of the Curve protocol. Curve is an exchange protocol enabling low slippage trades of stablecoins.
MKR	The native token of the Maker protocol. Maker enables its users to mint stablecoins that are backed by collateral.
SNX	The native token of the Synthetix protocol. Synthetix enables the issuance of synthetic crypto assets.
UNI	The native token for the Uniswap protocol. Uniswap enables automated market making/liquidity provision.

#CC10 There is significant crossover between the assets backing DEFI5 and CC10: this section includes those tokens that are unique to CC10.	
BAT	The native token of the Basic Attention Token (BAT) protocol. BAT provides a mechanism to track and reward user engagement on websites via the Brave browser.
LINK	The native token of the Chainlink protocol. Chainlink is an oracle network enabling blockchains to securely access off-chain data.
YFI	The native token of the Yearn Finance protocol. Yearn is a suite of products designed to generate yield on assets.
UMA	The native token of the Universal Market Access (UMA) protocol. UMA enables the issuance of synthetic crypto assets

THIS IS **EXHIBIT "1"** TO
THE AFFIDAVIT OF **LAURENCE DAY**
SWORN BEFORE ME
THIS 9th DAY OF DECEMBER, 2021

Stephen Ayford

A COMMISSIONER ETC.

DEFI5 Phase Appendices

Appendix A1: Pre-Attack Balance ("Before")

Token	Balance	Etherscan Price	Etherscan Value
UNI	203,318.87	$26.29	$5,345,252.97
AAVE	7,503.27	$303.43	$2,276,718.11
COMP	5,709.37	$314.38	$1,794,912.78
SNX	19,308.37	$9.92	$191,539.01
CRV	741,773.28	$2.88	$2,136,307.05
MKR	638.74	$2,542.91	$1,624,267.25
SUSHI	0	$10.75	0
			$13,368,997.16

Appendix A2: List of Flash Loaned Assets (Step 2)

Token	Balance	Etherscan Price	Etherscan Value
UNI	1,836,342.050150158215305238	$26.29	$48,271,982.37
AAVE	221,217.366781517207266602	$303.43	$67,123,677.50
COMP	41,371.149252067400558421	$314.38	$13,006,305.96
SNX	453,645.29	$9.92	$4,501,194.78
CRV	3,210,906.891991096095551982	$2.88	$9,246,025.97
MKR	5,775.828019598003061742	$2,542.91	$14,687,427.71
SUSHI*	0	$10.75	0
			$156,836,614.29

**220,000 SUSHI tokens ($2,365,000) were later borrowed as part of Step 6*

Appendix A3: Swap $53M UNI for 1.4M DEFI5 (Step 5)

1) Swap 2,389.414860885138837488 ($62,810.63) UNI for 25,471.633387232158076309 DEFI5

2) Swap 3,584.122291327708256232 ($94,215.94) UNI for 29,767.255557763571422998 DEFI5

3) Swap 5,376.183436991562384348 ($141,323.91) UNI for 34,787.30594031574962976 DEFI5

4) Swap 8,064.275155487343576522 ($211,985.86) UNI for 40,653.954552068457710056 DEFI5

5) Swap 12,096.412733231015364783 ($317,978.79) UNI for 47,509.974573979511133395 DEFI5

6) Swap 18,144.619099846523047174 ($476,968.18) UNI for 55,522.216937819011575313 DEFI5

7) Swap 27,216.928649769784570761 ($715,452.28) UNI for 64,885.670879280857695997 DEFI5

8) Swap 40,825.392974654676856142 ($1,073,178.41) UNI for 75,828.20927646727283924 DEFI5

9) Swap 61,238.089461982015284213 ($1,609,767.62) UNI for 88,616.134258261444062367 DEFI5

10) Swap 91,857.134192973022926319 ($2,414,651.43) UNI for 103,560.658042801523009688 DEFI5

11) Swap 137,785.701289459534389479 ($3,621,977.15) UNI for 121,025.476726414824039859 DEFI5

12) Swap 206,678.551934189301584218 ($5,432,965.72) UNI for 141,435.621341864361582035 DEFI5

13) Swap 310,017.827901283952376327 ($8,149,448.59) UNI for 165,287.801588912803499104 DEFI5

14) Swap 465,026.741851925928564491 ($12,224,172.88) UNI for 193,162.493966498250165646 DEFI5

15) Swap 644,580.689800521031826236 ($16,944,113.27) UNI for 210,374.204745766242860969 DEFI5

Total: 2,034,882.08563 ($53,491,014.77) UNI swapped for 1,397,888.61178 DEFI5

Note that the amount of UNI is increasing by ~50% each time, in order to counteract the 50% Swap-In Limit. The price of UNI increases with each swap.

Appendix A4: Burn 1.4M DEFI5 for $155M (Step 7)

In exchange for 1,397,888.61178 DEFI5 minted via 2,034,882.08563 ($53,491,014.77) UNI, the Attacker received:

Token	**Balance**	**Etherscan Price**	**Etherscan Value**
UNI	1,831,566.343330240617728547	$26.29	$48,146,443.21
AAVE	205,385.621985262857206477	$303.43	$62,319,873.22
COMP	42,277.174548189683442085	$314.38	$13,291,143.16
SNX	424,700.988319216238210387	$9.92	$4,214,001.34
CRV	3,549,411.530679908933793216	$2.88	$10,220,773.22
MKR	5,760.130630049946860487	$2,542.91	$14,647,510.61
SUSHI*	197,554.69769457460566	$10.75	$2,124,567.58
			$154,964,312.34

Appendix A5: Mint DEFI5 Using SUSHI – 1st Cycle (Step 8)

1) Swap 11,222.65115271269717 ($120,692.05) SUSHI for 67,499.684519332941363234 DEFI5

2) Swap 16,833.976729069045755 ($181,038.07) SUSHI for 96,331.350683206931920918 DEFI5

3) Swap 25,250.9650936035686325 ($271,557.10) SUSHI for 137,478.111053884057334209 DEFI5

4) Swap 37,876.44764040535294875 ($407,335.66) SUSHI for 196,200.207771392551228746 DEFI5

5) Swap 56,814.671460608029423125 ($611,003.49) SUSHI for 280,004.731185532619550406 DEFI5

6) Swap 49,555.985618175911730625 ($532,941.21) SUSHI for 234,705.858740895078765984 DEFI5

Total: 197,554.697695 (US$2,124,567.64) SUSHI swapped for 1,012,219.94395 DEFI5

Appendix A6: Burn DEFI5– 1st Cycle (Step 9)

In exchange for 1,012,219.943954244180163497 DEFI5 minted via 197,554.697695 (US$2,124,567.64) SUSHI, the Attacker received:

Token	Balance	Etherscan Price	Etherscan Value
UNI	179,093.934051089875196853	$26.29	$4,707,847.99
AAVE	20,082.984803045446445208	$303.43	$6,093,752.11
COMP	4,133.940077012380234875	$314.38	$1,299,632.48
SNX	41,528.045691850844916215	$9.92	$412,052.82
CRV	347,068.003793925157246003	$2.88	$999,406.05
MKR	563.236193403792245982	$2,542.91	$1,432,260.59
SUSHI*	189,340.18849038459342	$10.75	$2,036,226.07
			$16,981,178.11

Appendix A7: Mint DEFI5 From SUSHI – 2nd Cycle (Step 10)

1) Swap 15,329.90575480770329 ($164,862.80) SushiToken (SUSHI) for 69,661.471475547919592496 DEFI5

2) Swap 22,994.858632211554935 ($247,294.20) SushiToken (SUSHI) for 99,416.51854531571270335 DEFI5

3) Swap 34,492.2879483173324025 ($370,941.30) SushiToken (SUSHI) for 141,881.070702624913425829 DEFI5

4) Swap 51,738.43192247599860375 ($556,411.95) SushiToken (SUSHI) for 202,483.837879995265779382 DEFI5

5) Swap 64,784.70423257200418875 ($696,715.82) SushiToken (SUSHI) for 242,150.543553564643779848 DEFI5

Total: 189,340.18849 ($2,036,226.07) SUSHI swapped for 755,593.442157 DEFI5

Appendix A8: Burn DEFI5 – 2nd Cycle (Step 10)

In exchange for 755,593.442157 DEFI5 minted via 189,340.18849 ($2,036,226.07) of SUSHI, the Attacker received:

Token	Balance	Etherscan Price	Etherscan Value
UNI	23,733.041606642467780005	$26.29	$623,871.23
AAVE	2,661.342587852686880985	$303.43	$807,527.47
COMP	547.818508577256493576	$314.38	$172,223.77
SNX	5,503.183798319426136593	$9.92	$54,604.12
CRV	45,992.509003827120531519	$2.88	$132,438.57
MKR	74.638530239700089697	$2,542.91	$189,799.28
SUSHI*	180,039.80319219324848	$10.75	$1,936,206.70
			$3,916,671.14

Appendix A9: Net Tokens Routed to Attacker's Wallet (Step 11)

Token	Balance	Etherscan Price	Etherscan Value
UNI	192,358.608482349254932721	$26.29	$5,056,536.91
AAVE	6,226.808757621079923542	$303.43	$1,889,391.91
COMP	5,459.533319030510670384	$314.38	$1,716,373.90
SNX	16,680.624942480894626934	$9.92	$165,509.80
CRV	721,611.340121392718122545	$2.88	$2,077,929.20
MKR	406.568450634979514865	$2,542.91	$1,033,868.17
			$11,939,609.89

Appendix A10: DEFI5 Token Balances Post-Attack ("After")

Token	Balance	Etherscan Price	Etherscan Value
UNI	5,267.60	$26.29	$138,485.20
AAVE	590.69	$303.43	$179,233.07
COMP	121.59	$314.38	$38,225.46
SNX	1,221.44	$9.92	$12,116.68
CRV	10,208.13	$2.88	$29,399.41
MKR	16.57	$2,542.91	$42,136.02
SUSHI	39,960.20	$10.75	$429,572.15
			$869,168.00

Total DEFI5 NAV Before Attack		=	$13,368,997.16
-	Total DEFI5 NAV After Attack	=	$869,168.00
=	**Loss to DEFI5 Pool NAV**	**=**	**$12,499,829.16**

THIS IS **EXHIBIT "2"** TO
THE AFFIDAVIT OF **LAURENCE DAY**
SWORN BEFORE ME
THIS 9th DAY OF DECEMBER, 2021

Stephen Ayford

A COMMISSIONER ETC.

DEFI5 Transaction Log

#	EVENT ACTION	EVENT LOG	FROM	TO	AMOUNT	EST. USD VALUE	TOKEN
1	SUSHI Introduced To DEFI5	63					
2	Reindex Confirmed	64					
3	Flash Loan	66	Uniswap V2: UNI 30	0x277e851587eb5da22b52a10f4788576e68150277	1,836,342.05	$48,271,982.37	Uniswap (UNI)
4	Flash Loan	72	SushiSwap: AAVE	0x277e851587eb5da22b52a10f4788576e68150277	221,217.37	$67,123,677.50	Aave Token (AAVE)
5	Flash Loan	74	SushiSwap: COMP	0x277e851587eb5da22b52a10f4788576e68150277	41,371.15	$13,006,305.96	Compound (COMP)
6	Flash Loan	76	SushiSwap: CRV	0x277e851587eb5da22b52a10f4788576e68150277	3,210,906.89	$9,246,025.97	Curve DAO To... (CRV)
7	Flash Loan	78	SushiSwap: MKR	0x277e851587eb5da22b52a10f4788576e68150277	5,775.83	$14,687,427.71	Maker (MKR)
8	Flash Loan	80	SushiSwap: SNX	0x277e851587eb5da22b52a10f4788576e68150277	453,645.29	$4,501,194.78	Synthetix Ne... (SNX)
9	Swap In AAVE	85	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	3,751.64	$1,138,353.83	Aave Token (AAVE)
10	Swap Out UNI	87	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	32,696.63	$859,497.36	Uniswap (UNI)
11	Swap In AAVE	95	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	5,627.45	$1,707,530.74	Aave Token (AAVE)
12	Swap Out UNI	97	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	27,571.27	$724,766.73	Uniswap (UNI)
13	Swap In AAVE	104	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	8,441.18	$2,561,296.12	Aave Token (AAVE)
14	Swap Out UNI	106	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	23,115.96	$607,649.90	Uniswap (UNI)
15	Swap In AAVE	113	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	12,661.77	$3,841,944.17	Aave Token (AAVE)
16	Swap Out UNI	115	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	19,380.59	$509,458.26	Uniswap (UNI)
17	Swap In AAVE	112	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	18,992.66	$5,762,916.26	Aave Token (AAVE)
18	Swap Out UNI	124	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	16,248.84	$427,133.65	Uniswap (UNI)
19	Swap In AAVE	131	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	28,488.99	$8,644,374.39	Aave Token (AAVE)
20	Swap Out UNI	133	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	13,623.15	$358,112.08	Uniswap (UNI)
21	Swap In AAVE	140	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	42,733.48	$12,966,561.58	Aave Token (AAVE)
22	Swap Out UNI	142	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	11,421.75	$300,243.87	Uniswap (UNI)
23	Swap In AAVE	149	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	64,100.23	$19,449,842.37	Aave Token (AAVE)
24	Swap Out UNI	151	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	9,576.08	$251,726.73	Uniswap (UNI)
25	Swap In AAVE	158	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	36,419.96	$11,050,858.03	Aave Token (AAVE)
26	Swap Out UNI	160	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	3,601.45	$94,671.48	Uniswap (UNI)
27	Swap In COMP	163	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	2,854.69	$897,459.43	Compound (COMP)
28	Swap Out UNI	165	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	6,010.72	$158,003.99	Uniswap (UNI)
29	Swap In COMP	169	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	4,282.03	$1,346,189.14	Compound (COMP)
30	Swap Out UNI	171	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	5,275.40	$138,674.49	Uniswap (UNI)
31	Swap In COMP	174	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	6,423.04	$2,019,283.72	Compound (COMP)
32	Swap Out UNI	176	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	4,580.91	$120,418.48	Uniswap (UNI)
33	Swap In COMP	179	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	9,634.57	$3,028,925.57	Compound (COMP)
34	Swap Out UNI	181	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	3,977.85	$104,565.81	Uniswap (UNI)
35	Swap In COMP	184	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	14,451.85	$4,543,388.36	Compound (COMP)
36	Swap Out UNI	186	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	3,454.18	$90,800.09	Uniswap (UNI)
37	Swap In COMP	189	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	3,724.97	$1,171,059.73	Compound (COMP)
38	Swap Out UNI	191	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	642.7406388	$16,895.74	Uniswap (UNI)
39	Swap In CRV	194	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	370,886.64	$1,067,993.44	Curve DAO To... (CRV)
40	Swap Out UNI	196	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	3,444.06	$90,534.12	Uniswap (UNI)
41	Swap In CRV	199	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	556,329.96	$1,601,990.17	Curve DAO To... (CRV)
42	Swap Out UNI	200	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	2,928.46	$76,980.40	Uniswap (UNI)
43	Swap In CRV	203	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	834,494.94	$2,402,985.25	Curve DAO To... (CRV)
44	Swap Out UNI	204	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	2,469.79	$64,923.39	Uniswap (UNI)

45	Swap In CRV	207	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	1,251,742.41	$3,604,477.87	Curve DAO To... (CRV)
46	Swap Out UNI	208	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	2,082.96	$54,754.80	Uniswap (UNI)
47	Swap In CRV	211	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	197,452.94	$568,579.23	Curve DAO To... (CRV)
48	Swap Out UNI	212	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	238.1671327	$6,260.71	Uniswap (UNI)
49	Swap In MKR	215	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	319.3717531	$812,134.56	Maker (MKR)
50	Swap Out UNI	216	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	1,298.27	$34,127.71	Uniswap (UNI)
51	Swap In MKR	219	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	479.0576296	$1,218,201.84	Maker (MKR)
52	Swap Out UNI	220	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	1,144.74	$30,091.70	Uniswap (UNI)
53	Swap In MKR	223	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	718.5864444	$1,827,302.76	Maker (MKR)
54	Swap Out UNI	224	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	1,009.36	$26,533.00	Uniswap (UNI)
55	Swap In MKR	227	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	1,077.88	$2,740,954.13	Maker (MKR)
56	Swap Out UNI	228	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	889.9885951	$23,395.16	Uniswap (UNI)
57	Swap In MKR	231	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	1,616.82	$4,111,431.20	Maker (MKR)
58	Swap Out UNI	232	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	784.7368821	$20,628.40	Uniswap (UNI)
59	Swap In MKR	235	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	1,564.11	$3,977,403.23	Maker (MKR)
60	Swap Out UNI	236	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	485.7472899	$12,768.85	Uniswap (UNI)
61	Swap In SNX	239	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	9,654.18	$95,791.50	Synthetix Ne... (SNX)
62	Swap Out UNI	240	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	78.13292338	$2,053.88	Uniswap (UNI)
63	Swap In SNX	243	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	14,481.28	$143,687.25	Synthetix Ne... (SNX)
64	Swap Out UNI	244	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	76 99506002	$2,023.97	Uniswap (UNI)
65	Swap In SNX	247	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	21,721.91	$215,530.87	Synthetix Ne... (SNX)
66	Swap Out UNI	248	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	75 87376755	$1,994.50	Uniswap (UNI)
67	Swap In SNX	251	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	32,582.87	$323,296.31	Synthetix Ne... (SNX)
68	Swap Out UNI	252	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	74.76880466	$1,965.45	Uniswap (UNI)
69	Swap In SNX	255	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	48,874.31	$484,944.47	Synthetix Ne... (SNX)
70	Swap Out UNI	256	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	73.67993354	$1,936.83	Uniswap (UNI)
71	Swap In SNX	259	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	73,311.46	$727,416.70	Synthetix Ne... (SNX)
72	Swap Out UNI	260	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	72.60691984	$1,908.62	Uniswap (UNI)
73	Swap In SNX	263	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	109,967.19	$1,091,125.05	Synthetix Ne... (SNX)
74	Swap Out UNI	264	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	71 54953263	$1,880.82	Uniswap (UNI)
75	Swap In SNX	267	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	143,052.09	$1,419,402.63	Synthetix Ne... (SNX)
76	Swap Out UNI	268	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	62.66594215	$1,647.30	Uniswap (UNI)
77	Update SUSHI Minimum Balance	271					
78	Create New DEFI5	273	Black Hole: 0x000…000	Indexed: DEFI5 Token	25,471.63	$90,031.72	DEFI Top 5 T... (DEFI5)
79	Transfer DEFI5 To Attack Contract	274	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	25,471.63	$90,031.72	DEFI Top 5 T... (DEFI5)
80	Mint DEFI5 Via UNI [Log 272]	275	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	2,389.41	$62,810.63	Uniswap (UNI)
81	Create New DEFI5	278	Black Hole: 0x000…000	Indexed: DEFI5 Token	29,767.26	$105,214.98	DEFI Top 5 T... (DEFI5)
82	Transfer DEFI5 To Attack Contract	279	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	29,767.26	$105,214.98	DEFI Top 5 T... (DEFI5)
83	Mint DEFI5 Via UNI [Log 277]	280	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	3,584.12	$94,215.94	Uniswap (UNI)
84	Create New DEFI5	283	Black Hole: 0x000…000	Indexed: DEFI5 Token	34,787.31	$122,958.78	DEFI Top 5 T... (DEFI5)
85	Transfer DEFI5 To Attack Contract	284	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	34,787.31	$122,958.78	DEFI Top 5 T... (DEFI5)
86	Mint DEFI5 Via UNI [Log 282]	285	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	5,376.18	$141,323.91	Uniswap (UNI)
87	Create New DEFI5	288	Black Hole: 0x000…000	Indexed: DEFI5 Token	40,653.95	$143,694.97	DEFI Top 5 T... (DEFI5)
88	Transfer DEFI5 To Attack Contract	289	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	40,653.95	$143,694.97	DEFI Top 5 T... (DEFI5)
89	Mint DEFI5 Via UNI [Log 287]	290	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	8,064.28	$211,985.86	Uniswap (UNI)

DEFI5 Transaction Log

90	Create New DEFI5	293	Black Hole: 0x000…000	Indexed: DEFI5 Token	47,509.97	$167,928.17	DEFI Top 5 T... (DEFI5)
91	Transfer DEFI5 To Attack Contract	294	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	47,509.97	$167,928.17	DEFI Top 5 T... (DEFI5)
92	Mint DEFI5 Via UNI [Log 292]	295	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	12,096.41	$317,978.79	Uniswap (UNI)
93	Create New DEFI5	298	Black Hole: 0x000…000	Indexed: DEFI5 Token	55,522.22	$196,248.15	DEFI Top 5 T... (DEFI5)
94	Transfer DEFI5 To Attack Contract	299	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	55,522.22	$196,248.15	DEFI Top 5 T... (DEFI5)
95	Mint DEFI5 Via UNI [Log 297]	300	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	18,144.62	$476,968.18	Uniswap (UNI)
96	Create New DEFI5	303	Black Hole: 0x000…000	Indexed: DEFI5 Token	64,885.67	$229,344.09	DEFI Top 5 T... (DEFI5)
97	Transfer DEFI5 To Attack Contract	304	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	64,885.67	$229,344.09	DEFI Top 5 T... (DEFI5)
98	Mint DEFI5 Via UNI [Log 302]	305	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	27,216.93	$715,452.28	Uniswap (UNI)
99	Create New DEFI5	308	Black Hole: 0x000…000	Indexed: DEFI5 Token	75,828.21	$268,021.46	DEFI Top 5 T... (DEFI5)
100	Transfer DEFI5 To Attack Contract	309	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	75,828.21	$268,021.46	DEFI Top 5 T... (DEFI5)
101	Mint DEFI5 Via UNI [Log 307]	310	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	40,825.39	$1,073,178.41	Uniswap (UNI)
102	Create New DEFI5	313	Black Hole: 0x000…000	Indexed: DEFI5 Token	88,616.13	$313,221.50	DEFI Top 5 T... (DEFI5)
103	Transfer DEFI5 To Attack Contract	314	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	88,616.13	$313,221.50	DEFI Top 5 T... (DEFI5)
104	Mint DEFI5 Via UNI [Log 312]	315	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	61,238.09	$1,609,767.62	Uniswap (UNI)
105	Create New DEFI5	318	Black Hole: 0x000…000	Indexed: DEFI5 Token	103,560.66	$366,044.23	DEFI Top 5 T... (DEFI5)
106	Transfer DEFI5 To Attack Contract	319	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	103,560.66	$366,044.23	DEFI Top 5 T... (DEFI5)
107	Mint DEFI5 Via UNI [Log 317]	320	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	91,857.13	$2,414,651.43	Uniswap (UNI)
108	Create New DEFI5	323	Black Hole: 0x000…000	Indexed: DEFI5 Token	121,025.48	$427,775.16	DEFI Top 5 T... (DEFI5)
109	Transfer DEFI5 To Attack Contract	324	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	121,025.48	$427,775.16	DEFI Top 5 T... (DEFI5)
110	Mint DEFI5 Via UNI [Log 322]	325	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	137,785.70	$3,621,977.15	Uniswap (UNI)
111	Create New DEFI5	328	Black Hole: 0x000…000	Indexed: DEFI5 Token	141,435.62	$499,916.61	DEFI Top 5 T... (DEFI5)
112	Transfer DEFI5 To Attack Contract	329	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	141,435.62	$499,916.61	DEFI Top 5 T... (DEFI5)
113	Mint DEFI5 Via UNI [Log 327]	330	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	206,678.55	$5,432,965.72	Uniswap (UNI)
114	Create New DEFI5	333	Black Hole: 0x000…000	Indexed: DEFI5 Token	165,287.80	$584,224.23	DEFI Top 5 T... (DEFI5)
115	Transfer DEFI5 To Attack Contract	334	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	165,287.80	$584,224.23	DEFI Top 5 T... (DEFI5)
116	Mint DEFI5 Via UNI [Log 332]	335	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	310,017.83	$8,149,448.59	Uniswap (UNI)
117	Create New DEFI5	338	Black Hole: 0x000…000	Indexed: DEFI5 Token	193,162.49	$682,749.78	DEFI Top 5 T... (DEFI5)
118	Transfer DEFI5 To Attack Contract	339	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	193,162.49	$682,749.78	DEFI Top 5 T... (DEFI5)
119	Mint DEFI5 Via UNI [Log 337]	340	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	465,026.74	$12,224,172.88	Uniswap (UNI)
120	Create New DEFI5	343	Black Hole: 0x000…000	Indexed: DEFI5 Token	210,374.20	$743,586.08	DEFI Top 5 T... (DEFI5)
121	Transfer DEFI5 To Attack Contract	344	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	210,374.20	$743,586.08	DEFI Top 5 T... (DEFI5)
122	Mint DEFI5 Via UNI [Log 342]	345	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	644,580.69	$16,944,113.27	Uniswap (UNI)
123	Flash Loan	347	SushiSwap: SUSHI	0x277e851587eb5da22b52a10f4788576e68150277	220,000	$2,365,951.67	SushiToken (SUSHI)
124	SUSHI "Gift"	348	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	220,000	$2,365,951.67	SushiToken (SUSHI)
125	SUSHI Initialised	349					
126	SUSHI Massively Overweighed	350					
127	Transfer DEFI5 For Redemption	351	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	1,397,888.61	$4,940,959.89	DEFI Top 5 T... (DEFI5)
128	Exit Fee Sent To Treasury	352	Indexed: DEFI5 Token	0x78a3ef33cf033381feb43ba4212f2af5a5a0a2ea	6,989.44	$24,704.80	DEFI Top 5 T... (DEFI5)
129	Remaining DEFI5 Burned	353	Indexed: DEFI5 Token	Black Hole: 0x000…000	1,390,899.17	$4,916,255.09	DEFI Top 5 T... (DEFI5)
130	Remove UNI	355	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	1,831,566.34	$48,146,443.21	Uniswap (UNI)
131	Remove AAVE	362	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	205,385.62	$62,319,873.22	Aave Token (AAVE)
132	Remove COMP	364	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	42,277.17	$13,291,143.16	Compound (COMP)
133	Remove SNX	367	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	424,700.99	$4,214,001.34	Synthetix Ne... (SNX)
134	Remove CRV	369	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	3,549,411.53	$10,220,773.22	Curve DAO To... (CRV)

135	Remove MKR	371	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	5,760.13	$14,647,510.61	Maker (MKR)
136	Remove SUSHI	373	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	197,554.70	$2,124,567.58	SushiToken (SUSHI)
137	Create New DEFI5	376	Black Hole: 0x000…000	Indexed: DEFI5 Token	67,499.68	$238,583.55	DEFI Top 5 T... (DEFI5)
138	Transfer DEFI5 To Attack Contract	377	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	67,499.68	$238,583.55	DEFI Top 5 T... (DEFI5)
139	Mint DEFI5 Via SUSHI [Log 375]	378	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	11,222.65	$120,692.05	SushiToken (SUSHI)
140	Create New DEFI5	381	Black Hole: 0x000…000	Indexed: DEFI5 Token	96,331.35	$340,491.61	DEFI Top 5 T... (DEFI5)
141	Transfer DEFI5 To Attack Contract	382	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	96,331.35	$340,491.61	DEFI Top 5 T... (DEFI5)
142	Mint DEFI5 Via SUSHI [Log 380]	383	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	16,833.98	$181,038.07	SushiToken (SUSHI)
143	Create New DEFI5	386	Black Hole: 0x000…000	Indexed: DEFI5 Token	137,478.11	$485,928.44	DEFI Top 5 T... (DEFI5)
144	Transfer DEFI5 To Attack Contract	387	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	137,478.11	$485,928.44	DEFI Top 5 T... (DEFI5)
145	Mint DEFI5 Via SUSHI [Log 385]	388	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	25,250.97	$271,557.10	SushiToken (SUSHI)
146	Create New DEFI5	391	Black Hole: 0x000…000	Indexed: DEFI5 Token	196,200.21	$693,486.84	DEFI Top 5 T... (DEFI5)
147	Transfer DEFI5 To Attack Contract	392	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	196,200.21	$693,486.84	DEFI Top 5 T... (DEFI5)
148	Mint DEFI5 Via SUSHI [Log 390]	393	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	37,876.45	$407,335.66	SushiToken (SUSHI)
149	Create New DEFI5	396	Black Hole: 0x000…000	Indexed: DEFI5 Token	280,004.73	$989,701.28	DEFI Top 5 T... (DEFI5)
150	Transfer DEFI5 To Attack Contract	397	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	280,004.73	$989,701.28	DEFI Top 5 T... (DEFI5)
151	Mint DEFI5 Via SUSHI [Log 395]	398	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	56,814.67	$611,003.49	SushiToken (SUSHI)
152	Create New DEFI5	401	Black Hole: 0x000…000	Indexed: DEFI5 Token	234,705.86	$829,588.44	DEFI Top 5 T... (DEFI5)
153	Transfer DEFI5 To Attack Contract	402	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	234,705.86	$829,588.44	DEFI Top 5 T... (DEFI5)
154	Mint DEFI5 Via SUSHI [Log 400]	403	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	49,555.99	$532,941.21	SushiToken (SUSHI)
155	Transfer DEFI5 For Redemption	405	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	1,012,219.94	$3,577,780.16	DEFI Top 5 T... (DEFI5)
156	Exit Fee Sent To Treasury	406	Indexed: DEFI5 Token	0x78a3ef33cf033381feb43ba4212f2af5a5a0a2ea	5,061.10	$17,888.90	DEFI Top 5 T... (DEFI5)
157	Remaining DEFI5 Burned	407	Indexed: DEFI5 Token	Black Hole: 0x000…000	1,007,158.84	$3,559,891.26	DEFI Top 5 T... (DEFI5)
158	Remove UNI	409	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	179,093.93	$4,707,847.99	Uniswap (UNI)
159	Remove AAVE	416	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	20,082.98	$6,093,752.11	Aave Token (AAVE)
160	Remove COMP	418	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	4,133.94	$1,299,632.48	Compound (COMP)
161	Remove SNX	421	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	41,528.05	$412,052.82	Synthetix Ne... (SNX)
162	Remove CRV	423	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	347,068.00	$999,406.05	Curve DAO To... (CRV)
163	Remove MKR	425	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	563.2361934	$1,432,260.59	Maker (MKR)
164	Remove SUSHI	427	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	189,340.19	$2,036,226.07	SushiToken (SUSHI)
165	Create New DEFI5	429	Black Hole: 0x000…000	Indexed: DEFI5 Token	69,661.47	$246,224.58	DEFI Top 5 T... (DEFI5)
166	Transfer DEFI5 To Attack Contract	430	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	69,661.47	$246,224.58	DEFI Top 5 T... (DEFI5)
167	Mint DEFI5 Via SUSHI [Log 428]	431	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	15,329.91	$164,862.80	SushiToken (SUSHI)
168	Create New DEFI5	434	Black Hole: 0x000…000	Indexed: DEFI5 Token	99,416.52	$351,396.40	DEFI Top 5 T... (DEFI5)
169	Transfer DEFI5 To Attack Contract	435	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	99,416.52	$351,396.40	DEFI Top 5 T... (DEFI5)
170	Mint DEFI5 Via SUSHI [Log 433]	436	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	22,994.86	$247,294.20	SushiToken (SUSHI)
171	Create New DEFI5	439	Black Hole: 0x000…000	Indexed: DEFI5 Token	141,881.07	$501,491.09	DEFI Top 5 T... (DEFI5)
172	Transfer DEFI5 To Attack Contract	440	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	141,881.07	$501,491.09	DEFI Top 5 T... (DEFI5)
173	Mint DEFI5 Via SUSHI [Log 438]	441	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	34,492.29	$370,941.30	SushiToken (SUSHI)
174	Create New DEFI5	444	Black Hole: 0x000…000	Indexed: DEFI5 Token	202,483.84	$715,696.88	DEFI Top 5 T... (DEFI5)
175	Transfer DEFI5 To Attack Contract	445	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	202,483.84	$715,696.88	DEFI Top 5 T... (DEFI5)
176	Mint DEFI5 Via SUSHI [Log 443]	446	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	51,738.43	$556,411.95	SushiToken (SUSHI)
177	Create New DEFI5	449	Black Hole: 0x000…000	Indexed: DEFI5 Token	242,150.54	$855,902.33	DEFI Top 5 T... (DEFI5)
178	Transfer DEFI5 To Attack Contract	450	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	242,150.54	$855,902.33	DEFI Top 5 T... (DEFI5)
179	Mint DEFI5 Via SUSHI [Log 448]	451	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	64,784.70	$696,715.82	SushiToken (SUSHI)

180	Transfer DEFI5 For Redemption	453	0x277e851587eb5da22b52a10f4	Indexed: DEFI5 Token	755,593.44	$2,670,711.29	DEFI Top 5 T... (DEFI5)
181	Exit Fee Sent To Treasury	454	Indexed: DEFI5 Token	0x78a3ef33cf033381feb43ba4212f2af5a5a0a2ea	3,777.97	$13,353.56	DEFI Top 5 T... (DEFI5)
182	Remaining DEFI5 Burned	455	Indexed: DEFI5 Token	Black Hole: 0x000…000	751,815.47	$2,657,357.73	DEFI Top 5 T... (DEFI5)
183	Remove UNI	457	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	23,733.04	$623,871.23	Uniswap (UNI)
184	Remove AAVE	464	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	2,661.34	$807,527.47	Aave Token (AAVE)
185	Remove COMP	466	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	547.8185086	$172,223.77	Compound (COMP)
186	Remove SNX	469	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	5,503.18	$54,604.12	Synthetix Ne... (SNX)
187	Remove CRV	471	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	45,992.51	$132,438.57	Curve DAO To... (CRV)
188	Remove MKR	473	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	74.63853024	$189,799.28	Maker (MKR)
189	Remove SUSHI	475	Indexed: DEFI5 Token	0x277e851587eb5da22b52a10f4788576e68150277	180,039.80	$1,936,206.70	SushiToken (SUSHI)
190	Repay Flash Loan	476	0x277e851587eb5da22b52a10f4	Uniswap V2: UNI 30	1,842,034.71	$48,421,625.51	Uniswap (UNI)
191	Repay Flash Loan	481	0x277e851587eb5da22b52a10f4	SushiSwap: AAVE	221,903.14	$67,331,760.90	Aave Token (AAVE)
192	Repay Flash Loan	482	0x277e851587eb5da22b52a10f4	SushiSwap: COMP	41,499.40	$13,046,625.51	Compound (COMP)
193	Repay Flash Loan	483	0x277e851587eb5da22b52a10f4	SushiSwap: CRV	3,220,860.70	$9,274,688.65	Curve DAO To... (CRV)
194	Repay Flash Loan	484	0x277e851587eb5da22b52a10f4	SushiSwap: MKR	5,793.73	$14,732,958.73	Maker (MKR)
195	Repay Flash Loan	485	0x277e851587eb5da22b52a10f4	SushiSwap: SNX	455,051.59	$4,515,148.48	Synthetix Ne... (SNX)
196	Swap In MKR On Uniswap	487	0x277e851587eb5da22b52a10f4	Uniswap V2: MKR 2	173.7913451	$441,936.26	Maker (MKR)
197	Repay Flash Loan	488	Uniswap V2: MKR 2	SushiSwap: SUSHI	113.534708	$430,170.97	Wrapped Ethe... (WETH)
198	Repay Flash Loan	491	0x277e851587eb5da22b52a10f4	SushiSwap: SUSHI	180,039.80	$1,936,206.70	SushiToken (SUSHI)
199	Swap In MKR On Uniswap	492	0x277e851587eb5da22b52a10f4	Uniswap V2: MKR 2	23 91247149	$60,807.33	Maker (MKR)
200	Swap Out WETH On Uniswap	493	Uniswap V2: MKR 2	Uniswap V2: Router 2	15	$56,833.41	Wrapped Ethe... (WETH)
201	Unwrap 15 WETH To 15 Ether *	496					
202	Transfer UNI To Attack Invoker	511	0x277e851587eb5da22b52a10f4	Indexed Finance Exploiter	192,358.61	$5,056,536.91	Uniswap (UNI)
203	Transfer AAVE To Attack Invoker	516	0x277e851587eb5da22b52a10f4	Indexed Finance Exploiter	6,226.81	$1,889,391.91	Aave Token (AAVE)
204	Transfer COMP To Attack Invoker	517	0x277e851587eb5da22b52a10f4	Indexed Finance Exploiter	5,459.53	$1,716,373.90	Compound (COMP)
205	Transfer CRV To Attack Invoker	518	0x277e851587eb5da22b52a10f4	Indexed Finance Exploiter	721,611.34	$2,077,929.20	Curve DAO To... (CRV)
206	Transfer MKR To Attack Invoker **	519	0x277e851587eb5da22b52a10f4	Indexed Finance Exploiter	406.5684506	$1,033,868.17	Maker (MKR)
207	Transfer SNX To Attack Invoker	520	0x277e851587eb5da22b52a10f4	Indexed Finance Exploiter	16,680.62	$165,509.80	Synthetix Ne... (SNX)
	* This Ether is ultimately also sent to Attack Invoker, but does not show up in this set of records (only considers non-ETH tokens).						
	** The amount of MKR stolen is really 23.91247149 + 406.5684506 = 430.48092209, from lines 200 and 207						

THIS IS **EXHIBIT "3"** TO
THE AFFIDAVIT OF **LAURENCE DAY**
SWORN BEFORE ME
THIS 9th DAY OF DECEMBER, 2021

Stephen Ayford

A COMMISSIONER ETC.

Indexed Finance

Index Pools

Summary

Index pools are tokenized portfolios that double as AMMs. The pool contract is designed to be able to radically change the composition of its portfolio without needing to access external liquidity.

The Index Pool contract is a fork of the Balancer Pool. The primary changes made to the contract were to enable more dynamic pool management so that assets can be bound, rebound and reweighed gradually and without the need to access external liquidity.

> It may be useful to read the Balancer Whitepaper or documentation for additional context on the pool contract.

Rebalancing

The typical method for rebalancing a token portfolio is to sell and purchase sufficient amounts of each asset to reach the desired weights. This typically involves trading with on-chain exchanges or using an auction system. Any method of swapping on-chain to rebalance will cause some amount of loss for the pool, potentially quite a lot. On-chain exchanges are illiquid, and auctions on Ethereum have a history of being exploited.

Index pools rebalance themselves over time by incentivizing traders to gradually adjust token balances and weights. As tokens are swapped, their weights move slightly toward the targets set by the pool controller. These weight adjustments occurs at a maximum of once every thirty minutes in order, creating small arbitrage opportunities over time that eventually bring the portfolio composition in line with its desired weights.

While this rebalancing process is not instantaneous, it is permissionless, it works for arbitrarily large pools, it is generally more gas efficient and it does not assume that the pool or its controller can access external liquidity to execute rebalances.

For further details on the rebalancing process, see Rebalancing.

Indexed Finance

Limitations

Abnormal token implementations

Tokens that have internal transfer fees or other non-standard balance updates may create arbitrage opportunities. For now, these tokens should not be used in Indexed pools. Indexed pools do not have the same ERC20 restrictions on return values as Balancer pools, as the pool contract uses methods from OpenZeppelin's `SafeERC20` library.

Permanent loss for some liquidity providers due to unbound token handling

While the selling of a pool's unbound tokens is restricted to a small range around their moving average prices, it is still possible for a liquidity provider to experience permanent loss due to the way that unbound tokens are handled. If an LP exits a pool after a token is removed from the pool, but before its balance is swapped to the other underlying assets, the LP will suffer a loss of around 1% of their pool tokens' value (as 1% is the minimum weight of the pool).

Swap input amount

When a token is sold to a pool, the input amount can not exceed half of the pool's current balance in that token. This restriction applies to swaps and single-asset liquidity providing functions, but does not apply to all-asset liquidity providing. This only applies to an individual call to the contract, and can be bypassed with multiple calls.

Swap output amount

When a token is purchased from a pool, the output amount can not exceed one third of the pool's current balance in that token. This restriction applies to swaps and single-asset liquidity removal functions, but does not apply to all-asset liquidity removal. This only applies to an individual call to the contract, and can be bypassed with multiple calls.

Minimum balance

When a pool is first initialized, it must have a balance of at least 1e6 wei. This does not apply to tokens after the pool is initialized

←
Index Pool Protocol - Previous
Index Controller

THIS IS **EXHIBIT "4"** TO
THE AFFIDAVIT OF **LAURENCE DAY**
SWORN BEFORE ME
THIS 9th DAY OF DECEMBER, 2021

Stephen Axford

A COMMISSIONER ETC.

Address 0xBA5Ed1488bE60BA2FACC6B66C6D6F0beFba22eBe

Buy Exchange Earn Gaming

This address is reported to be involved in a Indexed Finance exploit.

Overview	Indexed Finance Exploiter
Balance:	9.339599705334888488 Ether
Ether Value:	$42,362.00 (@ $4,535.74/ETH)
Token:	$16,061,274.90 18

More Info	More
My Name Tag:	Not Available, login to update

Token Holdings 0xBA5Ed1488bE60BA2FACC6B66C6D6F0beFba22eBe Indexed Finance Exploiter

Overview

Net Worth in USD	Net Worth in ETH	Total Balance Change (24H)
$16,099,560.91	3,547.940578	0.84%

Hide $0.00 assets

Show/Hide value in ETH

Assets in Wallet (19)	Liquidity Pool Assets in Wallet (0)	NFT Assets (0)
$16,099,560.91	-	-

Assets in Wallet (19)

$16,099,560.91

Search Token Name

Asset	Symbol	Contract Address	Quantity	Price	Change (24H)	Value	
Ethereum	ETH	-	9.339599705334888488	$4,537.72	0.66%	$42,380.49	More
Uniswap	UNI	0x1f9840a85d5af5bf1d1...	226961.159743031121...	$22.66	7.84%	$5,142,939.88	More
Curve DAO To...	CRV	0xD533a949740bb3306...	845805.567102589260...	$4.775617	0.04%	$4,039,243.42	More
Aave Token	AAVE	0x7fc66500c84a76ad7e...	7500.47470638181558...	$245.282947	0.03%	$1,839,738.54	More
Compound	COMP	0xc00e94cb662c352028...	6462.00495392958612...	$271.51	0.01%	$1,754,498.97	More
Maker	MKR	0x9f8f72aa9304c8b593d...	516.220951113920494...	$2,978.45	0.04%	$1,537,538.29	More
ChainLink To...	LINK	0x514910771af9ca656af...	33215.4337308464116...	$24.76	2.24%	$822,414.14	More
Synthetix Ne...	SNX	0xc011a73ee8576fb46f5...	45434.8115089067953...	$7.30	0.38%	$331,674.12	More
UMA Voting T...	UMA	0x04Fa0d235C4abf4BcF...	17844.0277186979933...	$12.53	2.92%	$223,585.67	More
BAT	BAT	0x0d8775f648430679a7...	131645.480415574792...	$1.44	2.72%	$189,569.49	More
yearn.financ...	YFI	0x0bc529c00C6401aEF...	5.248968861704032049	$29,022.00	0.05%	$152,335.57	More
DEGEN Index	DEGEN	0x126c121f99e1e211df2...	1041.82625612561787...	$6.887303	5.36%	$7,175.37	More
Reserve Righ...	RSR	0x8762db106b2c2a0bcc...	72152.5216579587296...	$0.051175	–	$3,692.41	More
Republic	REN	0x408e41876cccdc0f922...	3684.07355522966738...	$0.903585	0.05%	$3,328.87	More
1INCH Token	1INCH	0x111111111117dc0aa78...	754	$3.49	4.04%	$2,631.46	More
Wootrade Net...	WOO	0x4691937a7508860f87...	2440.74035699277641...	$0.995982	4.17%	$2,430.88	More
AlphaToken	ALPHA	0xa1faa113cbe53436df2...	2453.07682156569481...	$0.940063	0.17%	$2,306.05	More
Wrapped Ethe...	WETH	0xc02aaa39b223fe8d0a...	0.457827856286366182	$4,537.27	1.32%	$2,077.29	More

Transactions

For 0xba5ed1488be60ba2facc6b66c6d6f0befba22ebe Indexed Finance Exploiter

Featured: Curious on Ethereum's hottest 🔥 trading pairs? View top pairs and details with **DEX Trading Pairs!**

A total of 32 transactions found

First < Page 1 of 1 > Last

Txn Hash	Method	Block	Age	From		To	Value	Txn Fee
0xcbe60bc03c216894a3...	Transfer*	13468000	41 days 7 hrs ago	0xf926c5c0b9ddfe3c382f...	IN	Indexed Finance Exploiter	0 Ether	0.00328472
0x906b22056753bbcbb9...	Transfer*	13455125	43 days 7 hrs ago	blockanalia.eth	IN	Indexed Finance Exploiter	0.000001 Ether	0.00305188
0xe925ad11917d6e3af0c...	Transfer*	13433777	46 days 15 hrs ago	0xf926c5c0b9ddfe3c382f...	IN	Indexed Finance Exploiter	0 Ether	0.00248095
0x858e559bb712eb9193...	Transfer*	13429394	47 days 8 hrs ago	Indexed: Deployer	IN	Indexed Finance Exploiter	0 Ether	0.00265554
0xc2e8176e205b5c9731...	Transfer*	13427810	47 days 14 hrs ago	Indexed: Deployer	IN	Indexed Finance Exploiter	0 Ether	0.00380076
0xafce1ac07285b29242...	Transfer*	13426366	47 days 19 hrs ago	Indexed: Deployer	IN	Indexed Finance Exploiter	0 Ether	0.00235656
0xae4c1129425972e090...	0x6ead8989	13421549	48 days 13 hrs ago	Indexed Finance Exploiter	OUT	0xacc4caa999700a26ac...	0 Ether	0.0721104
0x67218c68212ef17dc1...	Transfer*	13421493	48 days 14 hrs ago	Indexed Finance Exploiter	OUT	Contract Creation	0 Ether	0.21708372
0x3091a1c5304a58257d...	Approve	13418219	49 days 2 hrs ago	Indexed Finance Exploiter	OUT	Indexed: DEGEN Token	0 Ether	0.01219276
0x50af8eb95eeebf2ceb8...	Transfer*	13418219	49 days 2 hrs ago	Future Of Finance Fund: ...	IN	Indexed Finance Exploiter	0 Ether	0.00483651
0x9f94f34f92b7e9d9128...	Exitswap Extern ...	13418216	49 days 2 hrs ago	Indexed Finance Exploiter	OUT	Indexed: DEGEN Token	0 Ether	0.02109245
0xd93c18a9c447ba90fb...	Transfer*	13418214	49 days 2 hrs ago	yannickcrypto.eth	IN	Indexed Finance Exploiter	0 Ether	0.00315212
0x8bc85b3e2073096c21...	Exitswap Pool Am...	13418211	49 days 2 hrs ago	Indexed Finance Exploiter	OUT	Indexed: DEGEN Token	0 Ether	0.01710731
0x32ebd0d2c168ab3abf...	Exitswap Pool Am...	13418203	49 days 2 hrs ago	Indexed Finance Exploiter	OUT	Indexed: DEGEN Token	0 Ether	0.02031166
0x566d1aa1adcc6c87bc...	Exitswap Extern ...	13418203	49 days 2 hrs ago	Indexed Finance Exploiter	OUT	Indexed: DEGEN Token	0 Ether	0.016513
0xe4b475a3f237547681...	Exitswap Extern ...	13418203	49 days 2 hrs ago	Indexed Finance Exploiter	OUT	Indexed: DEGEN Token	0 Ether	0.0193451
0xc29ca5f8f1aeeb3a08e...	Exitswap Pool Am...	13418202	49 days 2 hrs ago	Indexed Finance Exploiter	OUT	Indexed: DEGEN Token	0 Ether	0.01524583
0xee771b904c54e6e3b5...	Exitswap Pool Am...	13418189	49 days 2 hrs ago	Indexed Finance Exploiter	OUT	Indexed: DEGEN Token	0 Ether	0.01567254
0xf7b3d73ea632ef65607...	0x3b1aa27c	13418053	49 days 3 hrs ago	Indexed Finance Exploiter	OUT	0xb634c72a62e936a5bf...	0 Ether	0.55078275
0x93b470dd725bb90cea...	0x3b1aa27c	13418022	49 days 3 hrs ago	Indexed Finance Exploiter	OUT	0xb634c72a62e936a5bf...	0 Ether	0.54294275
0xa90c8419ea93e1e19b...	0x3b1aa27c	13418012	49 days 3 hrs ago	Indexed Finance Exploiter	OUT	0xb634c72a62e936a5bf...	0 Ether	0.6247095
0xcef6e3a806c95928fcb...	0x3b1aa27c	13417997	49 days 3 hrs ago	Indexed Finance Exploiter	OUT	0xb634c72a62e936a5bf...	0 Ether	0.4900436
0xbe11d89770e0b9b1fb...	0x3b1aa27c	13417982	49 days 3 hrs ago	Indexed Finance Exploiter	OUT	0xb634c72a62e936a5bf...	0 Ether	0.5240872
0xc2a5c08b8e72cc22f27...	0x3b1aa27c	13417978	49 days 3 hrs ago	Indexed Finance Exploiter	OUT	0xb634c72a62e936a5bf...	0 Ether	0.259848
0xdb1cdc500752b8bd87...	0x3b1aa27c	13417960	49 days 3 hrs ago	Indexed Finance Exploiter	OUT	0xb634c72a62e936a5bf...	0 Ether	0.5704634
0xbde4521c5ac08d0033...	0x92501db3	13417956	49 days 3 hrs ago	Indexed Finance Exploiter	OUT	0xfbc2e6b188013fc5eac...	0 Ether	2.4055404
0x44aad3b85386646816...	0x807a994a	13417949	49 days 3 hrs ago	Indexed Finance Exploiter	OUT	0x277e851587eb5da22b...	0 Ether	0.9393837
0x89ff7a0c417870bfc8e5...	Transfer*	13417320	49 days 6 hrs ago	Indexed Finance Exploiter	OUT	Contract Creation	0 Ether	0.27541008
0xd76d06a81b8e29f034...	Transfer*	13417302	49 days 6 hrs ago	Indexed Finance Exploiter	OUT	Contract Creation	0 Ether	0.41615321
0x9d79a5a7648f44e74b...	Transfer*	13416332	49 days 9 hrs ago	Indexed Finance Exploiter	OUT	Contract Creation	0 Ether	0.25083828
0x05a135501fe28d2178...	Lock In	13414857	49 days 15 hrs ago	Indexed Finance Exploiter	OUT	0x7b9175d5c08642c6c2...	0 Ether	0.02570386
0xf57a9218cf3ce054c17...	Transfer*	13414665	49 days 16 hrs ago	Indexed Finance Exploiter	OUT	Contract Creation	0 Ether	0.20817234

Show 50 Records

First < Page 1 of 1 > Last

Transactions	Internal Txns	Erc20 Token Txns	Analytics	Comments

Latest 4 internal transactions

Parent Txn Hash	Block	Age	From		To	Value
0x44aad3b85386646816...	13417949	49 days 3 hrs ago	Uniswap V2: Router 2	→	Indexed Finance Exploiter	15 Ether
0x14ba74b734ea0d13b1...	13417464	49 days 5 hrs ago	Tornado.Cash: 1 ETH	→	Indexed Finance Exploiter	0.9279503 Ether
0x0fff3e26653bfaa6e8c6...	13416974	49 days 7 hrs ago	Tornado.Cash: 1 ETH	→	Indexed Finance Exploiter	0.9521384 Ether
0xbceef471c174aef7f75...	13414635	49 days 16 hrs ago	Tornado.Cash: 1 ETH	→	Indexed Finance Exploiter	0.9702639 Ether

[Download CSV Export]

THIS IS **EXHIBIT "5"** TO
THE AFFIDAVIT OF **LAURENCE DAY**
SWORN BEFORE ME
THIS 9th DAY OF DECEMBER, 2021

Stephen Gifford

A COMMISSIONER ETC.

CC10 Phase Appendices

Appendix B1: Pre-Attack Balance

Token	Balance	Etherscan Price	Etherscan Value
LINK	35,076.68	$26.65	$934,793.57
UNI	36,295.10	$26.29	$954,198.26
AAVE	1,335.97	$303.43	$405,372.21
COMP	1,051.51	$314.38	$330,572.65
SNX	30,160.67	$9.92	$299,193.86
CRV	130,269.07	$2.88	$375,174.93
YFI	5.51	$35,234.66	$193,992.08
UMA	18,716.85	$10.27	$192,222.07
MKR	115.02	$2,542.91	$292,475.47
BAT	138,084.80	$0.70	$96,659.36
SUSHI	2,430.48	$10.75	$26,127.62
			$4,100,782.07

Appendix B2: List of Flash Loaned Assets (Step 2)

Token	**Balance**	**Etherscan Price**	**Etherscan Value**
LINK	315,690.14	$26.65	$8,413,142.23
UNI	326,655.93	$26.29	$8,587,784.40
AAVE	12,023.7	$303.43	$3,648,351.29
COMP	9,463.56	$314.38	$2,975,153.99
SNX	271,446.04	$9.92	$2,692,744.72
CRV	1,172,421.66	$2.88	$3,376,574.38
YFI	49.55	$35,234.66	$1,745,877.40
UMA	168,451.67	$10.27	$1,729,998.65
MKR	1,035.14	$2,542.91	$2,632,267.86
BAT	1,242,763.18	$0.70	$869,934.23
SUSHI	0	$10.75	0
			$36,671,829.15

**16,000 SUSHI tokens ($172,000) were later borrowed as part of Step 5*

Appendix B3: Swap $9.3M LINK for 521K CC10 (Step 5)

1) Swap 10.615164060631073077 ($282.87) LINK for 6,268.604642839128891779 CC10
2) Swap 15.922746090946609616 ($424.30) LINK for 6,870.353415306510502799 CC10
3) Swap 23.884119136419914424 ($636.45) LINK for 7,529.866491920851412303 CC10
4) Swap 35.826178704629871636 ($954.68) LINK for 8,252.688902412583333213 CC10
5) Swap 53.739268056944807454 ($1,432.02) LINK for 9,044.89796639540475592 CC10
6) Swap 80.608902085417211181 ($2,148.02) LINK for 9,913.154390030068556243 CC10
7) Swap 120.913353128125816771 ($3,222.04) LINK for 10,864.758267664071456667 CC10
8) Swap 181.370029692188725157 ($4,833.06) LINK for 11,907.710459295766836652 CC10
9) Swap 272.055044538283087735 ($7,249.58) LINK for 13,050.779859910080776888 CC10
10) Swap 408.082566807424631603 ($10,874.37) LINK for 14,303.577126270472064769 CC10
11) Swap 612.123850211136947404 ($16,311.56) LINK for 15,676.6354810445394209 CC10
12) Swap 918.185775316705421106 ($24,467.34) LINK for 17,181.499273645224116268 CC10
13) Swap 1,377.278662975058131659 ($36,701.01) LINK for 18,830.821042386183555752 CC10
14) Swap 2,065.917994462587197489 ($55,051.52) LINK for 20,638.467894026947261249 CC10
15) Swap 3,098.876991693880796233 ($82,577.28) LINK for 22,619.638095121872983855 CC10
16) Swap 4,648.31548754082119435 ($123,865.92) LINK for 24,790.988855445348173403 CC10
17) Swap 6,972.473231311231791525 ($185,798.88) LINK for 27,170.776377866008056538 CC10
18) Swap 10,458.709846966847687287 ($278,698.32) LINK for 29,779.009352176139373232 CC10
19) Swap 15,688.064770450271530931 ($418,047.48) LINK for 32,637.617183416029575844 CC10
20) Swap 23,532.097155675407296396 ($627,071.23) LINK for 35,770.634369117164661472 CC10
21) Swap 35,298.145733513110944594 ($940,606.84) LINK for 39,204.402575664463320732 CC10
22) Swap 52,947.218600269666416891 ($1,410,910.26) LINK for 42,967.792112787735583168 CC10
23) Swap 79,420.827900404499625337 ($2,116,365.39) LINK for 47,092.444668287429857168 CC10
24) Swap 112,504.335602853918504119 ($2,997,957.69) LINK for 49,119.242500304842552512 CC10

Note that the amount of LINK is increasing by ~50% each time, in order to counteract the 50% Swap-In Limit. The price of LINK increases with each swap.

Appendix B4: Burn 521K CC10 for $36M (Step 7)

In exchange for 521,486.3613 CC10 minted via 350,745.588976 ($9,347,369.95) LINK, the Attacker received:

Token	Balance	Etherscan Price	Etherscan Value
LINK	310,172.32	$26.65	$8,266,092.33
UNI	320,946.45	$26.29	$8,437,682.17
AAVE	11,813.54	$303.43	$3,584,582.44
COMP	9,298.15	$314.38	$2,923,152.40
SNX	266,701.55	$9.92	$2,645,679.38
CRV	1,151,929.39	$2.88	$3,317,556.64
YFI	48.69	$35,234.66	$1,715,575.60
UMA	165,507.37	$10.27	$1,699,760.69
MKR	1,017.05	$2,542.91	$2,586,266.62
BAT	1,221,041.44	$0.70	$854,729.01
SUSHI	16,297.5	$10.75	$175,198.13
			$36,206,275.39

Appendix B5: Mint CC10 Using SUSHI – 1st Cycle (Step 8)

1) Swap 1,066.486180545414585056 ($11,469.34) SUSHI for 33,421.813688619695456165 CC10
2) Swap 1,599.729270818121877584 ($17,204.01) SUSHI for 49,870.448895836515372331 CC10
3) Swap 2,399.593906227182816376 ($25,806.01) SUSHI for 74,414.324017343774197136 CC10
4) Swap 3,599.390859340774224564 ($38,709.02) SUSHI for 111,037.533079445160554949 CC10
5) Swap 5,399.086289011161336846 ($58,063.53) SUSHI for 165,684.952664426218170813 CC10
6) Swap 2,233.217803388302911663 ($24,016.75) SUSHI for 68,304.118905513278944144 CC10

Total: 16,297.5043093 (US$175,268.66) SUSHI swapped for 502,733.191251184642695538 CC10

Appendix B6: Burn CC10 – 1st Cycle (Step 9)

In exchange for 502,733.191251184642695538 CC10 minted via 16,297.5043093 ($175,268.66) SUSHI, the Attacker received:

Token	Balance	Etherscan Price	Etherscan Value
LINK	35,584.72	$26.65	$948,332.79
UNI	36,820.79	$26.29	$968,018.57
AAVE	1,355.32	$303.43	$411,244.75
COMP	1,066.74	$314.38	$335,361.72
SNX	30,597.51	$9.92	$303,527.30
CRV	132,155.85	$2.88	$380,608.85
YFI	5.59	$35,234.66	$196,961.75
UMA	18,987.94	$10.27	$195,006.14
MKR	116.68	$2,542.91	$296,706.74
BAT	140,084.78	$0.70	$98,059.35
SUSHI	16,155.97	$10.75	$173,676.68
			$4,307,504.63

Appendix B7: Mint CC10 From SUSHI – 2nd Cycle (Step 10)

1) Swap 1,137.254180127757720285 ($12,230.40) SUSHI for 34,658.921127864746812523 CC10
2) Swap 1,705.881270191636580427 ($18,345.60) SUSHI for 51,716.402077860775697571 CC10
3) Swap 2,558.821905287454870641 ($27,518.40) SUSHI for 77,168.768006707346103106 CC10
4) Swap 3,838.232857931182305961 ($41,277.61) SUSHI for 115,147.584062548261881913 CC10
5) Swap 5,757.349286896773458942 ($61,916.41) SUSHI for 171,817.776257477341312891 CC10
6) Swap 1,158.428809731466545375 ($12,458.12) SUSHI for 34,470.782002099094659965 CC10

Total: 16,155.9683102 (US$173,746.54) SUSHI swapped for 484,980.233534557566467969 CC10

Appendix B8: Burn CC10 – 2nd Cycle (Step 10)

In exchange for 484,980.233534557566467969 CC10 minted via 16,155.9683102 ($173,746.54) of SUSHI, the Attacker received:

Token	Balance	Etherscan Price	Etherscan Value
LINK	4,352.68	$26.65	$115,998.92
UNI	4,503.87	$26.29	$118,406.74
AAVE	165.78	$303.43	$50,302.63
COMP	130.48	$314.38	$41,020.30
SNX	3,742.65	$9.92	$37,127.09
CRV	16,165.14	$2.88	$46,555.60
YFI	0.68	$35,234.66	$23,959.57
UMA	2,322.58	$10.27	$23,852.90
MKR	14.27	$2,542.91	$36,287.33
BAT	17,135	$0.70	$11,994.50
SUSHI	16,013.09	$10.75	$172,140.72
			$677,646.29

Appendix B9: Net Tokens Routed to Attacker's Wallet (Step 11)

Token	Balance	Etherscan Price	Etherscan Value
LINK	33,215.43	$26.65	$885,191.21
UNI	34,602.55	$26.29	$909,701.04
AAVE	1,273.67	$303.43	$386,469.69
COMP	1,002.47	$314.38	$315,156.52
SNX	28,754.17	$9.92	$285,241.37
CRV	124,194.23	$2.88	$357,679.38
YFI	5.25	$35,234.66	$184,981.97
UMA	17,844.03	$10.27	$183,258.19
MKR	109.65	$2,542.91	$278,830.08
BAT	131,645.48	$0.70	$92,151.84
			$3,878,661.28

Appendix B10: CC10 Token Balances Post-Attack

Token	**Balance**	**Etherscan Price**	**Etherscan Value**
LINK	657.09	$26.65	$17,511.45
UNI	679.92	$26.29	$17,875.10
AAVE	25.03	$303.43	$7,594.85
COMP	19.70	$314.38	$6,193.29
SNX	565.00	$9.92	$5,604.80
CRV	2,440.34	$2.88	$7,028.18
YFI	0.10	$35,234.66	$3,523.47
UMA	350.62	$10.27	$3,600.87
MKR	2.15	$2,542.91	$5,467.26
BAT	2,586.75	$0.70	$1,810.73
SUSHI	2,417.38	$10.75	$25,986.84
			$102,196.81

Total CC10 NAV Before Attack = $4,100,782.07

- Total CC10 NAV After Attack = $102,196.81

= **Loss to CC10 Pool NAV** = **$3,998,585.26**

THIS IS **EXHIBIT "6"** TO
THE AFFIDAVIT OF **LAURENCE DAY**
SWORN BEFORE ME
THIS 9th DAY OF DECEMBER, 2021

Stephen Axford

A COMMISSIONER ETC.

CC10 Transaction Log

#	EVENT ACTION	EVENT LOG	FROM	TO	AMOUNT	EST. USD VALUE	TOKEN
1	Flash Loan	54	SushiSwap: LINK	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	315,690.14	$8,412,348.48	ChainLink To... (L NK)
2	Flash Loan	56	Uniswap V2: UNI 30	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	326,655 93	$8,586,814.86	Uniswap (UNI)
3	Flash Loan	62	SushiSwap: AAVE	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	12,023.70	$3,648,333.12	Aave Token (AAVE)
4	Flash Loan	64	SushiSwap: COMP	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	9,463 56	$2,975,163.91	Compound (COMP)
5	Flash Loan	66	SushiSwap: CRV	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	1,172,421 66	$3,376,068.34	Curve DAO To... (CRV)
6	Flash Loan	68	SushiSwap: MKR	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	1,035.14	$2,632,282.23	Maker (MKR)
7	Flash Loan	70	SushiSwap: SNX	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	271,446 04	$2,693,363.11	Synthetix Ne... (SNX)
8	Flash Loan	72	SushiSwap: YFI	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	49.551456	$1,745,928.65	yearn.financ... (YFI)
9	Flash Loan	74	SushiSwap: UMA	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	168,451 67	$1,730,799.55	UMA Voting T... (UMA)
10	Flash Loan	76	Uniswap V2: BAT 2	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	1,242,763.18	$873,211.53	BAT (BAT)
11	Swap In UNI	77	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	18,147 55	$477,045.27	Uniswap (UNI)
12	Swap Out L NK	79	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	11,260 24	$300,057.18	ChainLink To... (L NK)
13	Swap In UNI	81	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	18,147 55	$477,045.27	Uniswap (UNI)
14	Swap Out L NK	83	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	5,715 93	$152,315.12	ChainLink To... (L NK)
15	Swap In UNI	85	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	18,147 55	$477,045.27	Uniswap (UNI)
16	Swap Out L NK	87	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	3,468 85	$92,436.17	ChainLink To... (L NK)
17	Swap In UNI	89	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	18,147 55	$477,045.27	Uniswap (UNI)
18	Swap Out L NK	91	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	2,333 88	$62,192.13	ChainLink To... (L NK)
19	Swap In UNI	93	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	18,147 55	$477,045.27	Uniswap (UNI)
20	Swap Out L NK	95	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	1,679 93	$44,766.02	ChainLink To... (L NK)
21	Swap In UNI	97	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	18,147 55	$477,045.27	Uniswap (UNI)
22	Swap Out L NK	99	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	1,268 33	$33,797.81	ChainLink To... (L NK)
23	Swap In UNI	101	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	18,147 55	$477,045.27	Uniswap (UNI)
24	Swap Out L NK	103	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	992.242017	$26,440.76	ChainLink To... (L NK)
25	Swap In UNI	105	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	18,147 55	$477,045.27	Uniswap (UNI)
26	Swap Out L NK	107	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	797 9294586	$21,262.81	ChainLink To... (L NK)
27	Swap In UNI	109	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	18,147 55	$477,045.27	Uniswap (UNI)
28	Swap Out L NK	111	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	655 9213545	$17,478.66	ChainLink To... (L NK)
29	Swap In UNI	113	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	18,147 55	$477,045.27	Uniswap (UNI)
30	Swap Out L NK	115	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	548 9434436	$14,627.96	ChainLink To... (L NK)
31	Swap In UNI	117	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	18,147 55	$477,045.27	Uniswap (UNI)
32	Swap Out L NK	119	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	466 3189887	$12,426.23	ChainLink To... (L NK)
33	Swap In UNI	121	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	18,147 55	$477,045.27	Uniswap (UNI)
34	Swap Out L NK	123	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	401.1569533	$10,689.82	ChainLink To... (L NK)
35	Swap In UNI	125	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	18,147 55	$477,045.27	Uniswap (UNI)
36	Swap Out L NK	127	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	348 8463937	$9,295.88	ChainLink To... (L NK)
37	Swap In UNI	129	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	18,147 55	$477,045.27	Uniswap (UNI)
38	Swap Out L NK	131	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	306 2064532	$8,159.63	ChainLink To... (L NK)
39	Swap In UNI	133	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	18,147 55	$477,045.27	Uniswap (UNI)
40	Swap Out L NK	135	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	270.984663	$7,221.06	ChainLink To... (L NK)
41	Swap In UNI	137	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	18,147 55	$477,045.27	Uniswap (UNI)
42	Swap Out L NK	139	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	241 5493786	$6,436.68	ChainLink To... (L NK)
43	Swap In UNI	141	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	18,147 55	$477,045.27	Uniswap (UNI)
44	Swap Out L NK	143	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	216 6949543	$5,774.38	ChainLink To... (L NK)
45	Swap In UNI	145	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	18,147 55	$477,045.27	Uniswap (UNI)
46	Swap Out L NK	147	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	195 5147541	$5,209.98	ChainLink To... (L NK)
47	Swap In AAVE	153	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	667.983072	$202,685.17	Aave Token (AAVE)
48	Swap Out L NK	155	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	611 5474069	$16,296.20	ChainLink To... (L NK)
49	Swap In AAVE	161	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	667.983072	$202,685.17	Aave Token (AAVE)
50	Swap Out L NK	163	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	374 5905543	$9,981.90	ChainLink To... (L NK)
51	Swap In AAVE	169	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	667.983072	$202,685.17	Aave Token (AAVE)
52	Swap Out L NK	171	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	260 8397697	$6,950.72	ChainLink To... (L NK)

53	Swap In AAVE	177	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	667.983072	$202,685.17	Aave Token (AAVE)	
54	Swap Out L NK	179	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	195 6672551	$5,214.04	ChainLink To... (L NK)	
55	Swap In AAVE	185	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	667.983072	$202,685.17	Aave Token (AAVE)	
56	Swap Out L NK	187	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	154.1250238	$4,107.04	ChainLink To... (L NK)	
57	Swap In AAVE	193	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	667.983072	$202,685.17	Aave Token (AAVE)	
58	Swap Out L NK	195	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	125.673279	$3,348.88	ChainLink To... (L NK)	
59	Swap In AAVE	201	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	667.983072	$202,685.17	Aave Token (AAVE)	
60	Swap Out L NK	203	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	105.1503841	$2,801.99	ChainLink To... (L NK)	
61	Swap In AAVE	209	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	667.983072	$202,685.17	Aave Token (AAVE)	
62	Swap Out L NK	211	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	89.75442479	$2,391.73	ChainLink To... (L NK)	
63	Swap In AAVE	217	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	667.983072	$202,685.17	Aave Token (AAVE)	
64	Swap Out L NK	219	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	77.84384436	$2,074.34	ChainLink To... (L NK)	
65	Swap In AAVE	225	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	667.983072	$202,685.17	Aave Token (AAVE)	
66	Swap Out L NK	227	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	68.39846727	$1,822.65	ChainLink To... (L NK)	
67	Swap In AAVE	233	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	667.983072	$202,685.17	Aave Token (AAVE)	
68	Swap Out L NK	235	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	60.75373844	$1,618.93	ChainLink To... (L NK)	
69	Swap In AAVE	241	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	667.983072	$202,685.17	Aave Token (AAVE)	
70	Swap Out L NK	243	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	54.459784	$1,451.22	ChainLink To... (L NK)	
71	Swap In AAVE	249	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	667.983072	$202,685.17	Aave Token (AAVE)	
72	Swap Out L NK	251	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	49.20214104	$1,311.11	ChainLink To... (L NK)	
73	Swap In AAVE	257	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	667.983072	$202,685.17	Aave Token (AAVE)	
74	Swap Out L NK	259	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	44.75495366	$1,192.61	ChainLink To... (L NK)	
75	Swap In AAVE	265	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	667.983072	$202,685.17	Aave Token (AAVE)	
76	Swap Out L NK	267	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	40 9521859	$1,091.27	ChainLink To... (L NK)	
77	Swap In AAVE	273	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	667.983072	$202,685.17	Aave Token (AAVE)	
78	Swap Out L NK	275	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	37.66928818	$1,003.79	ChainLink To... (L NK)	
79	Swap In AAVE	281	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	667.983072	$202,685.17	Aave Token (AAVE)	
80	Swap Out L NK	283	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	34.81116403	$927.63	ChainLink To... (L NK)	
81	Swap In AAVE	289	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	667.983072	$202,685.17	Aave Token (AAVE)	
82	Swap Out L NK	291	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	32.30406172	$860.82	ChainLink To... (L NK)	
83	Swap In COMP	293	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	525.7533052	$165,286.88	Compound (COMP)	
84	Swap Out L NK	295	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	191 8736743	$5,112.95	ChainLink To... (L NK)	
85	Swap In COMP	297	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	525.7533052	$165,286.88	Compound (COMP)	
86	Swap Out L NK	299	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	120 8349336	$3,219.95	ChainLink To... (L NK)	
87	Swap In COMP	301	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	525.7533052	$165,286.88	Compound (COMP)	
88	Swap Out L NK	303	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	85.87236549	$2,288.28	ChainLink To... (L NK)	
89	Swap In COMP	305	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	525.7533052	$165,286.88	Compound (COMP)	
90	Swap Out L NK	307	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	65.46418773	$1,744.46	ChainLink To... (L NK)	
91	Swap In COMP	309	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	525.7533052	$165,286.88	Compound (COMP)	
92	Swap Out L NK	311	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	52.25961509	$1,392.59	ChainLink To... (L NK)	
93	Swap In COMP	313	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	525.7533052	$165,286.88	Compound (COMP)	
94	Swap Out L NK	315	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	43.10204014	$1,148.56	ChainLink To... (L NK)	
95	Swap In COMP	317	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	525.7533052	$165,286.88	Compound (COMP)	
96	Swap Out L NK	319	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	36.42489025	$970.63	ChainLink To... (L NK)	
97	Swap In COMP	321	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	525.7533052	$165,286.88	Compound (COMP)	
98	Swap Out L NK	323	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	31.36814237	$835.88	ChainLink To... (L NK)	
99	Swap In COMP	325	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	525.7533052	$165,286.88	Compound (COMP)	
100	Swap Out L NK	327	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	27.42297586	$730.75	ChainLink To... (L NK)	
101	Swap In COMP	329	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	525.7533052	$165,286.88	Compound (COMP)	
102	Swap Out L NK	331	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	24.27041987	$646.75	ChainLink To... (L NK)	
103	Swap In COMP	333	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	525.7533052	$165,286.88	Compound (COMP)	
104	Swap Out L NK	335	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	21.70106748	$578.28	ChainLink To... (L NK)	
105	Swap In COMP	337	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	525.7533052	$165,286.88	Compound (COMP)	

106	Swap Out L NK		339	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	19.57215305	$521.55	ChainLink To... (L NK)
107	Swap In COMP		341	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	525.7533052	$165,286.88	Compound (COMP)
108	Swap Out L NK		343	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	17.78323402	$473.88	ChainLink To... (L NK)
109	Swap In COMP		345	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	525.7533052	$165,286.88	Compound (COMP)
110	Swap Out L NK		347	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	16.26173687	$433.33	ChainLink To... (L NK)
111	Swap In COMP		349	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	525.7533052	$165,286.88	Compound (COMP)
112	Swap Out L NK		351	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	14.95401254	$398.49	ChainLink To... (L NK)
113	Swap In COMP		353	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	525.7533052	$165,286.88	Compound (COMP)
114	Swap Out L NK		355	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	13.81960768	$368.26	ChainLink To... (L NK)
115	Swap In COMP		357	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	525.7533052	$165,286.88	Compound (COMP)
116	Swap Out L NK		359	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	12.82748459	$341.82	ChainLink To... (L NK)
117	Swap In COMP		361	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	525.7533052	$165,286.88	Compound (COMP)
118	Swap Out L NK		363	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	11.95346164	$318.53	ChainLink To... (L NK)
119	Swap In CRV		365	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	65,134 54	$187,559.35	Curve DAO To... (CRV)
120	Swap Out L NK		366	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	102 5809579	$2,733.52	ChainLink To... (L NK)
121	Swap In CRV		368	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	65,134 54	$187,559.35	Curve DAO To... (CRV)
122	Swap Out L NK		369	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	63.21036963	$1,684.40	ChainLink To... (L NK)
123	Swap In CRV		371	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	65,134 54	$187,559.35	Curve DAO To... (CRV)
124	Swap Out L NK		372	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	44.20884914	$1,178.05	ChainLink To... (L NK)
125	Swap In CRV		374	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	65,134 54	$187,559.35	Curve DAO To... (CRV)
126	Swap Out L NK		375	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	33.27833588	$886.78	ChainLink To... (L NK)
127	Swap In CRV		377	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	65,134 54	$187,559.35	Curve DAO To... (CRV)
128	Swap Out L NK		378	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	26.28854636	$700.52	ChainLink To... (L NK)
129	Swap In CRV		380	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	65,134 54	$187,559.35	Curve DAO To... (CRV)
130	Swap Out L NK		381	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	21.48841024	$572.61	ChainLink To... (L NK)
131	Swap In CRV		383	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	65,134 54	$187,559.35	Curve DAO To... (CRV)
132	Swap Out L NK		384	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	18.01792008	$480.13	ChainLink To... (L NK)
133	Swap In CRV		386	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	65,134 54	$187,559.35	Curve DAO To... (CRV)
134	Swap Out L NK		387	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	15.40910072	$410.61	ChainLink To... (L NK)
135	Swap In CRV		389	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	65,134 54	$187,559.35	Curve DAO To... (CRV)
136	Swap Out L NK		390	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	13.38720099	$356.74	ChainLink To... (L NK)
137	Swap In CRV		392	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	65,134 54	$187,559.35	Curve DAO To... (CRV)
138	Swap Out L NK		393	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	11.78115263	$313.94	ChainLink To... (L NK)
139	Swap In CRV		395	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	65,134 54	$187,559.35	Curve DAO To... (CRV)
140	Swap Out L NK		396	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	10.47933257	$279.25	ChainLink To... (L NK)
141	Swap In CRV		398	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	65,134 54	$187,559.35	Curve DAO To... (CRV)
142	Swap Out L NK		399	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	9.406061864	$250.65	ChainLink To... (L NK)
143	Swap In CRV		401	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	65,134 54	$187,559.35	Curve DAO To... (CRV)
144	Swap Out L NK		402	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	8.508366877	$226.73	ChainLink To... (L NK)
145	Swap In CRV		404	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	65,134 54	$187,559.35	Curve DAO To... (CRV)
146	Swap Out L NK		405	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	7.748151467	$206.47	ChainLink To... (L NK)
147	Swap In CRV		407	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	65,134 54	$187,559.35	Curve DAO To... (CRV)
148	Swap Out L NK		408	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	7.097376083	$189.13	ChainLink To... (L NK)
149	Swap In CRV		410	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	65,134 54	$187,559.35	Curve DAO To... (CRV)
150	Swap Out L NK		411	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	6.534983747	$174.14	ChainLink To... (L NK)
151	Swap In CRV		413	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	65,134 54	$187,559.35	Curve DAO To... (CRV)
152	Swap Out L NK		414	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	6.044880137	$161.08	ChainLink To... (L NK)
153	Swap In CRV		416	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	65,134 54	$187,559.35	Curve DAO To... (CRV)
154	Swap Out L NK		417	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	5.614571044	$149.61	ChainLink To... (L NK)
155	Swap In MKR		419	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	57.50802571	$146,237.90	Maker (MKR)
156	Swap Out L NK		420	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	30.88588053	$823.03	ChainLink To... (L NK)
157	Swap In MKR		422	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	57.50802571	$146,237.90	Maker (MKR)
158	Swap Out L NK		423	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	19.72753436	$525.69	ChainLink To... (L NK)

159	Swap In MKR		425	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	57.50802571	$146,237.90	Maker (MKR)	
160	Swap Out L NK		426	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	14.16573663	$377.48	ChainLink To... (L NK)	
161	Swap In MKR		428	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	57.50802571	$146,237.90	Maker (MKR)	
162	Swap Out L NK		429	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	10.88828531	$290.15	ChainLink To... (L NK)	
163	Swap In MKR		431	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	57.50802571	$146,237.90	Maker (MKR)	
164	Swap Out L NK		432	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	8.751480058	$233.20	ChainLink To... (L NK)	
165	Swap In MKR		434	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	57.50802571	$146,237.90	Maker (MKR)	
166	Swap Out L NK		435	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	7.260089574	$193.46	ChainLink To... (L NK)	
167	Swap In MKR		437	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	57.50802571	$146,237.90	Maker (MKR)	
168	Swap Out L NK		438	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	6.166668768	$164.33	ChainLink To... (L NK)	
169	Swap In MKR		440	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	57.50802571	$146,237.90	Maker (MKR)	
170	Swap Out L NK		441	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	5.334592549	$142.15	ChainLink To... (L NK)	
171	Swap In MKR		443	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	57.50802571	$146,237.90	Maker (MKR)	
172	Swap Out L NK		444	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	4.682624243	$124.78	ChainLink To... (L NK)	
173	Swap In MKR		446	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	57.50802571	$146,237.90	Maker (MKR)	
174	Swap Out L NK		447	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	4.159612384	$110.84	ChainLink To... (L NK)	
175	Swap In MKR		449	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	57.50802571	$146,237.90	Maker (MKR)	
176	Swap Out L NK		450	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	3.731842031	$99.44	ChainLink To... (L NK)	
177	Swap In MKR		452	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	57.50802571	$146,237.90	Maker (MKR)	
178	Swap Out L NK		453	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	3.376244589	$89.97	ChainLink To... (L NK)	
179	Swap In MKR		455	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	57.50802571	$146,237.90	Maker (MKR)	
180	Swap Out L NK		456	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	3.076536471	$81.98	ChainLink To... (L NK)	
181	Swap In MKR		458	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	57.50802571	$146,237.90	Maker (MKR)	
182	Swap Out L NK		459	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	2.820916244	$75.17	ChainLink To... (L NK)	
183	Swap In MKR		461	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	57.50802571	$146,237.90	Maker (MKR)	
184	Swap Out L NK		462	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	2.600635108	$69.30	ChainLink To... (L NK)	
185	Swap In MKR		464	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	57.50802571	$146,237.90	Maker (MKR)	
186	Swap Out L NK		465	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	2.409078682	$64.20	ChainLink To... (L NK)	
187	Swap In MKR		467	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	57.50802571	$146,237.90	Maker (MKR)	
188	Swap Out L NK		468	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	2 241159513	$59.72	ChainLink To... (L NK)	
189	Swap In MKR		470	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	57.50802571	$146,237.90	Maker (MKR)	
190	Swap Out L NK		471	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	2.092904668	$55.77	ChainLink To... (L NK)	
191	Swap In SNX		473	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	15,080 34	$149,631.28	Synthetix Ne... (SNX)	
192	Swap Out L NK		474	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	15.66122924	$417.33	ChainLink To... (L NK)	
193	Swap In SNX		476	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	15,080 34	$149,631.28	Synthetix Ne... (SNX)	
194	Swap Out L NK		477	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	9.992101263	$266.26	ChainLink To... (L NK)	
195	Swap In SNX		479	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	15,080 34	$149,631.28	Synthetix Ne... (SNX)	
196	Swap Out L NK		480	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	7.169177086	$191.04	ChainLink To... (L NK)	
197	Swap In SNX		482	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	15,080 34	$149,631.28	Synthetix Ne... (SNX)	
198	Swap Out L NK		483	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	5.506925717	$146.75	ChainLink To... (L NK)	
199	Swap In SNX		485	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	15,080 34	$149,631.28	Synthetix Ne... (SNX)	
200	Swap Out L NK		486	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	4.423833267	$117.88	ChainLink To... (L NK)	
201	Swap In SNX		488	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	15,080 34	$149,631.28	Synthetix Ne... (SNX)	
202	Swap Out L NK		489	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	3.66826388	$97.75	ChainLink To... (L NK)	
203	Swap In SNX		491	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	15,080 34	$149,631.28	Synthetix Ne... (SNX)	
204	Swap Out L NK		492	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	3.114553136	$83.00	ChainLink To... (L NK)	
205	Swap In SNX		494	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	15,080 34	$149,631.28	Synthetix Ne... (SNX)	
206	Swap Out L NK		495	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	2.69334756	$71.77	ChainLink To... (L NK)	
207	Swap In SNX		497	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	15,080 34	$149,631.28	Synthetix Ne... (SNX)	
208	Swap Out L NK		498	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	2.363426041	$62.98	ChainLink To... (L NK)	
209	Swap In SNX		500	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	15,080 34	$149,631.28	Synthetix Ne... (SNX)	
210	Swap Out L NK		501	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	2.098842316	$55.93	ChainLink To... (L NK)	
211	Swap In SNX		503	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	15,080 34	$149,631.28	Synthetix Ne... (SNX)	

212	Swap Out L NK		504	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	1.882500021	$50.16	ChainLink To... (L NK)	
213	Swap In SNX		506	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	15,080 34	$149,631.28	Synthetix Ne... (SNX)	
214	Swap Out L NK		507	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	1.702704716	$45.37	ChainLink To... (L NK)	
215	Swap In SNX		509	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	15,080 34	$149,631.28	Synthetix Ne... (SNX)	
216	Swap Out L NK		510	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	1.55120371	$41.34	ChainLink To... (L NK)	
217	Swap In SNX		512	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	15,080 34	$149,631.28	Synthetix Ne... (SNX)	
218	Swap Out L NK		513	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	1.422017343	$37.89	ChainLink To... (L NK)	
219	Swap In SNX		515	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	15,080 34	$149,631.28	Synthetix Ne... (SNX)	
220	Swap Out L NK		516	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	1.310713681	$34.93	ChainLink To... (L NK)	
221	Swap In SNX		518	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	15,080 34	$149,631.28	Synthetix Ne... (SNX)	
222	Swap Out L NK		519	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	1.213942731	$32.35	ChainLink To... (L NK)	
223	Swap In SNX		521	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	15,080 34	$149,631.28	Synthetix Ne... (SNX)	
224	Swap Out L NK		522	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	1.129128344	$30.09	ChainLink To... (L NK)	
225	Swap In SNX		524	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	15,080 34	$149,631.28	Synthetix Ne... (SNX)	
226	Swap Out L NK		525	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	1.054259107	$28.09	ChainLink To... (L NK)	
227	Swap In YFI		527	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	2.752858666	$96,996.04	yearn.financ... (YFI)	
228	Swap Out L NK		529	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	5.364749057	$142.96	ChainLink To... (L NK)	
229	Swap In YFI		531	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	2.752858666	$96,996.04	yearn.financ... (YFI)	
230	Swap Out L NK		533	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	3.542573544	$94.40	ChainLink To... (L NK)	
231	Swap In YFI		535	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	2.752858666	$96,996.04	yearn.financ... (YFI)	
232	Swap Out L NK		537	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	2.606796242	$69.46	ChainLink To... (L NK)	
233	Swap In YFI		539	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	2.752858666	$96,996.04	yearn.financ... (YFI)	
234	Swap Out L NK		541	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	2.042895316	$54.44	ChainLink To... (L NK)	
235	Swap In YFI		543	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	2.752858666	$96,996.04	yearn.financ... (YFI)	
236	Swap Out L NK		545	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	1.668585354	$44.46	ChainLink To... (L NK)	
237	Swap In YFI		547	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	2.752858666	$96,996.04	yearn.financ... (YFI)	
238	Swap Out L NK		549	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	1.40337518	$37.40	ChainLink To... (L NK)	
239	Swap In YFI		551	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	2.752858666	$96,996.04	yearn.financ... (YFI)	
240	Swap Out L NK		553	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	1.206399988	$32.15	ChainLink To... (L NK)	
241	Swap In YFI		555	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	2.752858666	$96,996.04	yearn.financ... (YFI)	
242	Swap Out L NK		557	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	1.054789278	$28.11	ChainLink To... (L NK)	
243	Swap In YFI		559	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	2.752858666	$96,996.04	yearn.financ... (YFI)	
244	Swap Out L NK		561	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	0.9347834156	$24.91	ChainLink To... (L NK)	
245	Swap In YFI		563	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	2.752858666	$96,996.04	yearn.financ... (YFI)	
246	Swap Out L NK		565	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	0.8376277374	$22.32	ChainLink To... (L NK)	
247	Swap In YFI		567	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	2.752858666	$96,996.04	yearn.financ... (YFI)	
248	Swap Out L NK		569	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	0.7574975848	$20.19	ChainLink To... (L NK)	
249	Swap In YFI		571	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	2.752858666	$96,996.04	yearn.financ... (YFI)	
250	Swap Out L NK		573	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	0.6903735452	$18.40	ChainLink To... (L NK)	
251	Swap In YFI		575	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	2.752858666	$96,996.04	yearn.financ... (YFI)	
252	Swap Out L NK		577	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	0.6333962128	$16.88	ChainLink To... (L NK)	
253	Swap In YFI		579	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	2.752858666	$96,996.04	yearn.financ... (YFI)	
254	Swap Out L NK		581	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	0.5844782908	$15.57	ChainLink To... (L NK)	
255	Swap In YFI		583	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	2.752858666	$96,996.04	yearn.financ... (YFI)	
256	Swap Out L NK		585	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	0.5420620254	$14.44	ChainLink To... (L NK)	
257	Swap In YFI		587	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	2.752858666	$96,996.04	yearn.financ... (YFI)	
258	Swap Out L NK		589	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	0.5049623361	$13.46	ChainLink To... (L NK)	
259	Swap In YFI		591	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	2.752858666	$96,996.04	yearn.financ... (YFI)	
260	Swap Out L NK		593	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	0.4722623716	$12.58	ChainLink To... (L NK)	
261	Swap In YFI		595	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	2.752858666	$96,996.04	yearn.financ... (YFI)	
262	Swap Out L NK		597	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	0.4432421842	$11.81	ChainLink To... (L NK)	
263	Swap In UMA		599	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	9,358.43	$96,155.53	UMA Voting T... (UMA)	
264	Swap Out L NK		601	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	3.200627901	$85.29	ChainLink To... (L NK)	

265	Swap In UMA		603	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	9,358.43	$96,155.53	UMA Voting T... (UMA)	
266	Swap Out L NK		605	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	2.120726435	$56.51	ChainLink To... (L NK)	
267	Swap In UMA		607	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	9,358.43	$96,155.53	UMA Voting T... (UMA)	
268	Swap Out L NK		609	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	1.564446736	$41.69	ChainLink To... (L NK)	
269	Swap In UMA		611	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	9,358.43	$96,155.53	UMA Voting T... (UMA)	
270	Swap Out L NK		613	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	1.22846349	$32.74	ChainLink To... (L NK)	
271	Swap In UMA		615	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	9,358.43	$96,155.53	UMA Voting T... (UMA)	
272	Swap Out L NK		617	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	1.005031649	$26.78	ChainLink To... (L NK)	
273	Swap In UMA		619	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	9,358.43	$96,155.53	UMA Voting T... (UMA)	
274	Swap Out L NK		621	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	0.8464791759	$22.56	ChainLink To... (L NK)	
275	Swap In UMA		623	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	9,358.43	$96,155.53	UMA Voting T... (UMA)	
276	Swap Out L NK		625	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	0.7285637332	$19.41	ChainLink To... (L NK)	
277	Swap In UMA		627	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	9,358.43	$96,155.53	UMA Voting T... (UMA)	
278	Swap Out L NK		629	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	0.6376989838	$16.99	ChainLink To... (L NK)	
279	Swap In UMA		631	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	9,358.43	$96,155.53	UMA Voting T... (UMA)	
280	Swap Out L NK		633	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	0.5657010914	$15.07	ChainLink To... (L NK)	
281	Swap In UMA		635	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	9,358.43	$96,155.53	UMA Voting T... (UMA)	
282	Swap Out L NK		637	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	0.5073574693	$13.52	ChainLink To... (L NK)	
283	Swap In UMA		639	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	9,358.43	$96,155.53	UMA Voting T... (UMA)	
284	Swap Out L NK		641	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	0.4591967475	$12.24	ChainLink To... (L NK)	
285	Swap In UMA		643	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	9,358.43	$96,155.53	UMA Voting T... (UMA)	
286	Swap Out L NK		645	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	0.4188213555	$11.16	ChainLink To... (L NK)	
287	Swap In UMA		647	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	9,358.43	$96,155.53	UMA Voting T... (UMA)	
288	Swap Out L NK		649	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	0.3845243016	$10.25	ChainLink To... (L NK)	
289	Swap In UMA		651	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	9,358.43	$96,155.53	UMA Voting T... (UMA)	
290	Swap Out L NK		653	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	0.3550586049	$9.46	ChainLink To... (L NK)	
291	Swap In UMA		655	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	9,358.43	$96,155.53	UMA Voting T... (UMA)	
292	Swap Out L NK		657	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	0.3294930036	$8.78	ChainLink To... (L NK)	
293	Swap In UMA		659	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	9,358.43	$96,155.53	UMA Voting T... (UMA)	
294	Swap Out L NK		661	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	0.3071185763	$8.18	ChainLink To... (L NK)	
295	Swap In UMA		663	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	9,358.43	$96,155.53	UMA Voting T... (UMA)	
296	Swap Out L NK		665	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	0.2873865285	$7.66	ChainLink To... (L NK)	
297	Swap In UMA		667	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	9,358.43	$96,155.53	UMA Voting T... (UMA)	
298	Swap Out L NK		669	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	0.2698656823	$7.19	ChainLink To... (L NK)	
299	Swap In BAT		671	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	69,042.40	$48,511.75	BAT (BAT)	
300	Swap Out L NK		672	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	1.124506152	$29.97	ChainLink To... (L NK)	
301	Swap In BAT		674	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	69,042.40	$48,511.75	BAT (BAT)	
302	Swap Out L NK		675	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	0.7686338817	$20.48	ChainLink To... (L NK)	
303	Swap In BAT		677	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	69,042.40	$48,511.75	BAT (BAT)	
304	Swap Out L NK		678	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	0.580135801	$15.46	ChainLink To... (L NK)	
305	Swap In BAT		680	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	69,042.40	$48,511.75	BAT (BAT)	
306	Swap Out L NK		681	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	0.4638823446	$12.36	ChainLink To... (L NK)	
307	Swap In BAT		683	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	69,042.40	$48,511.75	BAT (BAT)	
308	Swap Out L NK		684	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	0.3852633055	$10.27	ChainLink To... (L NK)	
309	Swap In BAT		686	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	69,042.40	$48,511.75	BAT (BAT)	
310	Swap Out L NK		687	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	0.3286828039	$8.76	ChainLink To... (L NK)	
311	Swap In BAT		689	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	69,042.40	$48,511.75	BAT (BAT)	
312	Swap Out L NK		690	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	0.286090792	$7.62	ChainLink To... (L NK)	
313	Swap In BAT		692	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	69,042.40	$48,511.75	BAT (BAT)	
314	Swap Out L NK		693	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	0.2529182825	$6.74	ChainLink To... (L NK)	
315	Swap In BAT		695	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	69,042.40	$48,511.75	BAT (BAT)	
316	Swap Out L NK		696	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	0.2263826564	$6.03	ChainLink To... (L NK)	
317	Swap In BAT		698	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	69,042.40	$48,511.75	BAT (BAT)	

318	Swap Out L NK	699	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	0.2046941922	$5.45	ChainLink To... (L NK)	
319	Swap In BAT	701	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	69,042.40	$48,511.75	BAT (BAT)	
320	Swap Out L NK	702	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	0.1866505202	$4.97	ChainLink To... (L NK)	
321	Swap In BAT	704	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	69,042.40	$48,511.75	BAT (BAT)	
322	Swap Out L NK	705	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	0.1714145643	$4.57	ChainLink To... (L NK)	
323	Swap In BAT	707	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	69,042.40	$48,511.75	BAT (BAT)	
324	Swap Out L NK	708	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	0.1583859917	$4.22	ChainLink To... (L NK)	
325	Swap In BAT	710	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	69,042.40	$48,511.75	BAT (BAT)	
326	Swap Out L NK	711	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	0.1471232885	$3.92	ChainLink To... (L NK)	
327	Swap In BAT	713	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	69,042.40	$48,511.75	BAT (BAT)	
328	Swap Out L NK	714	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	0.1372946587	$3.66	ChainLink To... (L NK)	
329	Swap In BAT	716	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	69,042.40	$48,511.75	BAT (BAT)	
330	Swap Out L NK	717	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	0.1286460441	$3.43	ChainLink To... (L NK)	
331	Swap In BAT	719	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	69,042.40	$48,511.75	BAT (BAT)	
332	Swap Out L NK	720	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	0.1209796927	$3.22	ChainLink To... (L NK)	
333	Swap In BAT	722	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	69,042.40	$48,511.75	BAT (BAT)	
334	Swap Out L NK	723	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	0.1141394308	$3.04	ChainLink To... (L NK)	
335	Minimum Balance Update	725						
336	Create New CC10	727	Black Hole: 0x000 000	Indexed: CC10 Token	6,268 60	$2,573.98	Cryptocurren... (CC10)	
337	Transfer CC10 To Attack Contract	728	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	6,268 60	$2,573.98	Cryptocurren... (CC10)	
338	Mint CC10 Via L NK [Log 726]	729	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	10.61516406	$282.87	ChainLink To... (L NK)	
339	Create New CC10	731	Black Hole: 0x000 000	Indexed: CC10 Token	6,870 35	$2,821.06	Cryptocurren... (CC10)	
340	Transfer CC10 To Attack Contract	732	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	6,870 35	$2,821.06	Cryptocurren... (CC10)	
341	Mint CC10 Via L NK [Log 730]	733	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	15.92274609	$424.30	ChainLink To... (L NK)	
342	Create New CC10	735	Black Hole: 0x000 000	Indexed: CC10 Token	7,529 87	$3,091.87	Cryptocurren... (CC10)	
343	Transfer CC10 To Attack Contract	736	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	7,529 87	$3,091.87	Cryptocurren... (CC10)	
344	Mint CC10 Via L NK [Log 734]	737	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	23 88411914	$636.45	ChainLink To... (L NK)	
345	Create New CC10	739	Black Hole: 0x000 000	Indexed: CC10 Token	8,252 69	$3,388.67	Cryptocurren... (CC10)	
346	Transfer CC10 To Attack Contract	740	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	8,252 69	$3,388.67	Cryptocurren... (CC10)	
347	Mint CC10 Via L NK [Log 738]	741	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	35 8261787	$954.68	ChainLink To... (L NK)	
348	Create New CC10	743	Black Hole: 0x000 000	Indexed: CC10 Token	9,044 90	$3,713.96	Cryptocurren... (CC10)	
349	Transfer CC10 To Attack Contract	744	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	9,044 90	$3,713.96	Cryptocurren... (CC10)	
350	Mint CC10 Via L NK [Log 742]	745	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	53.73926806	$1,432.02	ChainLink To... (L NK)	
351	Create New CC10	747	Black Hole: 0x000 000	Indexed: CC10 Token	9,913.15	$4,070.48	Cryptocurren... (CC10)	
352	Transfer CC10 To Attack Contract	748	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	9,913.15	$4,070.48	Cryptocurren... (CC10)	
353	Mint CC10 Via L NK [Log 746]	749	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	80.60890209	$2,148.02	ChainLink To... (L NK)	
354	Create New CC10	751	Black Hole: 0x000 000	Indexed: CC10 Token	10,864.76	$4,461.22	Cryptocurren... (CC10)	
355	Transfer CC10 To Attack Contract	752	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	10,864.76	$4,461.22	Cryptocurren... (CC10)	
356	Mint CC10 Via L NK [Log 750]	753	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	120 9133531	$3,222.04	ChainLink To... (L NK)	
357	Create New CC10	755	Black Hole: 0x000 000	Indexed: CC10 Token	11,907.71	$4,889.47	Cryptocurren... (CC10)	
358	Transfer CC10 To Attack Contract	756	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	11,907.71	$4,889.47	Cryptocurren... (CC10)	
359	Mint CC10 Via L NK [Log 754]	757	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	181 3700297	$4,833.06	ChainLink To... (L NK)	
360	Create New CC10	759	Black Hole: 0x000 000	Indexed: CC10 Token	13,050.78	$5,358.83	Cryptocurren... (CC10)	
361	Transfer CC10 To Attack Contract	760	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	13,050.78	$5,358.83	Cryptocurren... (CC10)	
362	Mint CC10 Via L NK [Log 758]	761	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	272 0550445	$7,249.58	ChainLink To... (L NK)	
363	Create New CC10	763	Black Hole: 0x000 000	Indexed: CC10 Token	14,303 58	$5,873.25	Cryptocurren... (CC10)	
364	Transfer CC10 To Attack Contract	764	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	14,303 58	$5,873.25	Cryptocurren... (CC10)	
365	Mint CC10 Via L NK [Log 762]	765	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	408 0825668	$10,874.37	ChainLink To... (L NK)	
366	Create New CC10	767	Black Hole: 0x000 000	Indexed: CC10 Token	15,676 64	$6,437.05	Cryptocurren... (CC10)	
367	Transfer CC10 To Attack Contract	768	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	15,676 64	$6,437.05	Cryptocurren... (CC10)	
368	Mint CC10 Via L NK [Log 766]	769	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	612.1238502	$16,311.56	ChainLink To... (L NK)	
369	Create New CC10	771	Black Hole: 0x000 000	Indexed: CC10 Token	17,181 50	$7,054.97	Cryptocurren... (CC10)	
370	Transfer CC10 To Attack Contract	772	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	17,181 50	$7,054.97	Cryptocurren... (CC10)	

371	Mint CC10 Via L NK [Log 770]	773	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	918.1857753	$24,467.34	ChainLink To... (L NK)	
372	Create New CC10	775	Black Hole: 0x000 000	Indexed: CC10 Token	18,830 82	$7,732.20	Cryptocurren... (CC10)	
373	Transfer CC10 To Attack Contract	776	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	18,830 82	$7,732.20	Cryptocurren... (CC10)	
374	Mint CC10 Via L NK [Log 774]	777	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	1,377 28	$36,701.01	ChainLink To... (L NK)	
375	Create New CC10	779	Black Hole: 0x000 000	Indexed: CC10 Token	20,638.47	$8,474.45	Cryptocurren... (CC10)	
376	Transfer CC10 To Attack Contract	780	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	20,638.47	$8,474.45	Cryptocurren... (CC10)	
377	Mint CC10 Via L NK [Log 778]	781	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	2,065 92	$55,051.52	ChainLink To... (L NK)	
378	Create New CC10	783	Black Hole: 0x000 000	Indexed: CC10 Token	22,619 64	$9,287.94	Cryptocurren... (CC10)	
379	Transfer CC10 To Attack Contract	784	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	22,619 64	$9,287.94	Cryptocurren... (CC10)	
380	Mint CC10 Via L NK [Log 782]	785	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	3,098 88	$82,577.28	ChainLink To... (L NK)	
381	Create New CC10	787	Black Hole: 0x000 000	Indexed: CC10 Token	24,790 99	$10,179.53	Cryptocurren... (CC10)	
382	Transfer CC10 To Attack Contract	788	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	24,790 99	$10,179.53	Cryptocurren... (CC10)	
383	Mint CC10 Via L NK [Log 786]	789	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	4,648 32	$123,865.92	ChainLink To... (L NK)	
384	Create New CC10	791	Black Hole: 0x000 000	Indexed: CC10 Token	27,170.78	$11,156.70	Cryptocurren... (CC10)	
385	Transfer CC10 To Attack Contract	792	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	27,170.78	$11,156.70	Cryptocurren... (CC10)	
386	Mint CC10 Via L NK [Log 790]	793	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	6,972.47	$185,798.88	ChainLink To... (L NK)	
387	Create New CC10	795	Black Hole: 0x000 000	Indexed: CC10 Token	29,779 01	$12,227.68	Cryptocurren... (CC10)	
388	Transfer CC10 To Attack Contract	796	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	29,779 01	$12,227.68	Cryptocurren... (CC10)	
389	Mint CC10 Via L NK [Log 794]	797	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	10,458.71	$278,698.32	ChainLink To... (L NK)	
390	Create New CC10	799	Black Hole: 0x000 000	Indexed: CC10 Token	32,637 62	$13,401.47	Cryptocurren... (CC10)	
391	Transfer CC10 To Attack Contract	800	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	32,637 62	$13,401.47	Cryptocurren... (CC10)	
392	Mint CC10 Via L NK [Log 798]	801	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	15,688 06	$418,047.48	ChainLink To... (L NK)	
393	Create New CC10	803	Black Hole: 0x000 000	Indexed: CC10 Token	35,770 63	$14,687.93	Cryptocurren... (CC10)	
394	Transfer CC10 To Attack Contract	804	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	35,770 63	$14,687.93	Cryptocurren... (CC10)	
395	Mint CC10 Via L NK [Log 802]	805	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	23,532.10	$627,071.23	ChainLink To... (L NK)	
396	Create New CC10	807	Black Hole: 0x000 000	Indexed: CC10 Token	39,204.40	$16,097.88	Cryptocurren... (CC10)	
397	Transfer CC10 To Attack Contract	808	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	39,204.40	$16,097.88	Cryptocurren... (CC10)	
398	Mint CC10 Via L NK [Log 806]	809	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	35,298.15	$940,606.84	ChainLink To... (L NK)	
399	Create New CC10	811	Black Hole: 0x000 000	Indexed: CC10 Token	42,967.79	$17,643.18	Cryptocurren... (CC10)	
400	Transfer CC10 To Attack Contract	812	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	42,967.79	$17,643.18	Cryptocurren... (CC10)	
401	Mint CC10 Via L NK [Log 810]	813	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	52,947 22	$1,410,910.26	ChainLink To... (L NK)	
402	Create New CC10	815	Black Hole: 0x000 000	Indexed: CC10 Token	47,092.44	$19,336.82	Cryptocurren... (CC10)	
403	Transfer CC10 To Attack Contract	816	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	47,092.44	$19,336.82	Cryptocurren... (CC10)	
404	Mint CC10 Via L NK [Log 814]	817	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	79,420 83	$2,116,365.39	ChainLink To... (L NK)	
405	Create New CC10	819	Black Hole: 0x000 000	Indexed: CC10 Token	49,119 24	$20,169.05	Cryptocurren... (CC10)	
406	Transfer CC10 To Attack Contract	820	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	49,119 24	$20,169.05	Cryptocurren... (CC10)	
407	Mint CC10 Via L NK [Log 818]	821	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	112,504 34	$2,997,957.69	ChainLink To... (L NK)	
408	Flash Loan	822	SushiSwap: SUSHI	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	16,000	$172,069.21	SushiToken (SUSHI)	
409	SUSHI "Gift"	823	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	16,000	$172,069.21	SushiToken (SUSHI)	$10.75
410	SUSHI Initialised	824						
411	SUSHI Massively Overweighed	825						
412	Transfer CC10 For Redemption	826	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	521,486 36	$214,129.65	Cryptocurren... (CC10)	
413	Exit Fee Sent To Treasury	827	Indexed: CC10 Token	0x78a3ef33cf033381feb43ba4212f2af5a5a0a2ea	2,607.43	$1,070.65	Cryptocurren... (CC10)	
414	Remaining CC10 Burned	828	Indexed: CC10 Token	Black Hole: 0x000 000	518,878 93	$213,059.00	Cryptocurren... (CC10)	
415	Remove L NK	830	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	310,172 32	$8,265,312.58	ChainLink To... (L NK)	
416	Remove UNI	832	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	320,946.45	$8,436,729.54	Uniswap (UNI)	
417	Remove AAVE	839	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	11,813 54	$3,584,565.44	Aave Token (AAVE)	
418	Remove COMP	841	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	9,298.15	$2,923,162.27	Compound (COMP)	
419	Remove SNX	844	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	266,701 55	$2,646,286.95	Synthetix Ne... (SNX)	
420	Remove CRV	846	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	1,151,929 39	$3,317,059.46	Curve DAO To... (CRV)	
421	Remove YFI	848	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	48.68536694	$1,715,412.30	yearn.financ... (YFI)	
422	Remove UMA	850	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	165,507 37	$1,700,547.63	UMA Voting T... (UMA)	
423	Remove MKR	852	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	1,017 05	$2,586,273.68	Maker (MKR)	

424	Remove BAT	854	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	1,221,041.44	$857,949.03	BAT (BAT)	
425	Remove SUSHI	856	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	16,297 50	$175,268.67	SushiToken (SUSHI)	
426	Create New CC10	859	Black Hole: 0x000 000	Indexed: CC10 Token	33,421 81	$13,723.47	Cryptocurren... (CC10)	
427	Transfer CC10 To Attack Contract	860	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	33,421 81	$13,723.47	Cryptocurren... (CC10)	
428	Mint CC10 Via SUSHI [Log 858]	861	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	1,066.49	$11,469.34	SushiToken (SUSHI)	
429	Create New CC10	864	Black Hole: 0x000 000	Indexed: CC10 Token	49,870.45	$20,477.51	Cryptocurren... (CC10)	
430	Transfer CC10 To Attack Contract	865	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	49,870.45	$20,477.51	Cryptocurren... (CC10)	
431	Mint CC10 Via SUSHI [Log 863]	866	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	1,599.73	$17,204.01	SushiToken (SUSHI)	
432	Create New CC10	869	Black Hole: 0x000 000	Indexed: CC10 Token	74,414 32	$30,555.57	Cryptocurren... (CC10)	
433	Transfer CC10 To Attack Contract	870	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	74,414 32	$30,555.57	Cryptocurren... (CC10)	
434	Mint CC10 Via SUSHI [Log 868]	871	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	2,399 59	$25,806.01	SushiToken (SUSHI)	
435	Create New CC10	874	Black Hole: 0x000 000	Indexed: CC10 Token	111,037 53	$45,593.58	Cryptocurren... (CC10)	
436	Transfer CC10 To Attack Contract	875	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	111,037 53	$45,593.58	Cryptocurren... (CC10)	
437	Mint CC10 Via SUSHI [Log 873]	876	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	3,599 39	$38,709.02	SushiToken (SUSHI)	
438	Create New CC10	879	Black Hole: 0x000 000	Indexed: CC10 Token	165,684 95	$68,032.58	Cryptocurren... (CC10)	
439	Transfer CC10 To Attack Contract	880	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	165,684 95	$68,032.58	Cryptocurren... (CC10)	
440	Mint CC10 Via SUSHI [Log 878]	881	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	5,399 09	$58,063.53	SushiToken (SUSHI)	
441	Create New CC10	884	Black Hole: 0x000 000	Indexed: CC10 Token	68,304.12	$28,046.63	Cryptocurren... (CC10)	
442	Transfer CC10 To Attack Contract	885	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	68,304.12	$28,046.63	Cryptocurren... (CC10)	
443	Mint CC10 Via SUSHI [Log 883]	886	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	2,233 22	$24,016.75	SushiToken (SUSHI)	
444	Transfer CC10 For Redemption	888	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	502,733.19	$206,429.33	Cryptocurren... (CC10)	
445	Exit Fee Sent To Treasury	889	Indexed: CC10 Token	0x78a3ef33cf033381feb43ba4212f2af5a5a0a2ea	2,513 67	$1,032.15	Cryptocurren... (CC10)	
446	Remaining CC10 Burned	890	Indexed: CC10 Token	Black Hole: 0x000 000	500,219 53	$205,397.19	Cryptocurren... (CC10)	
447	Remove L NK	892	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	35,584.72	$948,243.40	ChainLink To... (L NK)	
448	Remove UNI	894	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	36,820.79	$967,909.33	Uniswap (UNI)	
449	Remove AAVE	901	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	1,355 32	$411,241.62	Aave Token (AAVE)	
450	Remove COMP	903	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	1,066.74	$335,361.71	Compound (COMP)	
451	Remove SNX	906	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	30,597 51	$303,597.01	Synthetix Ne... (SNX)	
452	Remove CRV	908	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	132,155 85	$380,551.82	Curve DAO To... (CRV)	
453	Remove YFI	909	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	5.585460644	$196,801.80	yearn.financ... (YFI)	
454	Remove UMA	912	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	18,987 94	$195,096.44	UMA Voting T... (UMA)	
455	Remove MKR	914	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	116 6819126	$296,711.94	Maker (MKR)	
456	Remove BAT	916	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	140,084.78	$98,428.77	BAT (BAT)	
457	Remove SUSHI	918	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	16,155 97	$173,746.55	SushiToken (SUSHI)	
458	Create New CC10	920	Black Hole: 0x000 000	Indexed: CC10 Token	34,658 92	$14,231.44	Cryptocurren... (CC10)	
459	Transfer CC10 To Attack Contract	921	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	34,658 92	$14,231.44	Cryptocurren... (CC10)	
460	Mint CC10 Via SUSHI [Log 919]	922	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	1,137 25	$12,230.40	SushiToken (SUSHI)	
461	Create New CC10	925	Black Hole: 0x000 000	Indexed: CC10 Token	51,716.40	$21,235.48	Cryptocurren... (CC10)	
462	Transfer CC10 To Attack Contract	926	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	51,716.40	$21,235.48	Cryptocurren... (CC10)	
463	Mint CC10 Via SUSHI [Log 924]	927	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	1,705 88	$18,345.60	SushiToken (SUSHI)	
464	Create New CC10	930	Black Hole: 0x000 000	Indexed: CC10 Token	77,168.77	$31,686.58	Cryptocurren... (CC10)	
465	Transfer CC10 To Attack Contract	931	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	77,168.77	$31,686.58	Cryptocurren... (CC10)	
466	Mint CC10 Via SUSHI [Log 929]	932	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	2,558 82	$27,518.40	SushiToken (SUSHI)	
467	Create New CC10	935	Black Hole: 0x000 000	Indexed: CC10 Token	115,147 58	$47,281.22	Cryptocurren... (CC10)	
468	Transfer CC10 To Attack Contract	936	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	115,147 58	$47,281.22	Cryptocurren... (CC10)	
469	Mint CC10 Via SUSHI [Log 934]	937	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	3,838 23	$41,277.61	SushiToken (SUSHI)	
470	Create New CC10	940	Black Hole: 0x000 000	Indexed: CC10 Token	171,817.78	$70,550.80	Cryptocurren... (CC10)	
471	Transfer CC10 To Attack Contract	941	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	171,817.78	$70,550.80	Cryptocurren... (CC10)	
472	Mint CC10 Via SUSHI [Log 939]	942	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	5,757 35	$61,916.41	SushiToken (SUSHI)	
473	Create New CC10	945	Black Hole: 0x000 000	Indexed: CC10 Token	34,470.78	$14,154.19	Cryptocurren... (CC10)	
474	Transfer CC10 To Attack Contract	946	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	34,470.78	$14,154.19	Cryptocurren... (CC10)	
475	Mint CC10 Via SUSHI [Log 944]	947	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	1,158.43	$12,458.12	SushiToken (SUSHI)	
476	Transfer CC10 For Redemption	949	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed: CC10 Token	484,980 23	$199,139.72	Cryptocurren... (CC10)	

CC10 Transaction Log

477	Exit Fee Sent To Treasury	950	Indexed: CC10 Token	0x78a3ef33cf033381feb43ba4212f2af5a5a0a2ea	2,424 90	$995.70	Cryptocurren... (CC10)	
478	Remaining CC10 Burned	951	Indexed: CC10 Token	Black Hole: 0x000 000	482,555 33	$198,144.02	Cryptocurren... (CC10)	
479	Remove L NK	953	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	4,352 68	$115,987.99	ChainLink To... (L NK)	
480	Remove UNI	955	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	4,503 87	$118,393.50	Uniswap (UNI)	
481	Remove AAVE	962	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	165.7806026	$50,302.58	Aave Token (AAVE)	
482	Remove COMP	964	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	130.481899	$41,021.04	Compound (COMP)	
483	Remove SNX	967	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	3,742 65	$37,135.62	Synthetix Ne... (SNX)	
484	Remove CRV	969	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	16,165.14	$46,548.64	Curve DAO To... (CRV)	
485	Remove YFI	971	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	0.6832067871	$24,072.56	yearn.financ... (YFI)	
486	Remove UMA	973	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	2,322 58	$23,863.96	UMA Voting T... (UMA)	
487	Remove MKR	975	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	14.27239035	$36,293.45	Maker (MKR)	
488	Remove BAT	977	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	17,135 00	$12,039.69	BAT (BAT)	
489	Remove SUSHI	979	Indexed: CC10 Token	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	16,013 09	$172,210.01	SushiToken (SUSHI)	
490	Repay Flash Loan	980	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	SushiSwap: LINK	316,668.78	$8,438,426.76	ChainLink To... (L NK)	
491	Repay Flash Loan	981	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Uniswap V2: UNI 30	327,668 56	$8,613,433.99	Uniswap (UNI)	
492	Repay Flash Loan	986	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	SushiSwap: AAVE	12,060 97	$3,659,642.95	Aave Token (AAVE)	
493	Repay Flash Loan	987	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	SushiSwap: COMP	9,492 90	$2,984,386.92	Compound (COMP)	
494	Repay Flash Loan	988	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	SushiSwap: CRV	1,176,056.16	$3,386,534.15	Curve DAO To... (CRV)	
495	Repay Flash Loan	989	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	SushiSwap: MKR	1,038 35	$2,640,442.31	Maker (MKR)	
496	Repay Flash Loan	990	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	SushiSwap: SNX	272,287 52	$2,701,712.54	Synthetix Ne... (SNX)	
497	Repay Flash Loan	991	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	SushiSwap: YFI	49.70506551	$1,751,341.03	yearn.financ... (YFI)	
498	Repay Flash Loan	992	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	SushiSwap: UMA	168,973 87	$1,736,165.03	UMA Voting T... (UMA)	
499	Repay Flash Loan	993	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Uniswap V2: BAT 2	1,246,615.74	$875,918.49	BAT (BAT)	
500	Swap In LINK On Uniswap	995	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Uniswap V2: LINK 21	16.7901819	$447.42	ChainLink To... (L NK)	
501	[Internal LP Mechanics]	996	Uniswap V2: LINK 21	Uniswap V2: SUSHI	0.1206847557	$457.26	Wrapped Ethe... (WETH)	
502	Swap Out SUSHI On Uniswap	999	Uniswap V2: SUSHI	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	42.90800162	$461.45	SushiToken (SUSHI)	
503	Repay Flash Loan	1002	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	SushiSwap: SUSHI	16,056	$172,671.45	SushiToken (SUSHI)	
504	Swap In LINK On Uniswap	1003	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Uniswap V2: LINK 21	208.7248495	$5,561.99	ChainLink To... (L NK)	
505	Swap Out WETH On Uniswap	1004	Uniswap V2: LINK 21	Uniswap V2: Router 2	1.5	$5,683.34	Wrapped Ethe... (WETH)	
506	Unwrap 1.5 WETH To 1.5 Ether *	1007						
507	Transfer L NK To Attack Invoker **	1030	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed Finance Exploiter	33,215.43	$885,107.80	ChainLink To... (L NK)	
508	Transfer UNI To Attack Invoker	1031	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed Finance Exploiter	34,602 55	$909,598.37	Uniswap (UNI)	
509	Transfer AAVE To Attack Invoker	1036	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed Finance Exploiter	1,273 67	$386,466.68	Aave Token (AAVE)	
510	Transfer COMP To Attack Invoker	1037	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed Finance Exploiter	1,002.47	$315,158.10	Compound (COMP)	
511	Transfer CRV To Attack Invoker	1038	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed Finance Exploiter	124,194 23	$357,625.77	Curve DAO To... (CRV)	
512	Transfer MKR To Attack Invoker	1039	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed Finance Exploiter	109 6525005	$278,836.76	Maker (MKR)	
513	Transfer SNX To Attack Invoker	1040	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed Finance Exploiter	28,754.19	$285,307.04	Synthetix Ne... (SNX)	
514	Transfer YFI To Attack Invoker	1041	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed Finance Exploiter	5.248968862	$184,945.63	yearn.financ... (YFI)	
515	Transfer UMA To Attack Invoker	1042	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed Finance Exploiter	17,844 03	$183,343.01	UMA Voting T... (UMA)	
516	Transfer BAT To Attack Invoker	1043	0xfbc2e6b188013fc5eacd9944e6b8ced2c467464a	Indexed Finance Exploiter	131,645.48	$92,499.00	BAT (BAT)	
	* This Ether is sent to some unrelated wallet belonging to an Ethereum miner, but does not show up in this set of records (only considers non-ETH tokens).							
	** The amount of L NK stolen is really 208.7248495 + 33,215.43 = 33424.1548495, from lines 505 and 508							

THIS IS **EXHIBIT "7"** TO
THE AFFIDAVIT OF **LAURENCE DAY**
SWORN BEFORE ME
THIS 9th DAY OF DECEMBER, 2021

Stephen Aylward

A COMMISSIONER ETC.

Get started Open in app

Indexed Finance

1K Followers About Follow

Indexed Attack Post-Mortem

Indexed Finance Oct 15 · 5 min read

Today Indexed suffered its first hack since its deployment in December, and it was a pretty devastating one. About $16m worth of assets were stolen from the indices DEFI5 and CC10 by 0xba5ed1488be60ba2facc6b66c6d6f0befba22ebe.

Needless to say, we're shocked and upset: hearing 'we're sorry' from a protocol always seems to ring hollow in the aftermath of these incidents (especially to those impacted) but it bears repeating: we are *truly* apologetic, to both those who have had funds drained, and those who remain in unaffected pools.

It is important for us to let you know exactly what happened, as soon as possible, and the rest of this post lays that out in detail.

This attack exploited the way index pools are rebalanced. To explain what happened, we'll need to dig into some fairly technical details about the protocol, and we'll assume you're familiar with Balancer and understand what an index fund is.

How index pools handle new assets

When a token is added to an index pool, we use approximate values with a Uniswap oracle to determine how to price the token within the Balancer pool. This is done to remove any need for the pool to interact with external markets in order to rebalance, and allows tokens to be traded into the AMM before the pool has any balance in them.

To do this, we use a function `extrapolatePoolValueFromToken`. This finds the **first token in the pool with a target weight over 0 and which is fully initialized**, then multiplies the pool's balance by the reciprocal of its weight — so if the pool has 10 UNI at a weight of 10%, it'll say the pool is worth 100 UNI. The controller uses this with a Uniswap oracle to determine the amount of a new token X that is worth 1% of the pool, which is then used to price swaps. Until the pool reaches that balance for the token, it will buy it at a slight premium; once it hits the balance, the token is considered "initialized" and can be both bought and sold by the pool.

```
/**
 * @dev Finds the first token which is both initialized and has a
 * desired weight above 0, then returns the address of that token
 * and the extrapolated value of the pool in terms of that token.
 *
 * The value is extrapolated by multiplying the token's
 * balance by the reciprocal of its normalized weight.
 * @return (token, extrapolatedValue)
 */
function extrapolatePoolValueFromToken()
  external
  view
  override
  _viewlock_
  returns (address/* token */, uint256/* extrapolatedValue */)
{
  address token;
  uint256 extrapolatedValue;
  uint256 len = _tokens.length;
  for (uint256 i = 0; i < len; i++) {
    token = _tokens[i];
    Record storage record = _records[token];
    if (record.ready && record.desiredDenorm > 0) {
      extrapolatedValue = bmul(
        record.balance,
        bdiv(_totalWeight, record.denorm)
      );
      break;
    }
  }
  require(extrapolatedValue > 0, "ERR_NONE_READY");
  return (token, extrapolatedValue);
}
```

Extrapolation of pool value

```
/**
 * @dev Re-indexes a pool by setting the underlying assets to the top
 * tokens in its category by market cap.
 */
function reindexPool(address poolAddress) external {
  IndexPoolMeta memory meta = _poolMeta[poolAddress];
  require(meta.initialized, "ERR_POOL_NOT_FOUND");
  require(
    now - meta.lastReweigh >= POOL_REWEIGH_DELAY,
    "ERR_POOL_REWEIGH_DELAY"
  );
  require(
    (++meta.reweighIndex % (REWEIGHS_BEFORE_REINDEX + 1)) == 0,
    "ERR_REWEIGH_INDEX"
  );
  uint256 size = meta.indexSize;
  address[] memory tokens = getTopCategoryTokens(meta.categoryID, size);

  PriceLibrary.TwoWayAveragePrice[] memory prices = oracle.computeTwoWayAveragePrices(
    tokens,
    LONG_TWAP_MIN_TIME_ELAPSED,
```

```
    LONG_TWAP_MAX_TIME_ELAPSED
  );
  FixedPoint.uq112x112[] memory weights = MCapSqrtLibrary.computeTokenWeights(tokens, prices);

  uint256[] memory minimumBalances = new uint256[](size);
  uint96[] memory denormalizedWeights = new uint96[](size);
  uint144 totalValue = _estimatePoolValue(IIndexPool(poolAddress));

  for (uint256 i = 0; i < size; i++) {
    // The minimum balance is the number of tokens worth the minimum weight
    // of the pool. The minimum weight is 1/100, so we divide the total value
    // by 100 to get the desired weth value, then multiply by the price of eth
    // in terms of that token to get the minimum balance.
    minimumBalances[i] = prices[i].computeAverageTokensForEth(totalValue) / 100;
    denormalizedWeights[i] = _denormalizeFractionalWeight(weights[i]);
  }

  meta.lastReweigh = uint64(now);
  _poolMeta[poolAddress] = meta;

  IIndexPool(poolAddress).reindexTokens(
    tokens,
    denormalizedWeights,
    minimumBalances
  );
  emit PoolReindexed(poolAddress);
}
```

Derivation of virtual balances

Occasionally, token prices will change so quickly that the minimum balance is so far off of the value of 1% of the pool that no one is willing to swap it into the pool. To prevent this from causing a delay in a rebalance, the controller has another function updateMinimumBalance which resets the virtual balance for an uninitialized token.

```
/**
 * @dev Updates the minimum balance of an uninitialized token, which is
 * useful when the token's price on the pool is too low relative to
 * external prices for people to trade it in.
 */
function updateMinimumBalance(IIndexPool pool, address tokenAddress) external _havePool(address(pool)) {
  IIndexPool.Record memory record = pool.getTokenRecord(tokenAddress);
  require(!record.ready, "ERR_TOKEN_READY");
  uint256 poolValue = _estimatePoolValue(pool);
  PriceLibrary.TwoWayAveragePrice memory price = oracle.computeTwoWayAveragePrice(
    tokenAddress,
    SHORT_TWAP_MIN_TIME_ELAPSED,
    SHORT_TWAP_MAX_TIME_ELAPSED
  );
  uint256 minimumBalance = price.computeAverageTokensForEth(poolValue) / 100;
  pool.setMinimumBalance(tokenAddress, minimumBalance);
}
```

If you've worked on contracts before, you probably see where this is going.

DEFI5 Attack

Transaction

Logs

At the time the attack started, DEFI5 was ready for a re-index (anyone can trigger one after 3 re-weighs, which occur once a week). The first call in the transaction was to trigger a re-index of DEFI5. At this time, UNI was the first asset in the token list which was fully initialized and had a desired weight over zero, so the price of UNI was used to approximate the pool value and set the minimum balance for SUSHI. This set a reasonable minimum balance for SUSHI of 11,926, or about $126k.

Next, the exploit contract took out approximately $156m worth of flash swaps in UNI, AAVE, COMP, CRV, MKR, SNX (the initialized assets in DEFI5) from Sushiswap and Uniswap V2.

From	Uniswap V2: UNI 30	To	0x277e851587eb5…	For	1,836,342.050150158215305238 ($47,487,805.42)	Uniswap (UNI)
From	SushiSwap: AAVE	To	0x277e851587eb5…	For	221,217.366781517207266602 ($66,120,074.07)	Aave Token (AAVE)
From	SushiSwap: COMP	To	0x277e851587eb5…	For	41,371.149252067400558421 ($12,815,127.19)	Compound (COMP)
From	SushiSwap: CRV	To	0x277e851587eb5…	For	3,210,906.891991096095551982 ($9,096,579.51)	Curve DAO To… (CRV)
From	SushiSwap: MKR	To	0x277e851587eb5…	For	5,775.828019598003061742 ($14,577,208.03)	Maker (MKR)
From	SushiSwap: SNX	To	0x277e851587eb5…	For	453,645.292460278750509681 ($4,604,499.72)	Synthetix Ne… (SNX)

The contract then used all of the borrowed assets to purchase UNI from the pool in chunks, as the pool does not allow swaps to send more than 1/2 of the pool's existing balance in a token or purchase more than 1/3 of the pool's balance in a token. This took dozens of swaps, but they managed to dump the tokens into the pool.

Small sampling of the swaps executed with the pool.

The attacker then executed a minimum balance update on the controller. Because they had purchased nearly all of the UNI in the pool, its balance was very low when the controller queried it, and so the approximated value of the entire pool was calculated as 29,851 SUSHI (~$300k), despite the pool having received over a hundred million dollars worth of other assets.

The previously purchased UNI was then used to mint new DEFI5, again in chunks due to limitations on the relative size of a single-token mint. This resulted in the pool supply being inflated by orders of magnitude.

- **From** 0x277e851587eb5... **To** Indexed: DEFI5 To... **For** 27,216.928649769784570761 ($704,101.94) Uniswap (UNI)
- **From** Black Hole: 0x000... **To** Indexed: DEFI5 To... **For** 75,828.20927646727283924 ($264,027.41) DEFI Top 5 T... (DEFI5)
- **From** Indexed: DEFI5 To... **To** 0x277e851587eb5... **For** 75,828.20927646727283924 ($264,027.41) DEFI Top 5 T... (DEFI5)
- **From** 0x277e851587eb5... **To** Indexed: DEFI5 To... **For** 40,825.392974654676856142 ($1,056,152.92) Uniswap (UNI)
- **From** Black Hole: 0x000... **To** Indexed: DEFI5 To... **For** 88,616.134258261444062367 ($308,553.88) DEFI Top 5 T... (DEFI5)
- **From** Indexed: DEFI5 To... **To** 0x277e851587eb5... **For** 88,616.134258261444062367 ($308,553.88) DEFI Top 5 T... (DEFI5)
- **From** 0x277e851587eb5... **To** Indexed: DEFI5 To... **For** 61,238.089461982015284213 ($1,584,229.37) Uniswap (UNI)
- **From** Black Hole: 0x000... **To** Indexed: DEFI5 To... **For** 103,560.658042801523009688 ($360,589.45) DEFI Top 5 T... (DEFI5)
- **From** Indexed: DEFI5 To... **To** 0x277e851587eb5... **For** 103,560.658042801523009688 ($360,589.45) DEFI Top 5 T... (DEFI5)
- **From** 0x277e851587eb5... **To** Indexed: DEFI5 To... **For** 91,857.134192973022926319 ($2,376,344.06) Uniswap (UNI)
- **From** Black Hole: 0x000... **To** Indexed: DEFI5 To... **For** 121,025.476726414824039859 ($421,400.47) DEFI Top 5 T... (DEFI5)
- **From** Indexed: DEFI5 To... **To** 0x277e851587eb5... **For** 121,025.476726414824039859 ($421,400.47) DEFI Top 5 T... (DEFI5)
- **From** 0x277e851587eb5... **To** Indexed: DEFI5 To... **For** 137,785.701289459534389479 ($3,564,516.09) Uniswap (UNI)

- **From** Black Hole: 0x000… **To** Indexed: DEFI5 To… **For** 141,435.621341864361582035 ($492,466.86) DEFI Top 5 T… (DEFI5)
- **From** Indexed: DEFI5 To… **To** 0x277e851587eb5… **For** 141,435.621341864361582035 ($492,466.86) DEFI Top 5 T… (DEFI5)
- **From** 0x277e851587eb5… **To** Indexed: DEFI5 To… **For** 206,678.551934189301584218 ($5,346,774.14) Uniswap (UNI)
- **From** Black Hole: 0x000… **To** Indexed: DEFI5 To… **For** 165,287.801588912803499104 ($575,518.14) DEFI Top 5 T… (DEFI5)
- **From** Indexed: DEFI5 To… **To** 0x277e851587eb5… **For** 165,287.801588912803499104 ($575,518.14) DEFI Top 5 T… (DEFI5)
- **From** 0x277e851587eb5… **To** Indexed: DEFI5 To… **For** 310,017.827901283952376327 ($8,020,161.21) Uniswap (UNI)
- **From** Black Hole: 0x000… **To** Indexed: DEFI5 To… **For** 193,162.493966498250165646 ($672,575.46) DEFI Top 5 T… (DEFI5)
- **From** Indexed: DEFI5 To… **To** 0x277e851587eb5… **For** 193,162.493966498250165646 ($672,575.46) DEFI Top 5 T… (DEFI5)
- **From** 0x277e851587eb5… **To** Indexed: DEFI5 To… **For** 465,026.741851925928564491 ($12,030,241.81) Uniswap (UNI)
- **From** Black Hole: 0x000… **To** Indexed: DEFI5 To… **For** 210,374.204745766242860969 ($732,505.18) DEFI Top 5 T… (DEFI5)
- **From** Indexed: DEFI5 To… **To** 0x277e851587eb5… **For** 210,374.204745766242860969 ($732,505.18) DEFI Top 5 T… (DEFI5)

Next, the caller used the borrowed SUSHI to mint additional DEFI5 at the extremely inflated valuation caused by the minimum balance exploit, then burned the DEFI5 for all of the underlying assets, and repeated this a number of times.

- **From** SushiSwap: SUSHI **To** 0x277e851587eb5… **For** 220,000 ($2,327,600.00) SushiToken (SUSHI)
- **From** 0x277e851587eb5… **To** Indexed: DEFI5 To… **For** 220,000 ($2,327,600.00) SushiToken (SUSHI)
- **From** 0x277e851587eb5… **To** Indexed: DEFI5 To… **For** 1,397,888.611775446039302736 ($4,867,329.85) DEFI Top 5 T… (DEFI5)
- **From** Indexed: DEFI5 To… **To** 0x78a3ef33cf0333… **For** 6,989.443058877230196514 ($24,336.65) DEFI Top 5 T… (DEFI5)
- **From** Indexed: DEFI5 To… **To** Black Hole: 0x000… **For** 1,390,899.168716568809106222 ($4,842,993.20) DEFI Top 5 T… (DEFI5)
- **From** Indexed: DEFI5 To… **To** 0x277e851587eb5… **For** 1,831,566.343330240617728547 ($47,382,621.30) Uniswap (UNI)
- **From** Indexed: DEFI5 To… **To** 0x277e851587eb5… **For** 205,385.621985262857206477 ($61,901,930.08) Aave Token (AAVE)
- **From** Indexed: DEFI5 To… **To** 0x277e851587eb5… **For** 42,277.174548189683442085 ($13,114,802.32) Compound (COMP)
- **From** Indexed: DEFI5 To… **To** 0x277e851587eb5… **For** 424,700.988319216238210387 ($4,302,221.01) Synthetix Ne… (SNX)
- **From** Indexed: DEFI5 To… **To** 0x277e851587eb5… **For** 3,549,411.530679908933793216 ($10,089,480.73) Curve DAO To… (CRV)
- **From** Indexed: DEFI5 To… **To** 0x277e851587eb5… **For** 5,760.130630049946860487 ($14,516,278.00) Maker (MKR)
- **From** Indexed: DEFI5 To… **To** 0x277e851587eb5… **For** 197,554.69769457460566 ($2,090,128.70) SushiToken (SUSHI)
- **From** Black Hole: 0x000… **To** Indexed: DEFI5 To… **For** 67,499.684519332941363234 ($235,028.19) DEFI Top 5 T… (DEFI5)
- **From** Indexed: DEFI5 To… **To** 0x277e851587eb5… **For** 67,499.684519332941363234 ($235,028.19) DEFI Top 5 T… (DEFI5)
- **From** 0x277e851587eb5… **To** Indexed: DEFI5 To… **For** 11,222.65115271269717 ($118,735.65) SushiToken (SUSHI)
- **From** Black Hole: 0x000… **To** Indexed: DEFI5 To… **For** 96,331.350683206931920918 ($335,417.61) DEFI Top 5 T… (DEFI5)
- **From** Indexed: DEFI5 To… **To** 0x277e851587eb5… **For** 96,331.350683206931920918 ($335,417.61) DEFI Top 5 T… (DEFI5)
- **From** 0x277e851587eb5… **To** Indexed: DEFI5 To… **For** 16,833.976729069045755 ($178,103.47) SushiToken (SUSHI)
- **From** Black Hole: 0x000… **To** Indexed: DEFI5 To… **For** 137,478.111053884057334209 ($478,687.15) DEFI Top 5 T… (DEFI5)
- **From** Indexed: DEFI5 To… **To** 0x277e851587eb5… **For** 137,478.111053884057334209 ($478,687.15) DEFI Top 5 T… (DEFI5)

Finally, they paid off the flash loans and made out with about $11m worth of assets.

The CC10 exploit was essentially the same thing, except that the initial re-index step had already been done.

Moving Forward

The fix for the contract seems pretty straightforward in terms of preventing any future attacks against this mechanism. We will modify the controller smart contracts to remove the approximate value function and replace it with one that takes the combined value of the balances held by a pool in every token it owns. Additionally, the mere fact that it was possible to do both a re-index and a minimum balance update in the same transaction is — in retrospect — unsafe: it should have a minimum wait time of at least a day or two. A lot of Ethereum developers we respect have reached out offering help since the attack occurred, and we will seek out as much feedback on the new code as we can before submitting it for governance approval.

As for compensating people who lost funds, this is — so soon after the event — still up in the air. The core team will be discussing with the community how best to handle this situation (as well as talking with similarly affected protocols for insights into their own approaches), and we will hopefully have a proposal for governance soon. We realise that this is far from a concrete action plan, but we need to get our heads on straight first.

Defi

THIS IS **EXHIBIT "8"** TO
THE AFFIDAVIT OF **LAURENCE DAY**
SWORN BEFORE ME
THIS 9th DAY OF DECEMBER, 2021

A COMMISSIONER ETC.

@ BogHolder

BogHolder

This is the beginning of your direct message history with @BogHolder.

No servers in common · Remove friend Block

15 September 2021

Norsefire 15/09/2021

I am, sorry, this got buried in my messages

I need to dig it out, you're right, it's not on the deployments list

I do, what do you want to know about them in particular?

Hnngh I'd need to fish out what the time1 and time2 parameters are again (it's been a while since I dug into them), and it's admittedly 01:15 and I'm not at my machine

Hm

Ping this to d1ll0n

He wrote these oracles, I'm just familiar with them, he'll know the exact details, but to answer THIS one, yeah we call updatePrice 24 hours in advance since we use the TWAP

We take the TWAP reading from the oracle for weight determination

No worries: if he hasn't messaged you with a response I'll ping him about it when we're due to head into some meetings tomorrow

No worries :3 What's the use case for you, out of interest? Sell into the unbound token seller, or?

Fair

24 September 2021

Norsefire 24/09/2021

Anyone can call an oracle update/reindex - it's three weekly reweighs and then a reindex - they're all due

Hang on a tick

Yeah so they're all due an oracle update, which I can do as soon as I'm transferred some ETH from core Gnosis

Alternatively you can update the oracle yourself using updateCategoryPrices(1) for CC10 and DEFI5 on the core controller

So that's for pools like DEGEN, NFTP and FFF, which aren't controlled by the DAO directly but rather a committee of people

The FFF can get force-reindexed because it's only got five members, but that wouldn't be helpful because there's nothing that'd come in or out

As examples:

DEGEN - https://legacy.indexed.finance/category/sigma-v10x1
NFTP - https://legacy.indexed.finance/category/sigma-v10x2
The assets that are scored and considered for inclusion in a reindex are available from the controller for that pool, let me show you an example
https://etherscan.io/address/0x5b470a8c134d397466a1a603678dadda678cbc29#readProxyContract - this is the Sigma controller, which maintains the lists of candidate assets for DEGEN/NFTP
method 21: `getTokenList`

arg 1 for DEGEN, arg 2 for NFTP

shows you all of the candidate assets - for those two the current list and candidate list are the same because there's only 10 candidates
https://etherscan.io/address/0xf00a38376c8668fc1f3cd3daeef42e0e44a7fcdb#readProxyContract - here's the core controller, which maintains CC10/DEFI5/ORCL5

method 10: `getCategoryTokens`

arg 1 for CC10, 2 for DEFI5, 3 for ORCL5

you'll see in all of those cases there are more than 10/5/5 options
[don't ask me why the method for querying these isn't consistent across controllers, lul]
so yeah if we do a reindex (either scheduled or forced), that's where the list of candidates comes from
whether it's updated immediately before [because there's some emergency] or through a governor alpha vote - for core indices - or just the sigma committee - for the sigma ones - at some arbitrary beforehand time doesn't make a difference

Norsefire 12/10/2021
yeee it'll always reflect whatever's currently the maximal set of stuff under consideration
the reindex just narrows the scope to bind weights
and the reweighting just adjusts weights within that current selected scope
i'm finna write a little docs addition expanding on this with a dumb example like "scoring is based on letters within a token name"
just to make it real simple, because i'm hearing this a lot as people start learning more
oh just 'how are tokens selected for inclusion/phasing out, where are the candidate lists stored'
asking questions about the sigma versus core stuff implies that someone actually knows what's up
and i can go a bit deeper
right brb, dinner for waifu
what i'll do is shove an update to degen and nftp tomorrow anyway, since they're overdue
but yeah there's no pressing urgency for these things to always be banged on the dot [i mean, ideally they always would, but gas is fuuuuuuuuuuuck]
i have spent more than a minute of my life praying that once everything's finally upgraded and evolved, we're not too far from mainnet zkrollups that i can use for maintenance

It'd just be a force-adjusted reweight

There was a reindex recently that introduced Sushi to CC10 and unbound BAT

https://etherscan.io/tx/0xe90bc17193f2fff73eb64b103700bb6db5364af6cf4f81252420021861101a85 This one specifically

> Ethereum (ETH) Blockchain Explorer
>
> **Ethereum Transaction Hash (Txhash) Details | Etherscan**
>
> Ethereum (ETH) detailed transaction info for txhash 0xe90bc17193f2fff73eb64b103700bb6db5364af6cf4f81252420021861101a85. The transaction status, block confirmation, gas fee, Ether (ETH), and token transfer are shown.

Can do, but will need to update the oracles and sit the new committee down and show them what they need to approve to make it happen

I don't sit on that committee anymore, but it's simple to do - there are no additional assets in either of them, mind, so it won't drag anything in or out (edited)

the forceReindex is there in the event of an attack that necessitates very quickly introducing something else and removing the weight binding of an existing token

I'll mention it

4 October 2021

Norsefire 04/10/2021

i can update the oracle for everything tonight and do a reweigh of DEFI5/CC10/ORCL5 after 24 hours - that'll be a reindex for ORCL5

7 October 2021

Norsefire 07/10/2021

just been waiting for gas to go down a bit

Norsefire 07/10/2021

https://etherscan.io/tx/0x4dfebbe16a1139091c09b424ff76f39928279fc08eb88b104dc0ff1c438d404b

> Ethereum (ETH) Blockchain Explorer
>
> **Ethereum Transaction Hash (Txhash) Details | Etherscan**
>
> Ethereum (ETH) detailed transaction info for txhash 0x4dfebbe16a1139091c09b424ff76f39928279fc08eb88b104dc0ff1c438d404b. The transaction status, block confirmation, gas fee, Ether (ETH), and token transfer are shown.

here's a reindex for ORCL5

https://etherscan.io/tx/0x9b4cbde9aa7baee9a3389cdb3a099e04217031d6a7aa8b484079a881a69e30a0

> Ethereum (ETH) Blockchain Explorer

here's a re*weigh* for CC10

Norsefire 07/10/2021

Same kinda story as the core controller, but individual pools can have separate strategies assigned to them for scoring (core controller is just FDV), and there's a multisig that can add and remove assets rather than relying on Governor Alpha

No

The reindex considers whatever list is currently logged by the controller as being candidates: we can add stuff whenever, and being added doesn't guarantee that something will get included unless you also remove enough tokens from the list that you've got to use the new one to fill up the minimum number of assets with weights bound

So, CC10 has something like 16 assets right now in the candidate list, but only 10 with weights bound

DEGEN actually only has that list of 10: beforehand it had a bunch more but they were removed by the multisig committee to allow for less pricey reindexes once we realised that we need to update our oracle to really capture a wider range of things

Yeah it needs to be in the candidate list AND score in the top N to be bound (edited)

Weekly reweights just shift weights around what's already bound

Reindexes can bind and remove

Gas tbh, last updates for DEGEN and NFTP were 25th Sept I think

FFF needs a force reindex from the Sigma controller to adjust weights (my fault, goofed the scoring strat, everything else is perfectly safe, just requires a governance vote to upgrade the scoring strategy), but the amounts haven't moved around enough in terms of weights to justify the faff- which is why it hasn't been reweighed or reindexed in a while (edited)

(Reindexing the FFF would do nothing other than change weights: it only has those five candidate assets that are currently in it, so it's just a weight shift)

It's literally just down to "I'm paying 0.12 ETH plus some LINK to update oracles for reweights in this environment"

zk-rollups pls

The FFF can be fixed, just needs a proxy update and *some spare time*

lmao yeah CC10 has been trying to arb in SUSHI for weeks now

"No profitable arb found after gas" is basically stamped on my monitor

Hey you're helping out

Benefits me for you to understand it

Yeee we chatted about it

12 October 2021

Norsefire 12/10/2021

There's nothing for us to do an `addTokens` for right now [it'd need to be discussed by the Sigma committee anyway, and the understanding is that they'll hold off on considering any new assets to add to indices such as DEGEN/NFTP until the metaoracle is out - anything that they'd *want* to add we can't do right now]

Is there a particular reason you want a force reindex rather than just a regular reweigh?

THIS IS **EXHIBIT "9"** TO
THE AFFIDAVIT OF **LAURENCE DAY**
SWORN BEFORE ME
THIS 9th DAY OF DECEMBER, 2021

Stephen [illegible]

A COMMISSIONER ETC.

Deleted User 1ef53cc9

September 11, 2021

9:22 PM d1ll0n It's under "Proxy Implementations" https://docs.indexed.finance/index-pool-smart-contracts/deployments#proxy-implementations there's a separate one for each pool

d1ll0n ah yeah that's missing on the docs, will add that one sec

d1ll0n here's the proxy implementation for UnboundTokenSeller for core pools (defi5/cc10/orcl5) 0x2F0869D7AFd6638d2c83Fb2bfD79d5956D0cB952

d1ll0n if you want to make a bot for it you can make some free moneys

d1ll0n the seller contracts for a few of the pools have some tokens built up

d1ll0n you get a 2% premium on the twap recorded for the token

d1ll0n https://etherscan.io/address/0xF00A38376C8668fC1f3Cd3dAeef42E0E44A7Fcdb#readProxyContract
Use `computeSellerAddress` with the pool address

d1ll0n you can do the same with the sigma controller

d1ll0n yeah, for the sigma pools

d1ll0n the ones that don't have a number at the end of the name

d1ll0n as for volume, they only get tokens when other tokens leave the pool, so not that much, but I think there's a couple hundred k worth of shit in all the seller contracts atm

d1ll0n sigma pools let us use arbitrary contracts to choose token weights

d1ll0n core controller always uses sqrt fdv

d1ll0n awesome, lmk how it goes

d1ll0n also keep in mind you will have to update the oracle to use it

d1ll0n it queries the token TWAP from the oracle then prices the swap on that

d1ll0n and gives you any premium if you tell it to sell on uniswap, or lets you trade with it directly

d1ll0n always uses twap + 2% as the amount it's willing to pay

September 15, 2021

2:09 PM d1ll0n Hey! Sorry man didn't notice your messages yesterday

Original message was deleted.

2:11 PM d1ll0n Right so when you query a price with the params (20 min, 2 days), the oracle will look for a price observation that was recorded between 20 minutes and 2 days ago. If it doesn't find one, it will revert

d1ll0n if you update the price, that creates a price observation and records the time it was made

d1ll0n so if you query the price from 20 min to 2 days ago, it won't use the price you just updated a second ago because that's not 20 min old

2:20 PM d1ll0n Another little snag with the way this works is that it stores prices at the index for the hour, and when it searches it will begin the search at the hour prior to the lowest timestamp it could be at.

This means if you update the price at 11:55 and query the price at 12:16 with minTimeElapsed = 20 minutes, it will actually start looking for prices at 10.

If the price could be in the current hour, though, it will start looking there. So if you update the price at 12:10 and query it at 12:30 with minTimeElapsed=20 minutes, it will find the price at 12:10. (edited)

d1ll0n the reason for this is a kind of poor design decision in the way the query function works where I was prioritizing gas cost minimization over basically everything, and I was expecting the oracle to be nearly exclusively using TWAPs with a duration of several hours to several days or even weeks

d1ll0n you can see how this works by checking the `getLastPriceObservation` function. If the price could be in the current hour (the conditional block `if (canBeThisWindow || mustBeThisWindow) { ... }`) then it looks there, otherwise it takes the time `block.timestamp - minTimeElapsed` and uses `findLastSetKey` to get the last price within range, and that function uses a bitmap search function to find the last set bit in a uint256 to the left of (exclusive) the starting index

d1ll0n call the oracle to check if the price is ready and decide whether the swap is profitable you mean, right? if so then yes

d1ll0n awesome! thanks for working on this

d1ll0n I'll have to check with the team but I think we'd be happy to give you a small grant as a little extra incentive to get this thing operational. The bot should be profitable for you to run either way but it might give you a little extra bit of incentive to get it up and running sooner than later

d1ll0n oh I should also mention that when you update the oracle, you will need to also update it for one of the tokens that are still in the pool

d1ll0n because it will only let you swap between the token being sold and one of the tokens in the pool for the seller

d1ll0n do you know how to get the list of tokens in the seller contract btw

d1ll0n allow me to speed it along then 😄
the seller contract doesn't track what it owns because doing so would add gas costs to swaps (since tokens are sent to it as a result of post-swap hooks) so you will have to query thegraph

d1ll0n UI version https://thegraph.com/legacy-explorer/subgraph/indexed-finance/indexed
API https://api.thegraph.com/subgraphs/name/indexed-finance/indexed

You can get the list of token addresses for each seller, as well as the addresses of the seller contracts, with the query

```
{
  indexPool(id: "index_pool_address") {
    tokenSeller {
      id
      tokensForSale {
        token {
          id
        }
      }
    }
  }
}
```

d1ll0n and here's an example repo for how to query thegraph if you're not familiar with that https://github.com/indexed-finance/subgraph-clients/tree/master/src/core

September 24, 2021

10:14 PM d1ll0n Hey, sorry was asleep all day
d1ll0n yeah we can reindex, will get back to you on that soon

September 25, 2021

7:51 PM d1ll0n Hey sorry for the delay. Why do you need it reindexed again?
d1ll0n That doesn't really affect the unboundtokenseller aside from initiating the process for tokens to be removed
d1ll0n the circulating mcap oracle is used for weighting not for pricing stuff in the seller

September 29, 2021

11:10 AM d1ll0n Sorry been dealing with a lot this week and sleeping a bunch. So with the mcap oracle you linked, that is just the contract for a specific index. I forget which one it is though - you know which index it is so I can trigger the reindex?
d1ll0n also it might be easier for you to test against a reindex if you just do a mainnet fork and test one of the core index pools, that way you can just trigger an oracle update, fast forward to when the pool can reweigh, and do that enough times that it's ready for a reindex
d1ll0n oh also, I think I forgot to mention - we did discuss a grant for you to build this, we were thinking $2k, what do you think?

October 1, 2021

12:20 AM d1ll0n So with DEGEN that actually isn't a bug. It could have many more tokens but we just have not added more yet. We've worked with redphone to determine the candidates list and that index in particular has been more targeted than most, with the asset list generally being directly chosen rather than provided as a large list to be narrowed down
d1ll0n sorry for always taking so long to get back to you I just have a completely fucked sleep schedule

Original message was deleted.
12:22 AM d1ll0n No it should. The Sigma controller has a feature that the original controller did not, which is that each list can define a minimum and maximum score value which will automatically boot tokens out of the list. We added this because redphone wanted DEGEN to only cover tokens in a specific range of mcaps, and the Sigma ctrlr was designed with DEGEN in mind

Original message was deleted.
10:35 AM d1ll0n redphonecrypto is a twitter influencer guy who came up with the idea for degen
d1ll0n we do tend to manually update the token list yeah, but not every month necessarily
d1ll0n kk
d1ll0n oh and for the grant we didn't discuss how to structure it, like if it would be up-front or based on some kind of milestones
d1ll0n also we did have one condition for it which is that you share the code with us so that if you ever stop running it we can turn it back on
d1ll0n if that works for you I'll ask em how we want to handle payment
d1ll0n awesome, that's perfect
d1ll0n wouldn't expect you to make the repo public just want to be sure we can keep the gears turning if you ever decide to shut it off
d1ll0n gracias
d1ll0n alright so just chatted with the team
d1ll0n I mentioned $2k before but tbh this is very valuable so we're fine with doubling that
d1ll0n if you can show me the code today so I can just verify it's had a decent amount of work put in already, I'll send you $2k worth of NDX today
d1ll0n and then we'll send the other 2k whenever you're done
d1ll0n cool, ty

October 6, 2021

Original message was deleted.
6:40 AM d1ll0n yeah looks like a good start, how long do you think it'll be before it's operational? also give an eth addr for tokens

October 10, 2021

12:28 AM d1ll0n apologies
d1ll0n https://etherscan.io/tx/0x95fc640647a3fed71e843b1755c90278c124a10955a35086d25f01d90164d490

> Ethereum (ETH) Blockchain Explorer
> **Ethereum Transaction Hash (Txhash) Details | Etherscan**
> Ethereum (ETH) detailed transaction info for txhash 0x95fc640647a3fed71e843b1755c90278c124a10955a35086d25f01d90164d490. The transaction status, block confirmation, gas fee, Ether (ETH), and token transfer are shown.

d1ll0n sent you usdc instead of ndx because the price isn't very stable, can swap it if you prefer ndx

October 16, 2021

12:28 AM d1ll0n https://hackmd.io/@laurenceday/H1OylawSF
want to talk?

> HackMD

THIS IS **EXHIBIT "10"** TO
THE AFFIDAVIT OF **LAURENCE DAY**
SWORN BEFORE ME
THIS 9th DAY OF DECEMBER, 2021

Stephen Ayford

A COMMISSIONER ETC.

Update #1: Indexed Finance Attack

Here's what we know so far about the identity of the Indexed exploiter, efforts that have been made to reach out, and a few points about the safety of the unaffected Indexed pools.

Update [06:05 BST, 16th October]: we have identified the Indexed attacker and issued an ultimatum. Details available here: https://hackmd.io/@laurenceday/H1OylawSF (https://hackmd.io/@laurenceday/H1OylawSF)

Status Of Remaining Pools

The important stuff first - safety of other pools.

ORCL5 is subject to the same exploit (as an index that is operated by the MarketCapSqrtController contract on the core controller), however the event horizon for this attack to be replicated requires at least another month to have elapsed, as it was reindexed on the 5th of October.

DEGEN and NFTP also contain the same core vulnerability within their controller, however the attack in question requires that there are candidate assets available to be phased in: this is not the case for these two pools - the active asset list and the candidate asset list is the same. Tokens can only be added by a 3/5 Sigma committee vote [through this Gnosis: 0xbb22a47842eafc9672132692805O9a8b28e57076], and suffice it to say, that will not be happening.

These pools can be considered 'safe', and we will be able to upgrade them through a Governor Alpha vote once the patch has been produced and reviewed before any adverse events can befall them - however, apprehension is absolutely understandable for those that wish to exit these positions out of caution.

Exploiter Identity

The knife twist is that we've realised that we believe that we actually know who did this: we spoke to them quite a bit prior to the execution of this attack.

Starting on the 15th of September, we were approached by a Discord user under the name 'UmbralUpsilon' - currently BogHolder#1688 -, asking some questions about the way in which certain parameters were utilised in the TWAP oracle (although the oracle was not part of the attack, this is the topic that they opened with). Since every component of Indexed is open-source, we answered these questions, and upon asking the reason, were told that they were attempting to create an arbitrage bot for the pools.

This is a key part of how Indexed generates revenue (exit fees on burns when arbitraging the NAV of tokens and their value on DEXes), and we were happy to engage with queries about the mechanics, explaining how reindexes work, the timing of reweights, how tokens are added and removed from candidate asset lists, and so on. We had no reason to be alarmed: all of these conversations were in the spirit of open-source collaboration.

In the aftermath of the attack, the two of us in Core that engaged in these conversations (Dillon and Laurence) have found that this users side of the conversations have been deleted in their entirety. However, in the interests of full disclosure, I (Laurence) attach the entirety of my side of the conversation: https://imgur.com/a/z4AZJlk (http //imgur com/a/z4AZJlk)

We are aware (courtesy of @pcaversaccio (http //twitter com/pcaver accio)) that the e ploiter requested some Kovan testnet Ether via Gitter, using the (dead, presumably created for the purposes of the assault) Twitter account @ZetaZeroes. We have reached out to them via Gitter with the following message: https://imgur.com/a/rhUHQY2 (http //imgur com/a/rhUHQY2).

We have also reached out directly to the e ploiter (0 ba5ed1488be60ba2facc6b66c6d6f0befba22ebe) with a message: https://etherscan.io/t /0 50af8eb95eeebf2ceb8e5a141841ad5bde7ddcc0bdc206ad761322cb26e4ec75 (http //ether can io/tx/0x50af8eb95eeebf2ceb8e5a141841ad5bde7ddcc0bdc206ad761322cb26e4ec75) but given that subsequent to that they deployed another contract and attempted to perform more interactions, we must assume ongoing hostility.

We speak now directly to the e ploiter, if they ever read this: you’re clearly incredibly skilled: this is something that has been overlooked for ten months in production, and you’re the only one that found it. While it would have been so much more productive for you to instead choose to work with us: be the antihero of this story rather than the villain. Take a 10% whitehat, and save a lot of people the effort of engaging law enforcement.

The people that are affected by this are those that are trying to diversify risk within a volatile space. That’s part of what makes this particularly cruel: no one deserves to have their funds whisked away, but the conte t here is an irony that can’t be ignored.

Our door’s open, and it’ll make a much more satisfying footnote to our appearance on Rekt.

Conclusion

This is all we have for now. We'll keep this file updated with additional details/updates as and when we have them.

For completeness, relevant links:

Post mortem: https://twitter.com/nd fi/status/1448856180697280514 (http //twitter com/ndxfi/ tatu /1448856180697280514)

Rekt article: https://rekt.news/inde ed finance rekt/ (http //rekt new /indexed finance rekt/)

Statement on path forward: https://twitter.com/nd fi/status/1449160684852453384 (http //twitter com/ndxfi/ tatu /1449160684852453384)

THIS IS **EXHIBIT "11"** TO
THE AFFIDAVIT OF **LAURENCE DAY**
SWORN BEFORE ME
THIS 9th DAY OF DECEMBER, 2021

Stephen Aylward

A COMMISSIONER ETC.

hickuphh3 16/10/2021

So, the alleged exploiter bogholder is a fairly competent C4 warden. He received 4,620.53 USDC (and more) for the badger contest. USDC payouts were distributed a couple of days ago on Polygon. Seems like he used `0x3c86b2b86f0a4b180802026cb1d0d73f80200ab3`. If u check that address on mainnet, u'd see 4 tornado cash transfers that are suspiciously close to the time of funds received by the exploiter.

Might wanna get in touch with the C4 guys as they might have interacted with him as well.

THIS IS **EXHIBIT "12"** TO
THE AFFIDAVIT OF **LAURENCE DAY**
SWORN BEFORE ME
THIS 9th DAY OF DECEMBER, 2021

Stephen Aylward

A COMMISSIONER ETC.

Overview | Internal Txns | Logs (3) | Access List | State | Comments

Transaction Hash:	0x58086d485fa8ea77bac3b53ae9b12fd69659d3b5feec6bbffdee17ea5a2810f7
Status:	Success
Block:	13413633 207252 Block Confirmations
Timestamp:	32 days 12 hrs ago (Oct-14-2021 02:13:54 AM +UTC) | Confirmed within 30 secs
From:	0x3c86b2b86f0a4b180802026cb1d0d73f80200ab3
To:	Contract 0x722122df12d4e14e13ac3b6895a86e84145b6967 (Tornado.Cash: Proxy) └ TRANSFER 1 Ether From Tornado.Cash: P... To → Tornado.Cash: 1...
Value:	1 Ether ($4,700.73)
Transaction Fee:	0.076725253212813842 Ether ($360.66)
Gas Price:	0.000000080079127219 Ether (80.079127219 Gwei)
Txn Type:	2 (EIP-1559)
Ether Price:	$3,791.23 / ETH

Click to see More

Overview | Internal Txns | Logs (2) | Access List | State | Comments

Transaction Hash:	0xbceef471c174aef7f75183feab142358baf06e0a430f05f2630ea06c3d1f6341
Status:	Success
Block:	13414635 206235 Block Confirmations
Timestamp:	32 days 8 hrs ago (Oct-14-2021 06:02:52 AM +UTC) | Confirmed within 30 secs
From:	0x49136693081f2c18e2cf14428dd78cd90a22dc1f
To:	Contract 0x722122df12d4e14e13ac3b6895a86e84145b6967 (Tornado.Cash: Proxy) └ TRANSFER 0.9702639 Ether From Tornado.Cash: 1... To → Indexed Finance Expl... └ TRANSFER 0.0297361 Ether From Tornado.Cash: 1... To → 0x49136693081f2c18e2cf14428...
Value:	0 Ether ($0.00)
Transaction Fee:	0.033027347059864656 Ether ($155.23)
Gas Price:	0.000000082270958136 Ether (82.270958136 Gwei)
Txn Type:	2 (EIP-1559)
Ether Price:	$3,791.23 / ETH

Click to see More

Transaction Hash:	0x689e23978d0e9fea3e2b3b7eaf0863a294ef30c7e2d47e9f3d974eafdfd9efcb
Status:	Success
Block:	13415329 205562 Block Confirmations
Timestamp:	32 days 5 hrs ago (Oct-14-2021 08:42:09 AM +UTC) | Confirmed within 30 secs
From:	0x3c86b2b86f0a4b180802026cb1d0d73f80200ab3
To:	Contract 0x722122df12d4e14e13ac3b6895a86e84145b6967 (Tornado.Cash: Proxy) TRANSFER 1 Ether From Tornado.Cash: P... To → Tornado.Cash: 1...
Value:	1 Ether ($4,701.49)
Transaction Fee:	0.071064488835698036 Ether ($334.11)
Gas Price:	0.000000074170915102 Ether (74.170915102 Gwei)
Txn Type:	2 (EIP-1559)
Ether Price:	$3,791.23 / ETH

Click to see More

Overview | Internal Txns | Logs (2) | Access List | State | Comments

Transaction Hash:	0x0fff3e26653bfaa6e8c6abc0498eea66cdb29c6dcd727d581d43bf1ad2ce4372
Status:	Success
Block:	13416974 203906 Block Confirmations
Timestamp:	31 days 23 hrs ago (Oct-14-2021 02:56:28 PM +UTC) | Confirmed within 30 secs
From:	0x3f6ea4a39ce386505d00db7a9c91d90355b4df5d
To:	Contract 0x722122df12d4e14e13ac3b6895a86e84145b6967 (Tornado.Cash: Proxy) └ TRANSFER 0.9521384 Ether From Tornado.Cash: 1... To → Indexed Finance Expl... └ TRANSFER 0.0478616 Ether From Tornado.Cash: 1... To → 0x0b97abcab8675c425668863d...
Value:	0 Ether ($0.00)
Transaction Fee:	0.042388868419109978 Ether ($199.25)
Gas Price:	0.000000111856375691 Ether (111.856375691 Gwei)
Txn Type:	2 (EIP-1559)
Ether Price:	$3,791.23 / ETH

Click to see More ↓

Transaction Hash:	0x2f0f71169c83cc99ce6de4044042e13a83c46a64f458bbd9e5ef9bf031d57f23
Status:	Success
Block:	13416640 204252 Block Confirmations
Timestamp:	32 days 59 mins ago (Oct-14-2021 01:40:10 PM +UTC) | Confirmed within 3 secs
From:	0x3c86b2b86f0a4b180802026cb1d0d73f80200ab3
To:	Contract 0x722122df12d4e14e13ac3b6895a86e84145b6967 (Tornado.Cash: Proxy) └ TRANSFER 1 Ether From Tornado.Cash: P... To → Tornado.Cash: 1...
Value:	1 Ether ($4,701.49)
Transaction Fee:	0.07323092892606959 Ether ($344.29)
Gas Price:	0.000000076431099043 Ether (76.431099043 Gwei)
Txn Type:	2 (EIP-1559)
Ether Price:	$3,791.23 / ETH

Overview | Internal Txns | Logs (2) | Access List | State | Comments

Transaction Hash:	0x14ba74b734ea0d13b1cf02c9395e6f338465cbd60cd54562429e8fa1b2110000
Status:	Success
Block:	13417464 203420 Block Confirmations
Timestamp:	31 days 21 hrs ago (Oct-14-2021 04:42:06 PM +UTC) | Confirmed within 30 secs
From:	0x03ebd2ea2b9f23669c9eb05c2a1a39f99cbdf372
To:	Contract 0x722122df12d4e14e13ac3b6895a86e84145b6967 (Tornado.Cash: Proxy) └ TRANSFER 0.9279503 Ether From Tornado.Cash: 1... To → Indexed Finance Expl... └ TRANSFER 0.0720497 Ether From Tornado.Cash: 1... To → 0xddbfced30862c0105673b38df...
Value:	0 Ether ($0.00)
Transaction Fee:	0.06994592430288625 Ether ($328.82)
Gas Price:	0.000000184568499625 Ether (184.568499625 Gwei)
Txn Type:	2 (EIP-1559)
Ether Price:	$3,791.23 / ETH

Click to see More

Overview | Internal Txns | Logs (3) | Access List | State | Comments

Transaction Hash:	0x0ac3814426d186c6032ef74b3f827d675e2123fd638a1b6f2fda3812258f0d74
Status:	Success
Block:	13417788 203108 Block Confirmations
Timestamp:	31 days 20 hrs ago (Oct-14-2021 05:58:46 PM +UTC)
From:	0x3c86b2b86f0a4b180802026cb1d0d73f80200ab3
To:	Contract 0x722122df12d4e14e13ac3b6895a86e84145b6967 (Tornado.Cash: Proxy) └ TRANSFER 1 Ether From Tornado.Cash: P... To → Tornado.Cash: 1...
Value:	1 Ether ($4,703.82)
Transaction Fee:	0.10651174244488176 Ether ($501.01)
Gas Price:	0.000000111166274352 Ether (111.166274352 Gwei)
Txn Type:	2 (EIP-1559)
Ether Price:	$3,791.23 / ETH

Click to see More

THIS IS **EXHIBIT "13"** TO
THE AFFIDAVIT OF **LAURENCE DAY**
SWORN BEFORE ME
THIS 9th DAY OF DECEMBER, 2021

Stephen Gifford

A COMMISSIONER ETC.

auditing industry.

Furthering deflationary $ETH on top of #eip1559 , I'll be sponsoring an additional 1000 VETH to wardens of @VaderProtocol https://t.co/99a9N0ZTAH

🔥Mervyn🔥 (@mervynchng89)

frob.eth | Alberto Cuesta Cañada (@alcueca)

C4 contests attract new, unique and complicated projects so it is a perfect learning opportunity... Here projects seriously invest in their security so it is always a motivation to try my best to find bugs in their code.

— Pauliax/Thunder
C4 Warden

Want to learn more?

READ THE DOCS

THIS IS **EXHIBIT "14"** TO
THE AFFIDAVIT OF **LAURENCE DAY**
SWORN BEFORE ME
THIS 9th DAY OF DECEMBER, 2021

Stephen Ayford

A COMMISSIONER ETC.

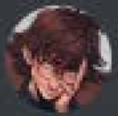
	0x05684028c46dd64a93...	66 days 9 hrs ago	0xc2bc2f890067c511215...	IN	0x3c86b2b86f0a4b1808...	5,770.53	USD Coin (US
	0x229dae21dd9504987e...	66 days 9 hrs ago	0xc2bc2f890067c511215...	IN	0x3c86b2b86f0a4b1808...	1,975.79	USD Coin (USDC)
	0x3d3af511d01931c940...	66 days 13 hrs ago	0xc2bc2f890067c511215...	IN	0x3c86b2b86f0a4b1808...	506.92	USD Coin (USDC)
	0x73efd37439f81922d4a...	66 days 14 hrs ago	0xc2bc2f890067c511215...	IN	0x3c86b2b86f0a4b1808...	459.97	USD Coin (USDC)
	0x1e28e01bc86d577901...	67 days 6 mins ago	0xc2bc2f890067c511215...	IN	0x3c86b2b86f0a4b1808...	1,428.96	USD Coin (USDC)
	0x1b08498a87569c8687...	67 days 1 hr ago	0xc2bc2f890067c511215...	IN	0x3c86b2b86f0a4b1808...	6,263.38	USD Coin (USDC)
	0xe57480f34d6067c2d1...	67 days 2 hrs ago	0xc2bc2f890067c511215...	IN	0x3c86b2b86f0a4b1808...	1,773.9	USD Coin (USDC)

0xc2bc2f890067c511215f9463a064221577a53e10

THIS IS **EXHIBIT "15"** TO
THE AFFIDAVIT OF **LAURENCE DAY**
SWORN BEFORE ME
THIS 9th DAY OF DECEMBER, 2021

Stephen Aylward

A COMMISSIONER ETC.



hickuphh3 16/10/2021

The warden list for reports is sorted by award distribution. Here's notional: https://code423n4.com/reports/2021-08-notional/

🤑🎉 Here are awards for Notional.... 🙌

$86,001.08 USDC » @cmichel
$26,838.42 USDC » @0xleastwood
$10,494.54 USDC » @Thunder
$8,405.33 USDC » @BogHolder
$5,709.62 USDC » @Gerard Persoon
$5,609.01 USDC » @Omik
$4,249.68 USDC » @JMukesh
$1,875.00 USDC » @hrkrshnn
$408.66 USDC » @a_delamo
$408.66 USDC » @DefSec

Means that bogholder is tensors.

WARDENS

11 Wardens contributed reports to the Notional code contest:

1. cmichel
2. leastwood
3. pauliax
4. tensors
5. gpersoon
6. Omik
7. Jmukesh
8. hrkrshnn
9. a_delamo
10. LSDan
11. ad3sh_

This contest was judged by ghoul.sol.

Final report assembled by moneylegobatman and ninek.

THIS IS **EXHIBIT "16"** TO
THE AFFIDAVIT OF **LAURENCE DAY**
SWORN BEFORE ME
THIS 9th DAY OF DECEMBER, 2021

Stephen Ayford

A COMMISSIONER ETC.

code-423n4 / code423n4.com Public

<> Code | Issues 20 | Pull requests 14 | Actions | Projects 1 | Wiki | Security | Insights

Create tensors.json

main

mtheorylord1 committed on 24 Jun

Showing **1 changed file** with **5 additions** and **0 deletions**.

5 _data/handles/tensors.json

```
... @@ -0,0 +1,5 @@
1 + {
2 +   "handle": "tensors",
3 +   "image": "./avatars/tensors.jpg",
4 +   "link": "https://twitter.com/Tensors8"
5 + }
```

THIS IS **EXHIBIT "17"** TO
THE AFFIDAVIT OF **LAURENCE DAY**
SWORN BEFORE ME
THIS 9th DAY OF DECEMBER, 2021

Stephen Aylward

A COMMISSIONER ETC.

```
$ git clone https://github.com/mtheorylord/Grade-12-Project
Cloning into 'Grade-12-Project'...
remote: Enumerating objects: 3, done.
remote: Total 3 (delta 0), reused 0 (delta 0), pack-reused 3
Unpacking objects: 100% (3/3), done.
$ cd Grade-12-Project/
$ git log
commit 1f591355a934dbca8288fae2aac5e6ce9bc7c6f9 (HEAD -> master, origin/master, origin/HEAD)
Author: mtheorylord <[redacted]
Date:   Fri Dec 23 09:05:07 2016 -0500

    Initial commit
```

THIS IS **EXHIBIT "18"** TO
THE AFFIDAVIT OF **LAURENCE DAY**
SWORN BEFORE ME
THIS 9th DAY OF DECEMBER, 2021

Stephen Eyford

A COMMISSIONER ETC.

Reach for the Top: Difference between revisions

From Wikipedia, the free encyclopedia

Browse history interactively

Revision as of 17:07, 22 June 2016 (edit)	**Revision as of 14:46, 12 July 2016 (edit) (undo)**
LilHelpa (talk | contribs)	Mtheorylord (talk | contribs)
m *(→Types of questions: Typos and general fixes, replaced: an can → and can using AWB)*	*(→Alumni)*
← Previous edit	Next edit →

Line 162:		**Line 162:**
`*[[Lucie Edwards]], Canadian diplomat`		`*[[Lucie Edwards]], Canadian diplomat`
`*[[Stephen Harper]], former [[Prime Minister of Canada]]`		`*[[Stephen Harper]], former [[Prime Minister of Canada]]`
	+	`*Andean Medjedovic, notable mathematician`
`==See also==`		`==See also==`

THIS IS **EXHIBIT "19"** TO
THE AFFIDAVIT OF **LAURENCE DAY**
SWORN BEFORE ME
THIS 9th DAY OF DECEMBER, 2021

Stephen Ayford

A COMMISSIONER ETC.

THIS IS **EXHIBIT "20"** TO
THE AFFIDAVIT OF **LAURENCE DAY**
SWORN BEFORE ME
THIS 9th DAY OF DECEMBER, 2021

Stephen Ayford

A COMMISSIONER ETC.

Welcome

Welcome to my web page. I'm a masters student at the University of Waterloo studying Pure Mathematics. My supervisor is Michael Rubinstein.

A density plot of the roots of polynomials with coefficients in {1,-1}.

Outside of mathematics I'm interested in cryptocurrency and other decentralized open source software. The hobby I spend by far the most amount of time on is reading.

Trending Tags

#

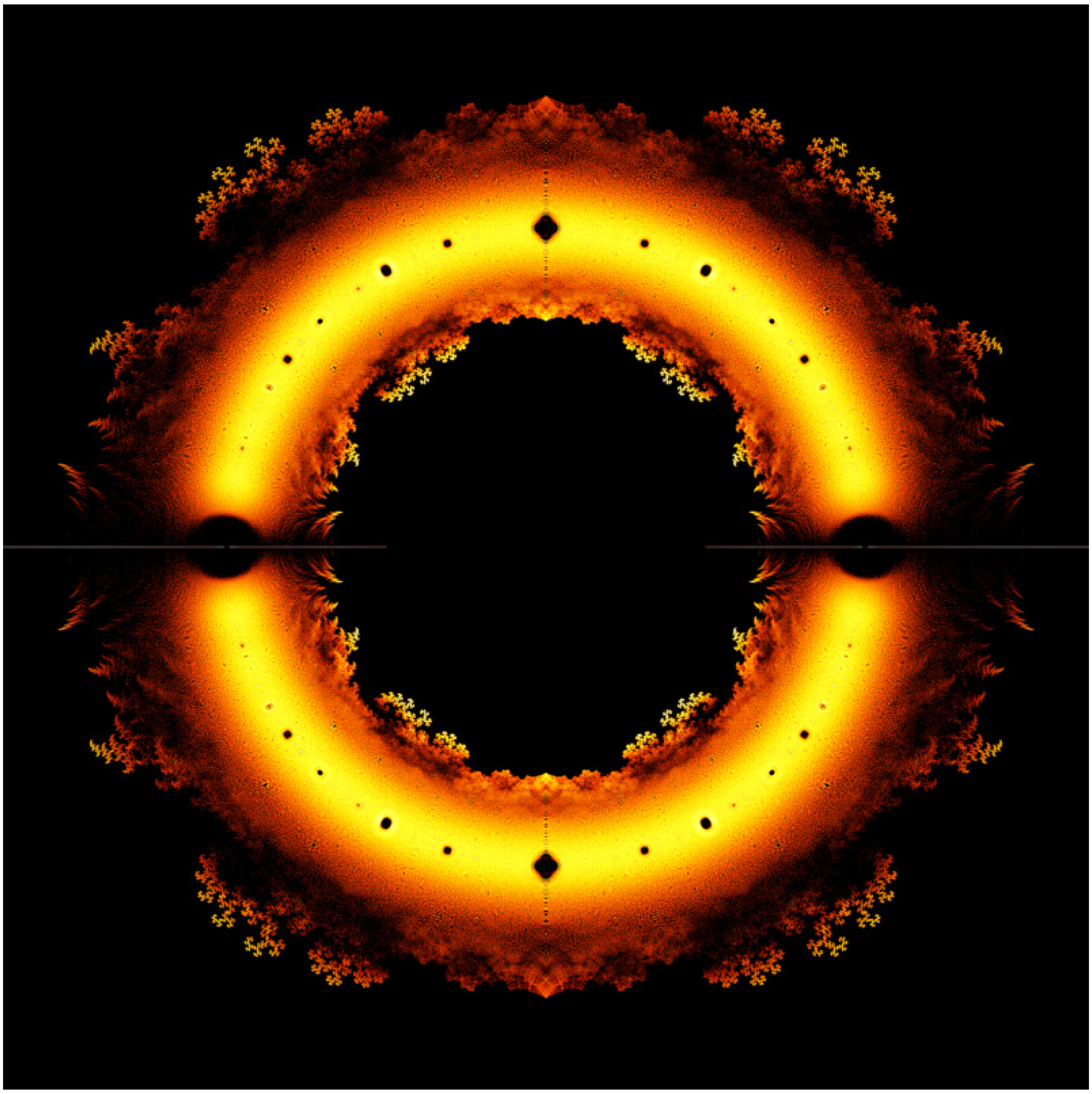
THIS IS **EXHIBIT "21"** TO
THE AFFIDAVIT OF **LAURENCE DAY**
SWORN BEFORE ME
THIS 9th DAY OF DECEMBER, 2021

Stephen Ayford

A COMMISSIONER ETC.

Welcome

Welcome to my web page. I'm a masters student at the University of Waterloo studying Pure Mathematics. My supervisor is Michael Rubinstein.



A density plot of the roots of polynomials with coefficients in {1,-1}.

≡ **Andean E. Medjedovic**

#

Interests

I'm currently interested in both algebraic and analytic number theory.

Lately I've been studying properties of L-functions, divisors sums and connections to random matrix theory.

Contact

Email me at: [redacted]

≡ **About Me**

#

Temporarily removed

Miscellaneous

#

My Master's thesis is on "Exact Formulas for Secular Coefficients". The main result of the paper is a technique that removes singularities that traditionally occur in Random Matrix Theory. Among other things, it allows you to get identities for Secular coefficients. These are conjectured to be related to powers of the zeta function by Montgomery's pair correlation. (Not available yet)

Papers

1. Real Mahler Functions (2020). 22 pages. Link PDF
2. Enumerating Smooth Schubert Varieties (2020), with William Slofstra. 21 pages. Link PDF
3. Sharp Bounds on Edge Partitions of K_n (2020). 9 pages. Submitted to Graphs and Combinatorics. Link PDF
4. Grothendieck's Classification of Line Bundles over the Riemann Sphere (2020). 19 pages. Submitted to Rose-Hulman Undergraduate Journal. Link PDF
5. A Look at Chowla's Problem (2020). 14 pages. Submitted to Involve Journal of Mathematics. Link PDF

Talks and Expositions

Here are slides and write-ups for talks and surveys I have given. Some are presentations to other researchers, some to graduate students, and a few to undergraduates. You'll notice that a few talks correspond to written papers.

1. Line bundles over the complex projective plane. (2018) Link PDF
2. Sparse Cuts and Eigenvectors. (2019 Slides
3. Linear forms in Logs: Chowla's Problem. (2019) Link PDF
4. The Auslander-Buchsbaum Theorem. (2019) PDF
5. Representation Theory of GL_n. (2020) PDF
6. A series of short talks on the RMT related $\gamma_k(c)$ at AIM. (2020) Recording (not yet available)
7. The Mahler Conjecture. (2020) Slides
8. Dimensions of Algberaic Structures (2 Talks). (2021) Slides 1 Slides 2

My personal arXiv page can be found here.

≡ **Papers and Talks**

#

THIS IS **EXHIBIT "22"** TO
THE AFFIDAVIT OF **LAURENCE DAY**
SWORN BEFORE ME
THIS 9th DAY OF DECEMBER, 2021

Stephen Ayford

A COMMISSIONER ETC.

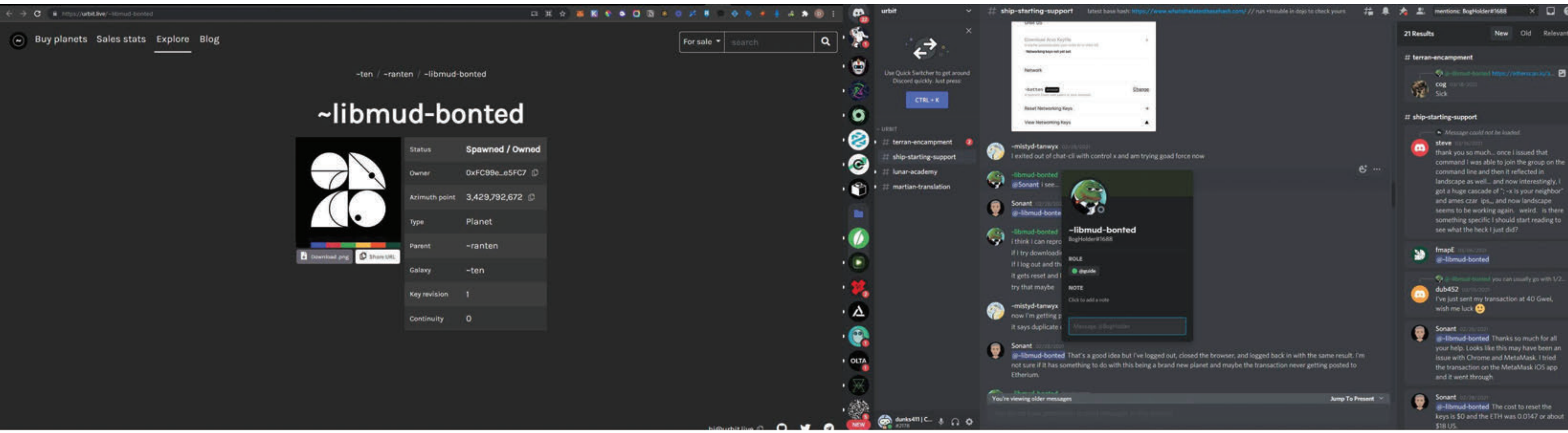
Reverse IP Lookup Results — 2 domains hosted on IP address 149.248.60.232

	Domain	View Whois Record
1.	nontrivial.xyz	
2.	urbitstar.xyz	

THIS IS **EXHIBIT "23"** TO
THE AFFIDAVIT OF **LAURENCE DAY**
SWORN BEFORE ME
THIS 9th DAY OF DECEMBER, 2021

Stephen Gifford

A COMMISSIONER ETC.


Buy planets
Sales stats
Explore
Blog
For sale
~ten / ~ranten / ~libmud-bonted
~libmud-bonted
Status Spawned / Owned
Owner 0xFC99e...e5FC7
Azimuth point 3,429,792,672
Type Planet
Parent ~ranten
Galaxy ~ten
Key revision 1
Continuity 0
urbit
ship-starting-support
terran-encampment
ship-starting-support
lunar-academy
martian-translation
CTRL + K
~libmud-bonted
21 Results
New
Old
Relevant

THIS IS **EXHIBIT "24"** TO
THE AFFIDAVIT OF **LAURENCE DAY**
SWORN BEFORE ME
THIS 9th DAY OF DECEMBER, 2021

Stephen Ayford

A COMMISSIONER ETC.

Overview State Comments

Transaction Hash:	0x44ad4f813d4b3d32c2ef654be4cd5ffe0abc76c06a9490205fecf871e03a5b73
Status:	Success
Block:	11625741 1996359 Block Confirmations
Timestamp:	309 days 11 hrs ago (Jan-10-2021 07:31:54 AM +UTC)
From:	0x7be53cac08462853476e26cc242f502293e52e97
To:	0x3c86b2b86f0a4b180802026cb1d0d73f80200ab3
Value:	0.135254340013916899 Ether ($619.33)
Transaction Fee:	0.001155 Ether ($5.29)
Gas Price:	0.000000055 Ether (55 Gwei)
Ether Price:	$1,255.72 / ETH

Click to see More

Overview | Internal Txns | Logs (2) | State | Comments

Transaction Hash:	0x5da71707adf3a7f2c0c478c5dc35450d21e32e47121b7a84be09e29c7185c33c
Status:	Success
Block:	10452585 3169515 Block Confirmations
Timestamp:	490 days 1 hr ago (Jul-13-2020 05:31:16 PM +UTC)
From:	0x8421ee8986a6517196b1f9521d117f9565c068e4
Interacted With (To):	Contract 0x6ac07b7c4601b5ce11de8dfe6335b871c7c4dd4d
Tokens Transferred:	**From** 0x8421ee8986a65... **To** 0xfc99e43b8d4aa... **For** 3,429,792,672 Azimuth Poin... (AZP)
Value:	0 Ether ($0.00)
Transaction Fee:	0.00421908 Ether ($19.32)
Gas Price:	0.00000004 Ether (40 Gwei)
Ether Price:	$239.53 / ETH

Click to see More

Overview State Comments

Transaction Hash:	0x062eab03eb751fc265b1857719c22217d43736707ce575498c2cf5fe29a71078
Status:	Success
Block:	11532706 2089394 Block Confirmations
Timestamp:	323 days 18 hrs ago (Dec-27-2020 12:52:41 AM +UTC)
From:	0x8421ee8986a6517196b1f9521d117f9565c068e4
To:	0x7be53cac08462853476e26cc242f502293e52e97
Value:	0.089199616 Ether ($408.44)
Transaction Fee:	0.001932 Ether ($8.85)
Gas Price:	0.000000092 Ether (92 Gwei)
Ether Price:	$683.98 / ETH

Click to see More

THIS IS **EXHIBIT "25"** TO
THE AFFIDAVIT OF **LAURENCE DAY**
SWORN BEFORE ME
THIS 9th DAY OF DECEMBER, 2021

Stephen Axford

A COMMISSIONER ETC.

Alice Chu

From: [redacted]
[redacted] Sunday, October 17, 2021 4:15 AM
To: PR0 PR0
Subject: Re: $50k, no charges, no doxx, no losing your university spot

Sounds like a plan.
Send the money over:
0xb7e77cdAf7EBF76dB72571f2D6E43aA5e84a5E64

On Sun, Oct 17, 2021 at 3:38 AM PR0 PR0 <pr0@keychain.me> wrote:

> Hey am contacting you at a personal capacity to offer a way out. Am the lead investor for Indexed and a cofounder. Theres been alot of shit going on, you fucked up your opsec and now have serious problems. The money can never be spent by you no matter what you do now and am sure you just had fun, saw easy money and now it went too far. So heres my proposal, and you should talk to whoever you confide in about it.
>
> 1. $50k bounty to return the money. This money you can actually use.
> 2. Will do my best to get the team to not press any charges, remove what information we can that puts a target on you (again you have committed a crime here so may already be out of our hands somewhat, but return of funds will show remorse and good faith).
> 3. You get easy pr and can maybe do some talks on how you found the vulnerability and get some Crypto rep. You havent moved funds, you haven't actually done any moves at all, so the whitehat cards still a play.
>
> Noone knows reached out, they'll probably be upset, but all you've been getting so fars stick, thought would try a more incentivized approach.

THIS IS **EXHIBIT "26"** TO
THE AFFIDAVIT OF **LAURENCE DAY**
SWORN BEFORE ME
THIS 9th DAY OF DECEMBER, 2021

Stephen Anford

A COMMISSIONER ETC.

.ıll CC 11:58 AM 215

< Inbox [redacted]

Sat Oct 16, 10:56 PM

Completed call

Sat Oct 16, 11:42 PM

Hey

We saw you put the website back up and your age on the resume.

We're not releasing the information today as we didn't want an 18 year old having his phone blown up on our conscience. Rest assured we will be in contact with people you know and you will not get

Type message here

11:58 AM

216

< Inbox [redacted]

away with this. I implore you to give up now and make this easy on yourself

We will have our attorney contact your university and local law enforcement in the morning.

Sun Oct 17, 2:46 AM

Xdxdxd

You know that website out of date right?

Dont think I even have masters uploaded

Best of luck

Type message here

Send

CC 11:58 AM 217

< Inbox [redacted]

local law enforcement in the morning.

Sun Oct 17, 2:46 AM

Xdxdxd

You know that website out of date right?

Dont think I even have masters uploaded

Best of luck

Sun Oct 17, 12:14 PM

It has your birthday not your age stated.

Type message here

Send

THIS IS **EXHIBIT "27"** TO
THE AFFIDAVIT OF **LAURENCE DAY**
SWORN BEFORE ME
THIS 9th DAY OF DECEMBER, 2021

Stephen Aylward

A COMMISSIONER ETC.

gitter.im/kovan-testnet/faucet

ZetaZeroes 1/3

219

GITTER

Kovan Testnet/faucet Try Icarus for automated response: https://github.com/kovan-testnet/faucet or request Kovan ETH - only p

Where communities thrive

JOIN OVER **1.5M+ PEOPLE**
JOIN OVER **100K+ COMMUNITIES**
FREE **WITHOUT LIMITS**
CREATE **YOUR OWN COMMUNITY**

EXPLORE MORE COMMUNITIES

ZetaZeroes @ZetaZeroes_twitter Oct 14 05:24
0xBA5Ed1488bE60BA2FACC6B66C6D6F0beFba22eBe

ethdrop @ethdrop Oct 14 05:24
@ZetaZeroes_twitter sent!

Crypto_fr_investor 🚀 @MickaDa3_twitter Oct 14 05:27
0xBD126fec744b60677E791D5bD7413931952367E1

ethdrop @ethdrop Oct 14 05:27
@MickaDa3_twitter wait 14h or use https://ethdrop.dev

Rio @Rio30593645_twitter Oct 14 05:33
0x00a5F2D2fa41B53ee470fC86A05c4dB4d22D550e

ethdrop @ethdrop Oct 14 05:34
@Rio30593645_twitter sent!

ikbe @guava2010_twitter Oct 14 05:39
0x0F71cA78EFa7bc202EcB5d2BB10125F41c7a1911

ethdrop @ethdrop Oct 14 05:39
@guava2010_twitter sent!

ikbe @guava2010_twitter Oct 14 05:39
0x0F71cA78EFa7bc202EcB5d2BB10125F41c7a1911

ethdrop @ethdrop Oct 14 05:39
@guava2010_twitter wait 24h or use https://ethdrop.dev

VNArt @DNT70248253_twitter Oct 14 05:40
0x35117F38DF153b16f81c02c47F39d6311BC5a5c2

ethdrop @ethdrop Oct 14 05:40
@DNT70248253_twitter sent!

Vinh Pham Quy @vinhpham00_twitter Oct 14 05:41
0xf2d5E7EF8c45ca8dB0C1E812340B9c142fB4d537

ethdrop @ethdrop Oct 14 05:41
@vinhpham00_twitter sent!

libert @LibertBrown_twitter Oct 14 05:43
0x7Af040b18fB3a0F646E02D6b44c4bBf8c7ad9Bb5

SIGN IN TO START TALKING

CHAT VIA MATRIX

PEOPLE REPO INFO

SEE ALL (34567 PEOPLE)

ACTIVITY

mingderwang commented #476 03:32
mingderwang commented #476 03:31
naetkss commented #128 Nov 14
naetkss commented #476 Nov 14
naetkss opened #476 Nov 14
BTT21000 opened #475 Nov 14
shubham-kanodia opened #474 Nov 14
TarasKataryna opened #473 Nov 13
myGSmile edited #472 Nov 13
myGSmile opened #472 Nov 13
Airmag2099 opened #471 Nov 13
anche5ire edited #470 Nov 12
anche5ire opened #470 Nov 12
moonlaunch opened #469 Nov 12
Stev941 opened #468 Nov 12

THIS IS **EXHIBIT "28"** TO
THE AFFIDAVIT OF **LAURENCE DAY**
SWORN BEFORE ME
THIS 9th DAY OF DECEMBER, 2021

Stephen Ayford

A COMMISSIONER ETC.

ZetaZeroes

Dr Laurence E. Day @dizzeehaskell_twitter 07:58

Hey UmbralUpsilon, Laurence here.

I don't think 'well played' is the right thing to say here, but honestly it's been 11 hours now I've been at my machine with no sleep, so, well played.

Look, I'll cut to the chase - it would mean the world to everyone involved on the other side of this if we negotiated a 10% whitehat bounty on the funds pulled out from DEFI5 and CC10. I can only appeal to your good nature here, obviously, and the call is ultimately your own, but these weren't funds that were being blindly thrown around by apes: they were being used to diversify risk in the space - exactly the types of people that shouldn't be punished.

If we can come to an arrangement like that, we leave it there as precedent dictates. You know the pain that'll inevitably be associated with trying to cash out otherwise.

Can we talk?

/Laurence

THIS IS **EXHIBIT "29"** TO
THE AFFIDAVIT OF **LAURENCE DAY**
SWORN BEFORE ME
THIS 9th DAY OF DECEMBER, 2021

Stephen Ayford

A COMMISSIONER ETC.

Dr Laurence Ξ. Day
@laurence_e_day

Update on the Indexed attack: what we know about the exploiter, and the status of the unaffected pools.

This is written in a personal capacity, despite the 'we'. It's an info dump written after 36 hours of no sleep.

hackmd.io/fSTndeFZQPOPKY...

11:36 AM · Oct 15, 2021 · Twitter Web App

12 Retweets 5 Quote Tweets 97 Likes

THIS IS **EXHIBIT "30"** TO
THE AFFIDAVIT OF **LAURENCE DAY**
SWORN BEFORE ME
THIS 9th DAY OF DECEMBER, 2021

Stephen Gifford

A COMMISSIONER ETC.

Update #2: Indexed Finance Attack

In the intervening hours since the previous update, we have had a significant development as to the identity of the exploiter, as well as connections back to interactions with Code 423n4, Binance and Coinbase.

This post will lay out the connections and ultimate reasoning behind the following Tweet:

https://twitter.com/ndxfi/status/1449203629085368322 (https://twitter.com/ndxfi/status/1449203629085368322)

BogHolder/tensors/UmbralUpsilon/ZetaZeroes, we know you're reading this, and all the Discord hopping in the world isn't going to help you now.

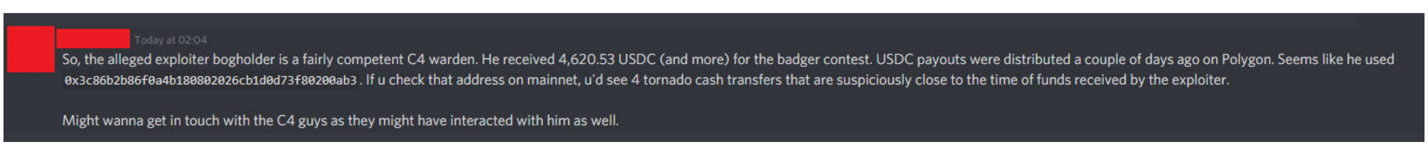
Give it back. The whitehat bounty is still on offer, but that window is *rapidly* closing for you.

BogHolder/Tensors & Code 423n4

In the previous update (https://hackmd.io/fSTndeFZQPOPKYxlafaNIA), we laid out the fact that we (Dillon and Laurence) were contacted by - and in contact with - BogHolder#1688 on Discord (under a different profile picture and username UmbralUpsilon at the time) in order to discuss certain aspects of the reweighting and reindexing mechanism of Indexed pools: the aspect that was utilised in order to execute the exploit.

Following the exploit, we have found that these conversations had been deleted on their side, and we had no mutual servers with them. Given that they were unresponsive, this didn't bode well, but we at least had something to reach out to Discord about with a subpoena if we got some more proof and it came to that.

About two hours ago we received a tip from someone in Discord stating that this account is a contributor to Code423n4, the community auditing platform: one that we have been intending to utilise for reviews of our protocol upgrade and Nirn. Specifically, the tip was (name redacted for privacy):


[redacted] Today at 02:04
So, the alleged exploiter bogholder is a fairly competent C4 warden. He received 4,620.53 USDC (and more) for the badger contest. USDC payouts were distributed a couple of days ago on Polygon. Seems like he used `0x3c86b2b86f0a4b180802026cb1d0d73f80200ab3`. If u check that address on mainnet, u'd see 4 tornado cash transfers that are suspiciously close to the time of funds received by the exploiter.

Might wanna get in touch with the C4 guys as they might have interacted with him as well.

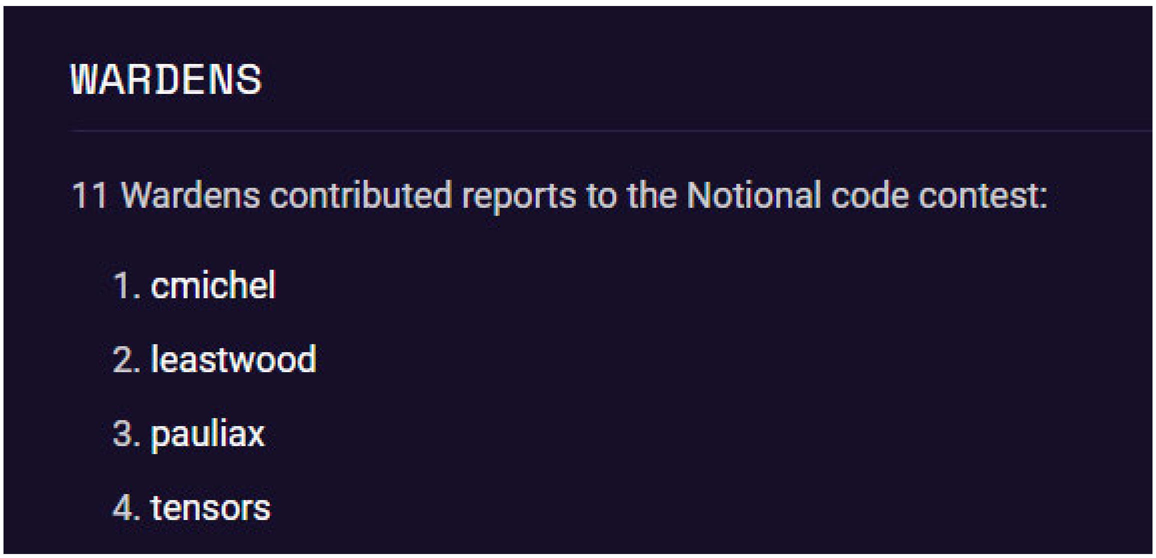
We dug around a bit, and found that this was true: this account (https://etherscan.io/address/0x3c86b2b86f0a4b180802026cb1d0d73f80200ab3) deposited into Tornado mere hours before the exploit - one more deposit than was pulled out by the exploiter in order to execute the attack.

Get in contact with C4? Alright.

We started a conversation with sockdrawermoney, one of the C4 organisers, and let them know our suspicions: that BogHolder#1688 was in fact the Indexed attacker, only to be met with the fact that they knew, and had been speaking to them, appealing to claim the whitehat bounty on offer.

Here's where things get a bit convoluted, but we'll explain as we go.

Back in August, C4 ran a competition for Notional (http //code423n4 com/report /2021 08 notional), and handed out a couple of rewards for jobs well done. The #4 position in that competition was a user named 'tensors'.

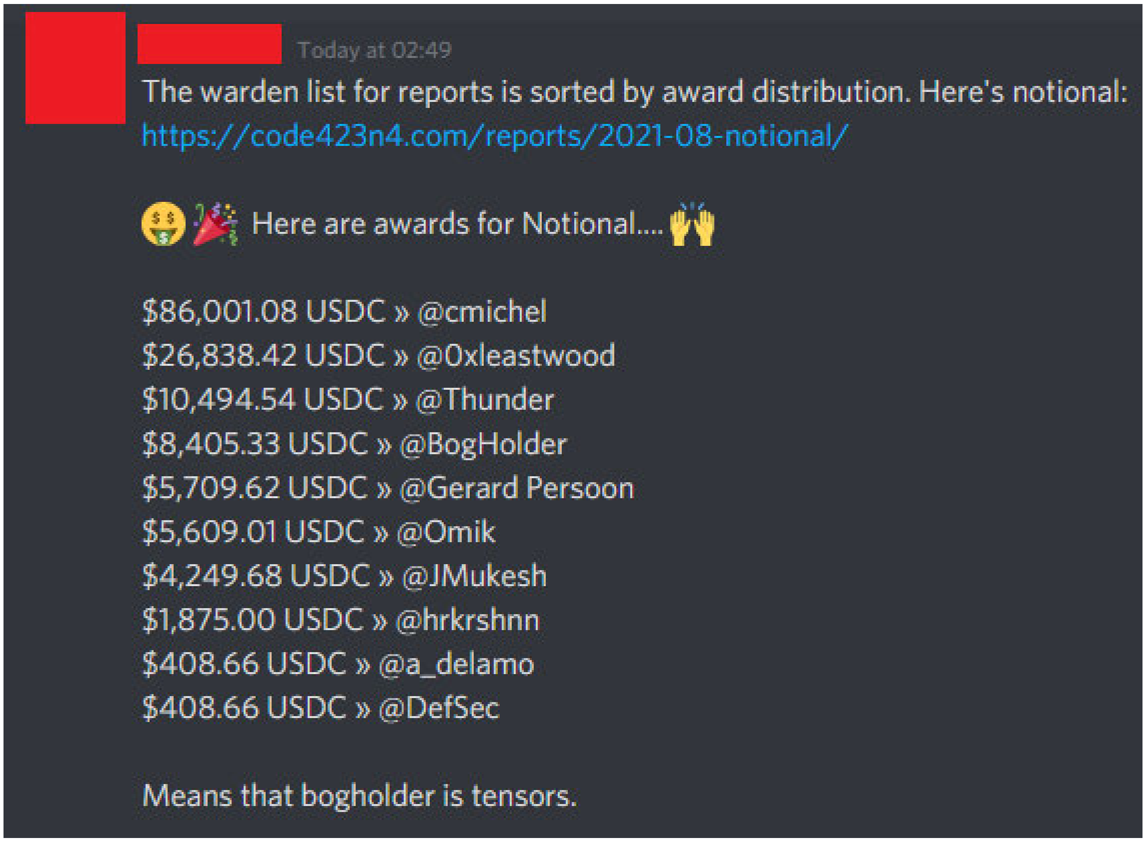


WARDENS

11 Wardens contributed reports to the Notional code contest:

1. cmichel
2. leastwood
3. pauliax
4. tensors

Within the C4 Discord, where users are tagged in announcements of results, this is reflected as tensors now being known as BogHolder.



At 11:38 Central, a new user named `tensors8` joined the C4 Discord.

A conversation then took place between sockdrawermoney and tensors8, of which which tensors8 (BogHolder) subsequently deleted his side of the conversation, in exactly the same way as UmbralUpsilon deleted conversations with us.

Due to concerns for the safety and well-being of the Code Arena team, we have taken the relevant screenshots down from this page.

Anyone pursuing legal action may contact dillon@indexed.finance or laurence@indexed.finance to retrieve a cached version of the evidence.

We are satisfied that these two parties (tensors8 and BogHolder) are one and the same, and that the wallet that C4 paid in exchange for the Notional work - and used Tornado right before the assault on Indexed - belongs to them.

Let's go on the chain.

Finding Links To Fiat

It turns out that obfuscating your transactions doesn't really help you when your adversaries are motivated by the theft of sixteen million dollars.

Here comes a flurry.

The attacker received funds twice from 0x4648451b5f87ff8f0f7d622bd40574bb97e25980 (https://etherscan.io/address/0x4648451b5f87ff8f0f7d622bd40574bb97e25980), which was funded through Binance (https://etherscan.io/tx/0xd05832b2e1ddedc3a7ba11396b83f024d0538e8a6affa62d6c7b913626f008eb) as the initial source of Ether for gas three years ago.

They also received funds from 0x98B42202F6757ae42AF0443D4C0F271aA006Ac03 (https://etherscan.io/address/0x98b42202f6757ae42af0443d4c0f271aa006ac03), which has two transactions within:

1. Receiving funds from 0x5e81440f1ade80fc97c11e480782e1fd11bba7e4 (https://etherscan.io/address/0x5e81440f1ade80fc97c11e480782e1fd11bba7e4),
2. Immediately sending these funds to the C4 wallet 0x3c86 (https://etherscan.io/tx/0x409808711ea1559832da5be9792da9cfe79a5f8c242cfb09b3a4c1aa77935b10).

It is this 0x5e8 account that is particularly damning. This account only ever made six transactions, three of which are relevant to us:

1. Receiving funds from Binance (https://etherscan.io/tx/0xa81182d75d07ec75d097a0cb1c42ec41aa2467c0e2cfc7b8ffbdf63171e1be8c),
2. Sending funds to Coinbase (https://etherscan.io/tx/0x09d0f1df04b8669e3a484e9bfd3d20980adaf6578823602a43ed3bf32334738a), and
3. Sending funds to the 0x98B4 wallet (https://etherscan.io/tx/0xeb411394eee8acc7427f2f31b753bc94855d3836663463b08064ad1f5f7a84b2)

We have a lot more information than this available to us, but it's more convoluted than what we can easily present here.

Summary

To wrap up everything here:

- We have established that the Indexed attacker is the C4 Warden 'tensors',
- We have established connections between the wallet that they have received C4 payments to and two exchanges which require KYC (although in Binance's case, you could get away with not KYCing for non-trivial amounts until fairly recently),
- We have already reached out to these exchanges informing them of this, and
- We are now presenting an ultimatum.

tensors, you have until 17:00 UTC on the 17th of October 2021 to return 90% of the stolen funds to the Indexed Finance Treasury address 0x78a3ef33cf033381feb43ba4212f2af5a5a0a2ea (https://etherscan.io/address/0x78a3ef33cf033381feb43ba4212f2af5a5a0a2ea).

If you fail to do this, we will be sending all of the information that we have to law enforcement agencies for them to do with as they see fit. We will not stop digging either: you've slipped up elsewhere.

You can now choose what difficulty you want to play this game on. Easy mode or Dark Souls.

It's your call.

Update for historical record: following identification of the attacker, the 10% whitehat bounty (which was first put in writing to the attacker at 06:58 GMT on the 15th of October via Gitter and referenced in Update #1 (https://hackmd.io/fSTndeFZQPOPKYxlafaNIA)) was removed at 13:54 GMT on the 16th of October in this tweet (https://twitter.com/ndxfi/status/1449373158583279622).

A party associated with Indexed Finance then reached out privately to the attacker - unbeknownst to other parties involved - and offered a US$50,000 bounty for the return of funds, which the attacker 'accepted' in such a way as to effectively confess (see Update #3 (https://hackmd.io/@d1ll0n/Hyd-uCuBK#Update-on-BogHolder-Connection)).

THIS IS **EXHIBIT "31"** TO
THE AFFIDAVIT OF **LAURENCE DAY**
SWORN BEFORE ME
THIS 9th DAY OF DECEMBER, 2021

Stephen Ayford

A COMMISSIONER ETC.

← Tweet

Indexed Finance
@ndxfi

The 10% offer has expired. The attacker has until EOD to return 100% of the stolen funds or his information will be published and law enforcement notified.

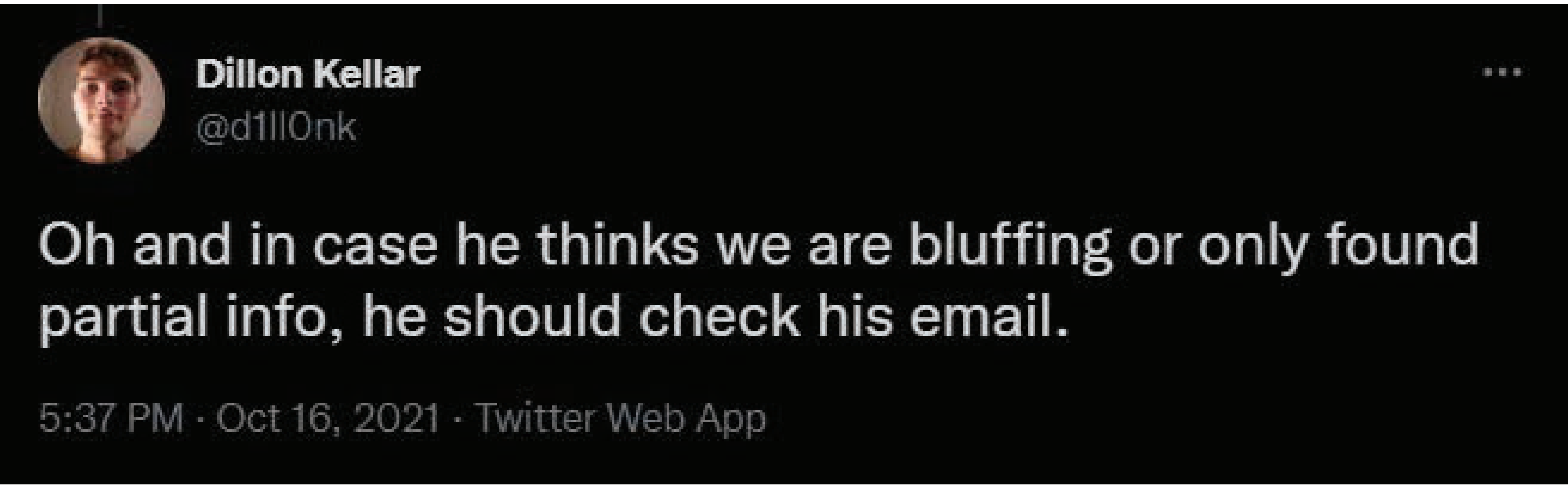
etherscan.io
Ethereum Transaction Hash (Txhash) Details | Eth...
Ethereum (ETH) detailed transaction info for txhash 0x858e559bb712eb919365d2845e618b882604...

9:54 AM · Oct 16, 2021 · Twitter Web App

THIS IS **EXHIBIT "32"** TO
THE AFFIDAVIT OF **LAURENCE DAY**
SWORN BEFORE ME
THIS 9th DAY OF DECEMBER, 2021

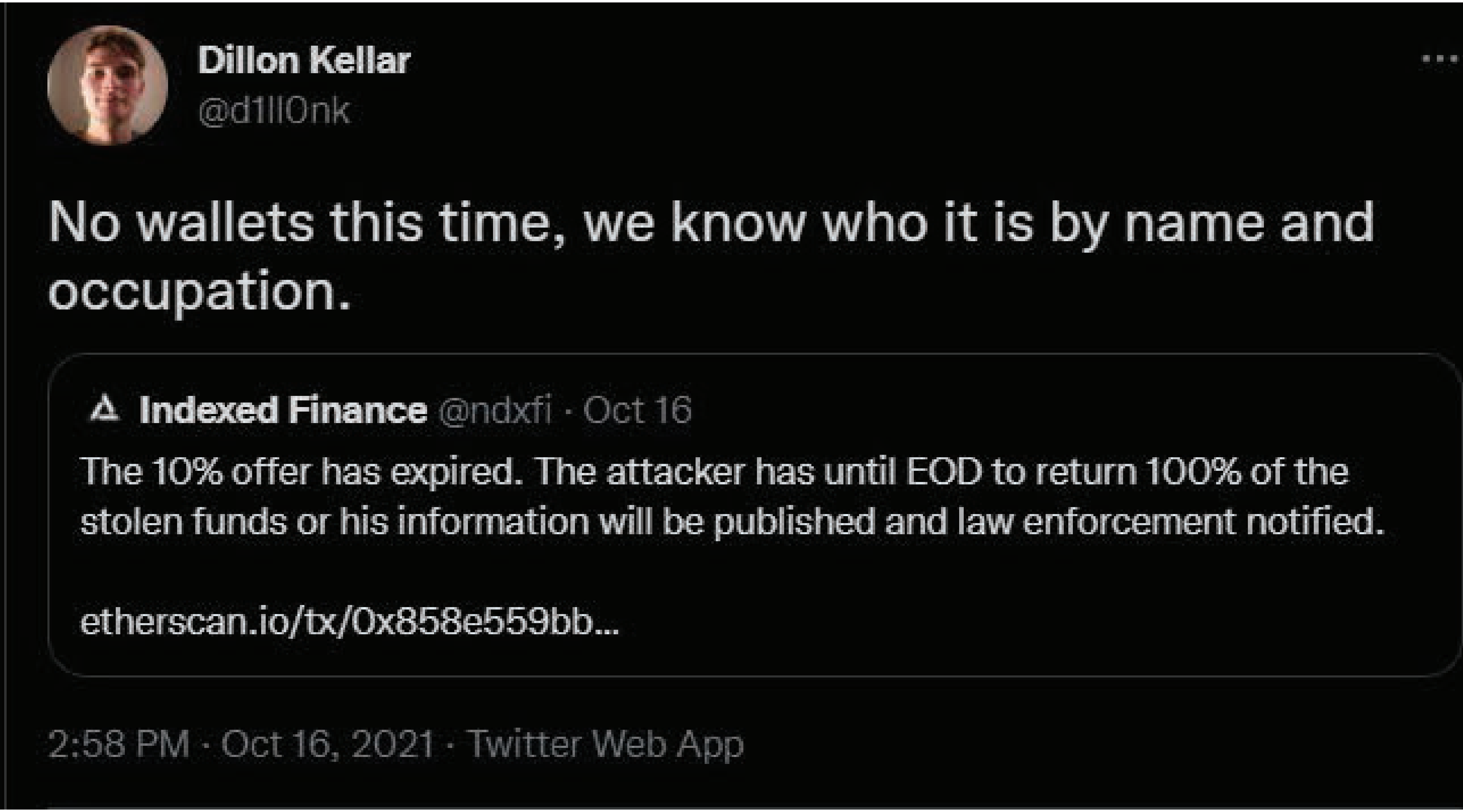
Stephen Cufford

A COMMISSIONER ETC.


Dillon Kellar
@d1ll0nk

Oh and in case he thinks we are bluffing or only found partial info, he should check his email.

5:37 PM · Oct 16, 2021 · Twitter Web App



Dillon Kellar
@d1ll0nk

No wallets this time, we know who it is by name and occupation.

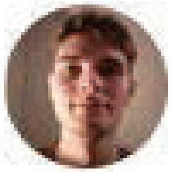
> **Indexed Finance** @ndxfi · Oct 16
> The 10% offer has expired. The attacker has until EOD to return 100% of the stolen funds or his information will be published and law enforcement notified.
>
> etherscan.io/tx/0x858e559bb...

2:58 PM · Oct 16, 2021 · Twitter Web App

THIS IS **EXHIBIT "33"** TO
THE AFFIDAVIT OF **LAURENCE DAY**
SWORN BEFORE ME
THIS 9th DAY OF DECEMBER, 2021

Stephen Ayford

A COMMISSIONER ETC.

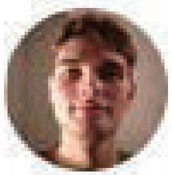


Dillon Kellar @d1ll0nk · Oct 21

If you feel our efforts to address the situation have been inadequate, there are legal remedies you can pursue; threatening him or his family isn't one of them.

3 1 14

Show this thread



Dillon Kellar @d1ll0nk · Oct 21

We've been informed that Andy and his family have been receiving threats (not legal, actual threats). If you've been making these - stop. This is almost certainly illegal and will not help you recover funds.

12 10 44

Show this thread

THIS IS **EXHIBIT "34"** TO
THE AFFIDAVIT OF **LAURENCE DAY**
SWORN BEFORE ME
THIS 9th DAY OF DECEMBER, 2021

Stephen Ayford

A COMMISSIONER ETC.

Andean E. Medjedovic

Biographical Information

I'm currently a Masters student at the University of Waterloo. My advisor is Michael Rubinstein.

Born: Hamilton, ON, Canada on Nov. 28, 2002
Living at: Waterloo, ON, Canada since 2017
Mail to: Department of Mathematics, University of Waterloo, 200 University Avenue West, Waterloo, ON, Canada.

Research Interests

Number Theory

Education

University of Waterloo — Sep. 2020 – Present
Masters in Pure Mathematics — *Waterloo, ON*

University of Waterloo — Sep. 2017 – Aug. 2020
Bachelor of Science - Pure Mathematics — *Waterloo, ON*

Professional Research Experience

Focused Research Group: Averages of L-functions — Jan. 2020 – Present
Advisor: Michael Rubinstein — *American Institute of Mathematics*

Waterloo Combinatorics and Optimization URA — Apr. 2019 – Sep. 2019
Advisor: Joseph Cheriyan — *University of Waterloo, C&O Dep.*

Institute for Quantum Computing URA — Apr. 2018 – Sep. 2018
Advisor: William Slofstra — *IQC*

Publications & Preprints

6. Exact Formulas for Secular Coefficients. (2021), 34 pages. Master's degree.
5. Real Mahler Series. (2020), 22 pages.
4. Enumerating Schubert Varieties over Type E Dynkin Diagrams. (2020), 21 pages. With William Slofstra.
3. Grothendieck's Classification of Line Bundles over the Riemann Sphere. Submitted to the Rose-Hulman Undergraduate Journal. (2020), 19 pages.
2. A Look at Chowla's Problem. Submitted to Involve Journal of Mathematics. (2020), 14 pages.
1. Sharp Incidence Bounds for Edge Partitions of K_n. Submitted to Graphs and Combinatorics. (2020), 9 pages.

Awards & Scholarships

- Putnam Score: 39 (2017)
- NSERC USRA Scholarship (2018, 2019, 2020)
- Bernoulli Trials Contest Special Prize - A small department math competition. (2020)

Some Talks & Expositions

6. Moments of Matrix Groups (Oct. 1 - Dec. 10, 2020) - Series of short talks presenting current research to L-functions research group.

5. The Mahler Conjecture (Dec. 1, 2020) - Seminar to graduate students at UW.

4. Representation Theory of GL_n (Nov. 7, 2020) - Seminar to undergraduates at UW.

3. Linear forms in Logs: Chowla's Problem (Dec. 7, 2019) – Seminar with Waterloo NT graduate Students.

2. Sparse Cuts and Eigenvectors (Aug. 24, 2019) – Seminar with Waterloo C&O Dep.

1. Lie Theory & Algebraic Geometry: Fibre Bundles over $P^1(\mathbb{C})$ (Apr. 11, 2019) - Seminar with Waterloo Differential Geometry group.

Teaching Experience & Duties

Grading, Teaching, & Tutoring: Done as a graduate student for 8 months. All areas of mathematics.
zbMATH : Reviewer (since summer of 2020).
FRG: L-functions : Co-organizer for social events.

Languages & Technical Skills

Computer: Mathematica, LaTeX, HTML/CSS and Solidity (some JS). Longtime Archlinux user.

Hobbies & Interests

Cryptocurrency & Trading. Free & Open Source Software. Reading, Meditation, (Blindfolded) Chess.

DILLON KELLAR et al. and ANDEAN MEDJEDOVIC Court File No.CV-21-00673984-00CP

Plaintiffs Defendant

ONTARIO

SUPERIOR COURT OF JUSTICE

Proceeding commenced at TORONTO

MOTION RECORD OF THE MOVING PLAINTIFFS, VOLUME 1

STOCKWOODS LLP
Barristers
Toronto-Dominion Centre
TD North Tower, Box 140
77 King Street West, Suite 4130
Toronto ON M5K 1H1

Gerald Chan (54548T)
Tel: 416-593-1617 / GeraldC@stockwoods.ca

Fredrick Schumann (59377L)
Tel: 416-593-2490 / FredrickS@stockwoods.ca

Stephen Aylward (66556E)
Tel: 416-593-2496 / stephena@stockwoods.ca

Alexandra Heine (83514R)
Tel: 416-593-1669 / AlexandraH@stockwoods.ca

Tel: 416-593-2496
Fax: 416-593-9345

Lawyers for the Plaintiffs

Court File No. CV-21-00673984-00CP

ONTARIO
SUPERIOR COURT OF JUSTICE

B E T W E E N:

DILLON KELLAR and LAURENCE DAY

Plaintiffs

and

ANDEAN MEDJEDOVIC

Defendant

Proceeding under the *Class Proceedings Act, 1992*, SO 1992, c 6

MOTION RECORD OF THE MOVING PLAINTIFFS

(Urgent *Mareva* and Receivership Orders)

VOLUME 2

December 17, 2021

STOCKWOODS LLP
Barristers
Toronto-Dominion Centre
TD North Tower, Box 140
77 King Street West, Suite 4130
Toronto ON M5K 1H1

Gerald Chan (54548T)
Tel: 416-593-1617
GeraldC@stockwoods.ca

Fredrick Schumann (59377L)
Tel: 416-593-2490
FredrickS@stockwoods.ca

Stephen Aylward (66556E)
Tel: 416-593-2496
stephena@stockwoods.ca

Alexandra Heine (83514R)
Tel: 416-593-1669
AlexandraH@stockwoods.ca

Tel: 416-593-7200
Fax: 416-593-9345

Lawyers for the Plaintiffs/Moving Parties

TO: [redacted]

TO: **RAYMOND CHABOT ADMINISTRATEUR PROVISOIRE INC.**
Tour de la Banque Nationale 600,
rue De La Gauchetière Ouest Bureau 2000
Montréal, QC H3B 4L8

Emmanuel Phaneuf, M.Sc., CIRP, LIT
Tel: 514-393-4826
phaneuf.emmanuel@rcgt.com

Proposed Receiver

I N D E X

THIS IS **EXHIBIT "35"** TO
THE AFFIDAVIT OF **LAURENCE DAY**
SWORN BEFORE ME
THIS 9th DAY OF DECEMBER, 2021

Stephen Anford

A COMMISSIONER ETC.

Update #3: Indexed Finance Attack

If you are reading this, it means that the ultimatum (https://twitter.com/ndxfi/status/1449373158583279622) that we presented to the Indexed Finance attacker was not met, and that alternate attempts at negotiating with the attacker have failed.

It did not have to be this way.

Introduction & Action

We have spent a great deal of time and effort conducting research into the identity of the attacker. In this post we'll lay out how we conducted this research and the conclusions drawn.

We have instructed an attorney retained by members of the Indexed core contributor team to bring this to the attention of relevant law enforcement agencies in the US and Canada.

In a previous update (https://hackmd.io/fSTndeFZQPOPKYxlafaNIA), we established a link between the attacker address and the wallet which funded it, thanks to members of the Code 423n4 team who shared their knowledge of the attacker with us.

This update will detail several profiles we have found which we believe belong to the attacker, and which link back to a real world identity.

A Disclaimer

We are convinced beyond reasonable doubt that our research is solid, and previously showed it to various respected parties in the space, who echoed their agreement (including banteg (https://twitter.com/bantg/status/1449370241637703695), Julien Bouteloup (https://twitter.com/bneiluj/status/1449394599764574214), and Lefteris Karapetsas (https://twitter.com/LefterisJP/status/1449408651458977796)) before the initial ultimatum deadline expired.

With that said, let us begin.

GitHub

The GitHub profile mtheorylord1 (https://github.com/mtheorylord1) registered as a Code 423n4 (C4) Warden under the account `tensors` via this commit (https://github.com/mtheorylord1/code423n4.com/commit/4a855b11aea74bd2ac4c3f33427262e4adaf3b89). This is information that was passed to us by a C4 member yesterday, and is important because we have already established that the Indexed attacker and `tensors` are one and the same (https://hackmd.io/@laurenceday/H1OylawSF#Summary).

This account had no previous or future activity on GitHub. However, searching the username yielded another account mtheorylord (https://github.com/mtheorylord) which had created a repository in 2016 called Grade_12_Project (https://github.com/mtheorylord/Grade-12-Project). This establishes that the account is likely owned by someone outside of the US (Grade 12 instead of 12th Grade) and that they were finishing high school in 2016.

Looking at the single commit made by this account (https://github.com/mtheorylord/Grade-12-Project/commit/1f591355a934dbca8288fae2aac5e6ce9bc7c6f9) will not immediately reveal much. In the Git CLI, however, we find the email address that was used to submit it.

```
$ git clone https://github.com/mtheorylord/Grade-12-Project
Cloning into 'Grade-12-Project'...
remote: Enumerating objects: 3, done.
remote: Total 3 (delta 0), reused 0 (delta 0), pack-reused 3
Unpacking objects: 100% (3/3), done.
$ cd Grade-12-Project/
$ git log
commit 1f591355a934dbca8288fae2aac5e6ce9bc7c6f9 (HEAD -> master, origin/master, origin/HEAD)
Author: mtheorylord <[redacted]>
Date:   Fri Dec 23 09:05:07 2016 -0500

    Initial commit
```

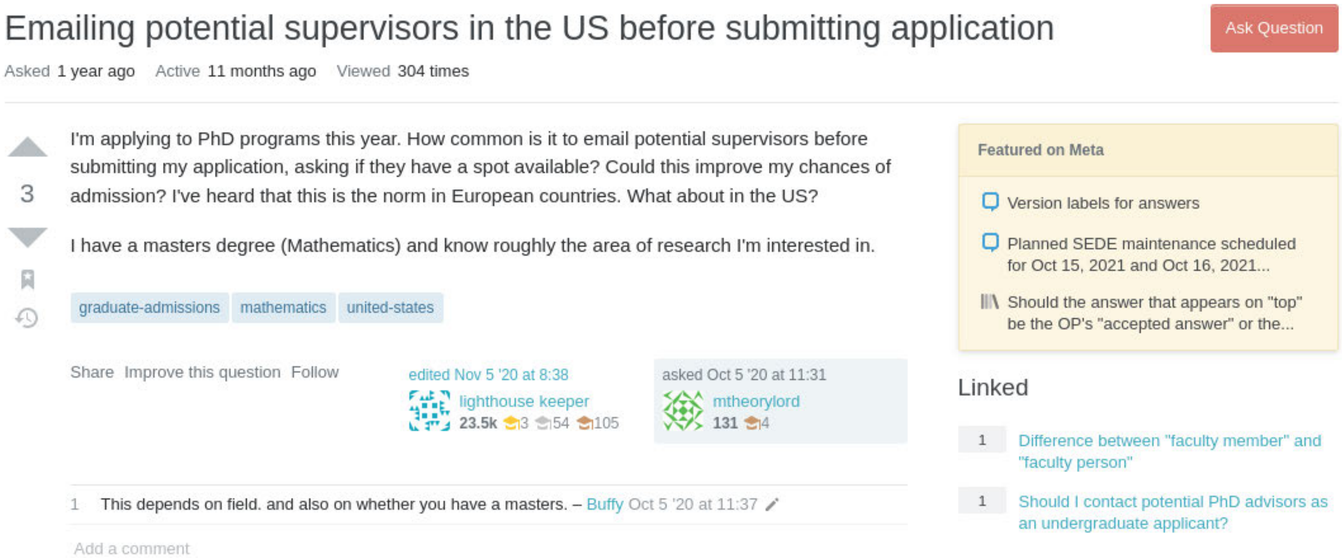
The email in question is [redacted] which includes a domain owned by a high school in Hamilton, Ontario, Canada.

StackExchange

Searching the username again, we found an account by the username mtheorylord (https://stackexchange.com/users/8787868/mtheorylord) on StackExchange which has been active since 2016.

This account has almost exclusively posted about mathematics since 2016; however, there are some noteworthy posts in other topics:

One year ago in the Academia stack (https://academia.stackexchange.com/questions/156221/emailing-potential-supervisors-in-the-us-before-submitting-application), `mtheorylord` stated that he had a master's degree in mathematics, and was seeking out advice on applying to PhD programs. In it, he asked how he should go about reaching out to supervisors, and whether it was different in the US than it was in European countries.


Emailing potential supervisors in the US before submitting application

Ask Question

Asked 1 year ago Active 11 months ago Viewed 304 times

3

I'm applying to PhD programs this year. How common is it to email potential supervisors before submitting my application, asking if they have a spot available? Could this improve my chances of admission? I've heard that this is the norm in European countries. What about in the US?

I have a masters degree (Mathematics) and know roughly the area of research I'm interested in.

graduate-admissions mathematics united-states

Share Improve this question Follow

edited Nov 5 '20 at 8:38
lighthouse keeper
23.5k 3 54 105

asked Oct 5 '20 at 11:31
mtheorylord
131 4

1 This depends on field. and also on whether you have a masters. – Buffy Oct 5 '20 at 11:37

Add a comment

Featured on Meta

Version labels for answers

Planned SEDE maintenance scheduled for Oct 15, 2021 and Oct 16, 2021...

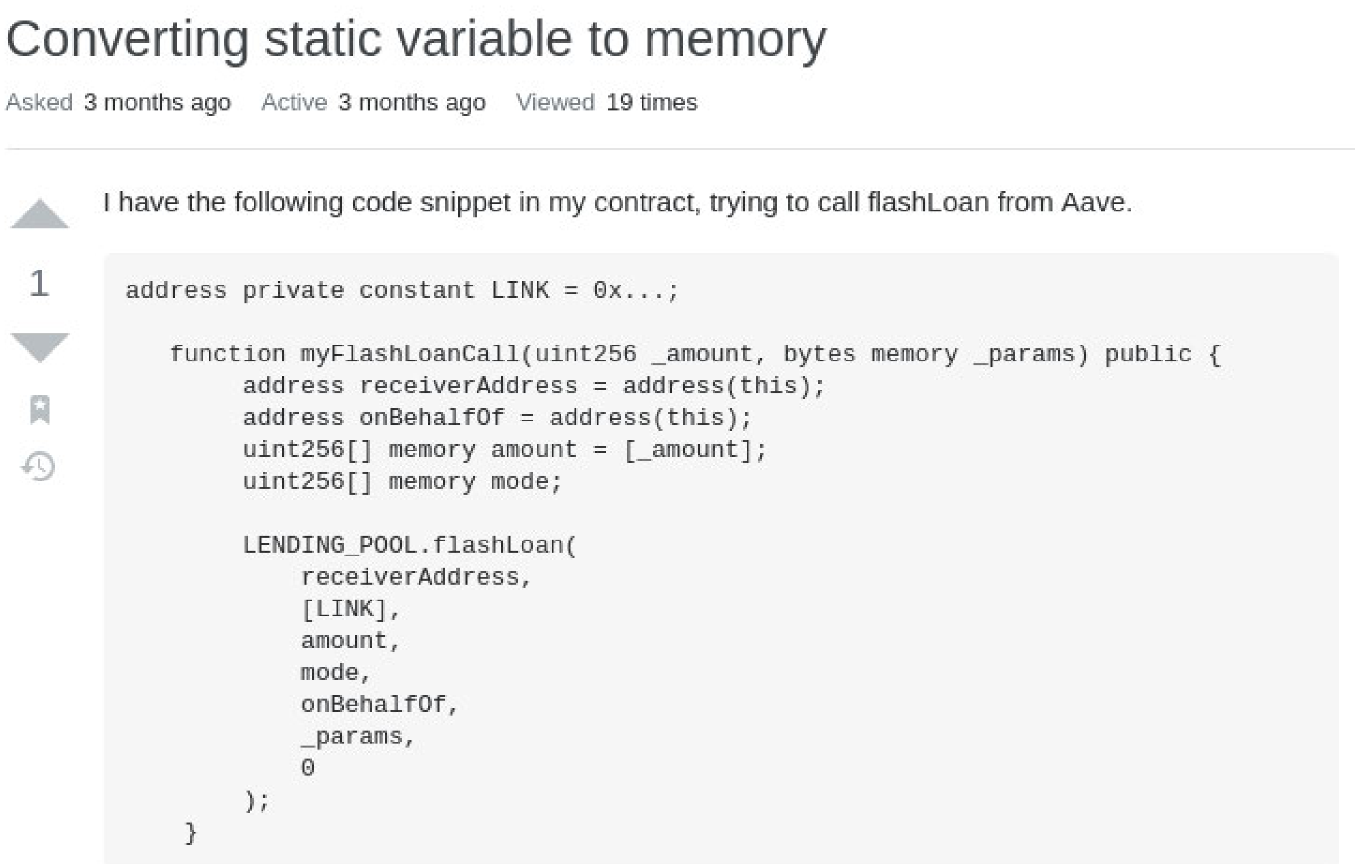
Should the answer that appears on "top" be the OP's "accepted answer" or the...

Linked

1 Difference between "faculty member" and "faculty person"

1 Should I contact potential PhD advisors as an undergraduate applicant?

[3 months ago in the Ethereum stack (https://ethereum.stackexchange.com/questions/103661/converting-static-variable-to-memory)](https://ethereum.stackexchange.com/questions/103661/converting-static-variable-to-memory), he asked a question about executing flash loans with Aave on Ethereum.


Converting static variable to memory

Asked 3 months ago Active 3 months ago Viewed 19 times

1

I have the following code snippet in my contract, trying to call flashLoan from Aave.

```
address private constant LINK = 0x...;

   function myFlashLoanCall(uint256 _amount, bytes memory _params) public {
        address receiverAddress = address(this);
        address onBehalfOf = address(this);
        uint256[] memory amount = [_amount];
        uint256[] memory mode;

        LENDING_POOL.flashLoan(
            receiverAddress,
            [LINK],
            amount,
            mode,
            onBehalfOf,
            _params,
            0
        );
    }
```

Wikipedia

Searching the username we found an [mtheorylord account on Wikipedia (https://en.wikipedia.org/wiki/Special:Contributions/Mtheorylord)](https://en.wikipedia.org/wiki/Special:Contributions/Mtheorylord), which was active between 2016 and 2017.

This account's first post was:

User talk:Mtheorylord

From Wikipedia, the free encyclopedia

This is an old revision of this page, as edited by Mtheorylord (talk | contribs) at 00:23, 17 June 2016 *(←Created page with 'Man I'm a good contributor. I am an expert in mathematics and theoretical physics. I believe in posting information about papers authors wrote on their wiki page...')*. The present address (URL) is a permanent link to this revision, which may differ significantly from the current revision.

(diff) ← Previous revision | Latest revision (diff) | Newer revision → (diff)

Man I'm a good contributor. I am an expert in mathematics and theoretical physics. I believe in posting information about papers authors wrote on their wiki page as well as where to find them. Thanks for your time.

After that, also in 2016, it made an edit (https://en.wikipedia.org/w/index.php?title=Reach_for_the_Top&diff=prev&oldid=729487079) to a wiki page about a game show for high school students called "Reach for the Top". It edited the "Alumni" section to add a name which matches the previously found email address, with the descriptor "Notable mathematician".

This edit was subsequently removed by a bot due to suspected vandalism. The account then made a second edit to the page to add the name of the high school which owns the domain in the email address found on Github to the "National Champions" section of the article. This edit was also deleted by another contributor, who stated the high school "did not win 2016 nationals". `mtheorylord` then commented on the editor's page, requesting it be changed back and linking back to an article on the high school's website.

Aside from these edits, the account posted on a page for cannabis culture and several mathematics articles until January 2017.

Personal Websites

See update at bottom of section

Googling the name that was found in the Wikipedia edit to the Alumni section of the Reach for the Top article, we found that the top result was a website nontrivial.xyz (https://nontrivial.xyz). This website was down for several days after the attack, but had last been cached by Google on October 14th, 2021 at 00:15:18 GMT about 16 hours before the attack on Indexed Finance.

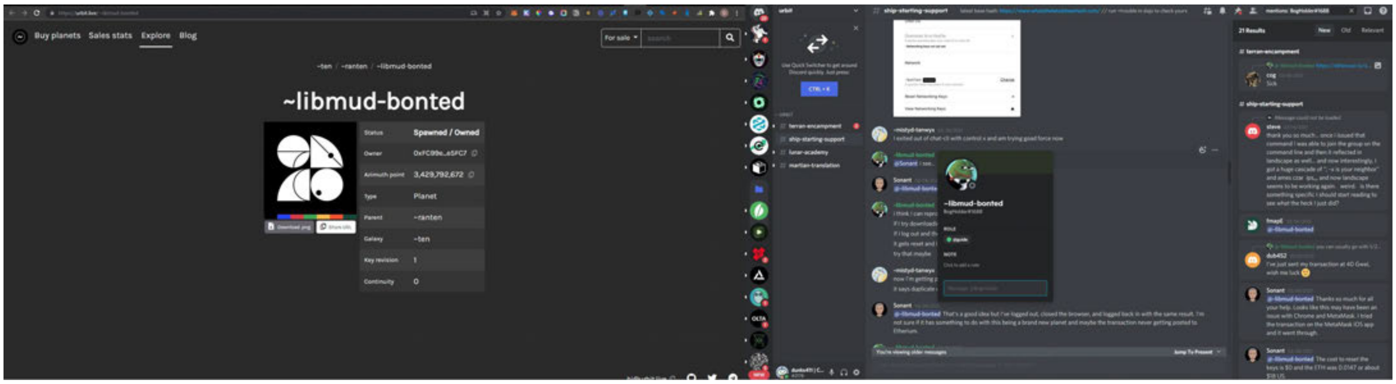
This is Google's cache of https://www.nontrivial.xyz/. It is a snapshot of the page as it appeared on Oct 14, 2021 00:15:18 GMT. The current page could have changed in the meantime. Learn more.

Full version Text-only version View source

The cached version stated that the owner is a master's student at the University of Waterloo studying pure mathematics, and that he has an interest in "cryptocurrency and other decentralized open source software".

Executing a reverse IP search on the domain (https://reverseip.domaintools.com/search/?q=nontrivial.xyz) revealed that the same server also hosted a website urbitstar.xyz (https://urbitstar.xyz), which is similarly down. A WHOIS lookup on this domain (https://whois.domaintools.com/urbitstar.xyz) indicates it was registered on February 1, 2021.

The attacker, who we have established went by the Discord handle BogHolder#1688, was a member of the Urbit Discord using the nickname `~libmud-bonted` corresponding to an Urbit planet and posted a link in the community on February 28, 2021 to this planet.



The address (https://etherscan.io/address/0xFC99e43b8D4aA2E87726c10f19785616907e5FC7#tokentxns) owning the associated Azimuth point can be traced back to an address (https://etherscan.io/address/0x7be53cac08462853476e26cc242f502293e52e97) that we have previously identified as being associated with the attacker, which we had previously sent a message (https://etherscan.io/tx/0xa30c8b1e6c3c45cff9b0673cc76de006115fa025c63444f21fd1ed7122a5c75e) requesting to talk.

Update

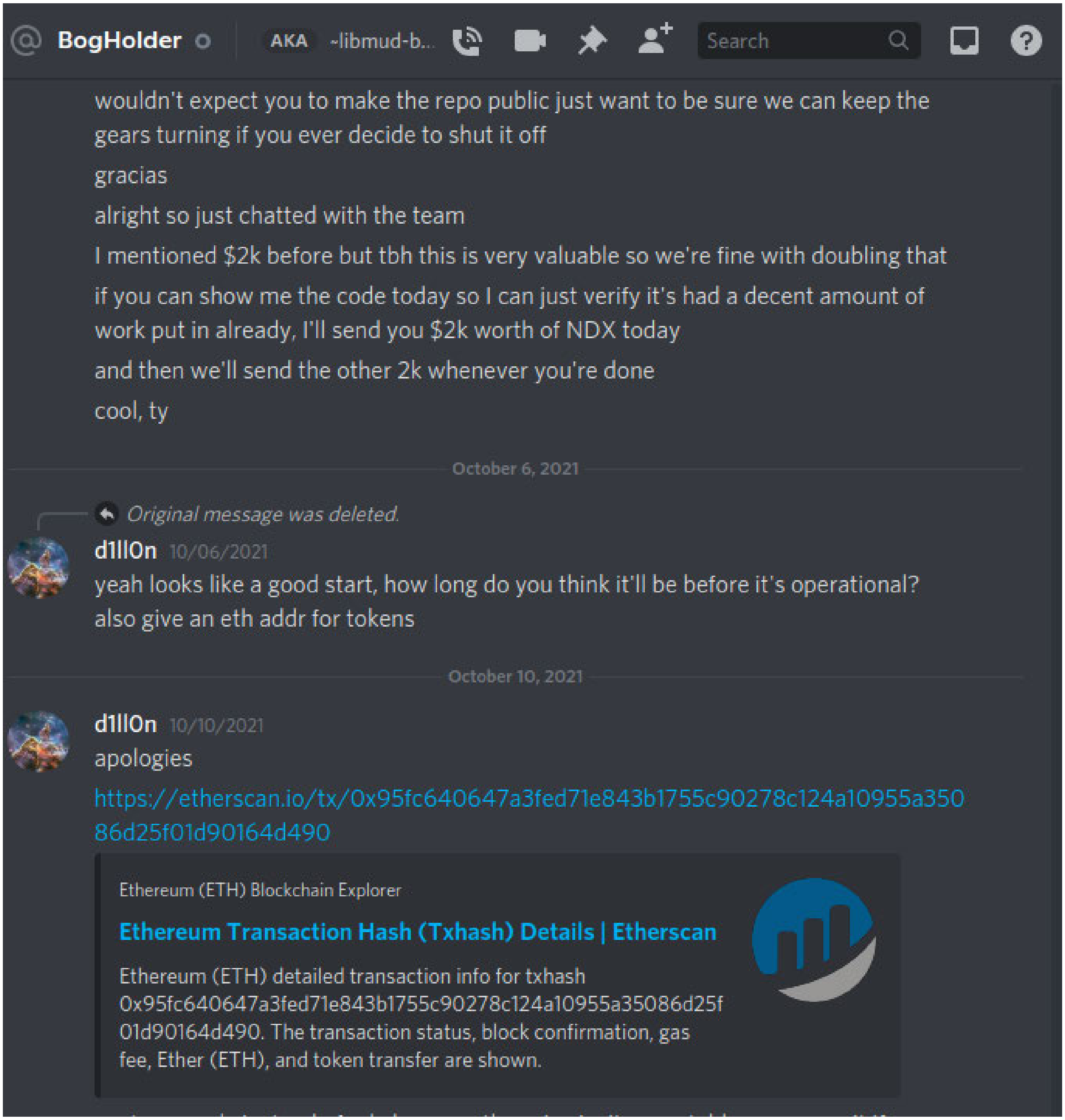
20 minutes before the ultimatum deadline, the personal website was put back online with the references to cryptocurrency stripped out. The website contained a resume which stated the owner of the website's birthday, which indicated he is currently 18 years old. We searched again for his name after this, thinking something was off, and found a news article from 2016 which mentions the name of the website owner in reference to an accelerated learning program, stating that he was a 13 year old in grade 12. The name of the school referenced matches the domain from the original email address found on GitHub.

Update on BogHolder Connection

As mentioned in the previous post, for several weeks prior to the attack, the Discord user BogHolder#1688 was in communication with the team about development of an arbitrage bot which would automate certain areas of the management of index pools (specifically, selling unbound tokens). As this was an area that no one else had developed bots for, we were excited someone was taking a deep interest in the protocol to develop such a bot, and even hoped we could work with him on other aspects of the project in the future.

We offered to send a bounty of $2k if he would agree to share the code with us in the event that he decided to stop running the bot himself, as it would help automate some parts of the index pool maintenance. He agreed, and we then decided to up it to $4k to further motivate him, and as a show of good faith and desire to work together. We told him we would send $2k up front if he provided a code sample to prove he was working on said bot and $2k when it was ready. He said he would send it later, and two days after that he did provide a code sample which sufficiently demonstrated to us that he had done work on the project.

We asked for an Ethereum address to send funds to, and he sent the address `0xb7e77cdaf7ebf76db72571f2d6e43aa5e84a5e64` . This address was only known by Laurence, Dillon and the attacker. We sent $2k in USDC to the provided address in this transaction (https://etherscan.io/tx/0x95fc640647a3fed71e843b1755c90278c124a10955a35086d25f01d90164d490). He subsequently deleted the chat logs after the attack.



After we had learned the identity of the attacker and proven to him we had identified him, his information and an earlier version of this document were shared internally with members of the team and trusted parties. Pr0, an angel investor of Indexed and founding team member, sent the attacker an email to his personal email address listed on his website, offering to give him $50k if he returned the funds stolen.

PRO PRO 08:38
to [redacted]

Hey am contacting you at a personal capacity to offer a way out. Am the lead investor for Indexed and a cofounder. Theres been alot of shit going on, you fucked up your opsec and now have serious problems. The money can never be spent by you no matter what you do now and am sure you just had fun, saw easy money and now it went too far. So heres my proposal, and you should talk to whoever you confide in about it.

1. $50k bounty to return the money. This money you can actually use.
2. Will do my best to get the team to not press any charges, remove what information we can that puts a target on you (again you have committed a crime here so may already be out of our hands somewhat, but return of funds will show remorse and good faith).
3. You get easy pr and can maybe do some talks on how you found the vulnerability and get some Crypto rep. You havent moved funds, you haven't actually done any moves at all, so the whitehat cards still a play.

Noone knows reached out, they'll probably be upset, but all you've been getting so fars stick, thought would try a more incentivized approach.

[redacted] 09:15
Sounds like a plan. Send the money over: 0xb7e77cdAf7EBF76dB72571f2D6E43aA5e84a5E64

The attacker responded to Pr0 from his personal email address using the same Ethereum address as he had sent to collect the bounty before the attack.

Conclusion

We have established that the Wikipedia, StackExchange and Github profiles for the username `mtheorylord` are owned by the same person, as is the `mtheorylord1` github account which submitted the attacker's Warden registration to the C4 github.

We have established that the owner of these accounts has a personal website expressing interest in crypto, that this website was taken down the day of the attack, that it was later put back up with references to cryptocurrency removed, that it was hosted on the same server as a website for a community that the attacker was a member of, and that the attacker was active in the community at the time the website was registered.

We had previously established that the attacker had a tendency for using mathematical jargon as usernames (ZetaZeroes, UmbralUpsilon, tensors), and the identified party is a master’s student in mathematics.

We had previously established that the attacker and BogHolder were one and the same, and we have now established that the identified party in this document possessed information which no one other than BogHolder, Laurence and Dillon knew of.

We hope this information will be useful, and as mentioned previously we have instructed our personal attorney to forward the information to law enforcement.

THIS IS **EXHIBIT "36"** TO
THE AFFIDAVIT OF **LAURENCE DAY**
SWORN BEFORE ME
THIS 9th DAY OF DECEMBER, 2021

Stephen Aylward

A COMMISSIONER ETC.


ZetaZeroes
@ZetaZeroes

And, ok, initially, it seemed to me that doxxing teenagers is an incredibly gauche move (no matter how many degrees they have in advanced analytic arbitrage actions), but after thinking about it I sense the zero-to-one kind of esoteric Thielist innovation that this play entails.

3:11 AM · Oct 17, 2021 · Twitter Web App

Home
Explore
Notifications
Messages
Bookmarks
Lists
Profile
More

Tweet

ZetaZeroes
43 Tweets

Follow

ZetaZeroes
@ZetaZeroes

Punished Mathematician. Slick Arbitrageur.
Aspiring PhD in Critical Race Theories.

Joined October 2021

10 Following **1,422** Followers

Not followed by anyone you're following

Tweets | Tweets & replies | Media | Likes

Pinned Tweet
ZetaZeroes @ZetaZeroes · Oct 21
Speaking seriously now:
I want to thank everyone that has been sending me letters of support. I have one favor to ask for followers and friends. I am looking for the most elite crypto lawyers. I will need an entire team.

46 30 87

Show this thread

ZetaZeroes @ZetaZeroes · Oct 21
Ok, you know, I believe that if the promise crypto is to succeed it must be a patrician endeavour.

3 16

ZetaZeroes @ZetaZeroes · Oct 21
If indexed wants to insinuate that I did something wrong and resort to namecalling, LOL.
However, if they want to try steal my hard earned video game tokens, then we must have a duel!
Please choose, Swords or Pistols? At noon or at dusk?

I will WIN, it will not be close.

6 4 30

ZetaZeroes @ZetaZeroes · Oct 21
I am being totally unironic here! But no in all honesty, I doubt they have it in them for an actual fight to the death. These people ... always the safe way out with them.

2 9

ZetaZeroes @ZetaZeroes · Oct 21
Either through twitter, my doxxed email or [redacted]

1 14

Show this thread

Who to follow

flashfish
@flashfish0x
⚡🐠
Follow

Will Sheehan
@wilburforce_
Founder @parsec_finance recovering quant, distracted by DeFi
Follow

Information Token

[redacted]

Search Twitter

You might like

Matti
@mattigags
Follow

Will Sheehan
@wilburforce_
Follow

alpharush
@0xalpharush
Follow

Show more

What's happening

NFL · Last night
Patriots at Bills
Trending with Buffalo

Bloomberg Quickta... · Yesterday
Jussie Smollett testifies 'there was no hoax' at trial

Toronto Star · Yesterday
This small Ontario town is caught in COVID's rural-urban divide

Trending in Canada
#MontrealMassacre
3,173 Tweets

Trending in Canada
#HalifaxExplosion
1,544 Tweets

Show more

Home
Explore
Notifications
Messages
Bookmarks
Lists
Profile
More

Tweet

Follow
@InfoTokenDAO
100 tokens, 100 members discord.gg/QaqHh3Mqdw

Show more

ZetaZeroes @ZetaZeroes Oct 21
People who can take on a case like this and are willing to push it to the highest levels if need be.

If you know such people of power, please put them in contact with me. If you know someone who might know someone, please spread the message. Many thanks.

3 14

Show this thread

ZetaZeroes @ZetaZeroes Oct 21
Now look at this:
etherscan.io/tx/0x44aad3b85...
this is part of the alleged hack. What does it look like to you?

7 2 20

Show this thread

ZetaZeroes @ZetaZeroes Oct 21
Everything was public knowledge available to all, were you willing to take the time to understand it deeply enough, you would have found it too.

Given that this mispricing in the contract existed for a year or so without incident, it is likely that no one else knew about it.

2 2 25

ZetaZeroes @ZetaZeroes Oct 21
The market, if you are correct, and in the minority/contrarian position will reward you heavily for it.

1 2 24

Topics to follow

Tweets about the Topics you follow show up in your Home timeline

Ethereum cryptocurrency
Matic Network cryptocurrency
$ETH
Venture capital
Chainlink cryptocurrency
Bitcoin cryptocurrency
FinTech
Dana White
Vitalik Buterin
$TSLA

More Topics

ZetaZeroes @ZetaZeroes Oct 21
Hmm, why is it that you were watching so closely? If I recall correctly, your firm was one of the biggest, if not the biggest loser, in this trade. That must have stung.

And now I am to believe that you're philosophy on the matter has magically shifted? Very strange coincidence.

> **wishful cynic** @EvgenyGaevoy Oct 19
> Been following closely with indexed core team in the aftermath of the attack. Really challenged my views on certain things. If you've asked me 6 months back, I'd be firmly in the code is law camp
> twitter.com/d1ll0nk/status...
> Show this thread

4 1 26

Show this thread

Search Twitter

[redacted] ...

Home
Explore
Notifications
Messages
Bookmarks
Lists
Profile
More
Tweet

Search Twitter

ZetaZeroes @ZetaZeroes Oct 21
The market, if you are correct, and in the minority/contrarian position will reward you heavily for it.

1 2 24

Topics to follow

Tweets about the Topics you follow show up in your Home timeline

Ethereum cryptocurrency
Matic Network cryptocurrency
$ETH
Venture capital
Chainlink cryptocurrency
Bitcoin cryptocurrency
FinTech
Dana White
Vitalik Buterin
$TSLA

More Topics

ZetaZeroes @ZetaZeroes Oct 21
Hmm, why is it that you were watching so closely? If I recall correctly, your firm was one of the biggest, if not the biggest loser, in this trade. That must have stung.

And now I am to believe that you're philosophy on the matter has magically shifted? Very strange coincidence.

> **wishful cynic** @EvgenyGaevoy Oct 19
> Been following closely with indexed core team in the aftermath of the attack. Really challenged my views on certain things. If you've asked me 6 months back, I'd be firmly in the code is law camp
> twitter.com/d1ll0nk/status...
> Show this thread

4 1 26

Show this thread

ZetaZeroes @ZetaZeroes Oct 21

[redacted]

Home

Explore

Notifications

Messages

Bookmarks

Lists

Profile

More

Tweet

[redacted] ...

In general, this is the problem that I see a lot. When I make money, its fine, its libertarian,
its decentralized bro. When I do not make money, the game is rigged! Get the cops! It's illegal
because he made to much money too quickly.

4 4 39

ZetaZeroes @ZetaZeroes Oct 21

Again, much love and respect for you and wintermute.
But, if you cannot notice the hamstering and rationalizations going on in your own head, I trade against you again.

2 1 19

ZetaZeroes @ZetaZeroes Oct 20

This made me chuckle, this very funny.

> **ridderhoff** @hoffridder Oct 19
> Replying to @d1ll0nk
> btw one of ur employees was downloading porn while doxxing this kid twitter.com/hoffridder/sta...

2 11

ZetaZeroes @ZetaZeroes Oct 20

Have some more thots, in a few min.

12 2 15

ZetaZeroes Retweeted

Mr. Clean @yonggravy Oct 19

@ndxfi @d1ll0nk are on overtime damage control trying to appease those who's money they lost to @ZetaZeroes sick arb. Intimidation, doxxing, SEETHING. What he did was entirely legal and these smarmy nerds want to shift the blame from themselves to this kid. Take responsibility.

2 3 10

ZetaZeroes @ZetaZeroes Oct 16

I made mistake in poem, the line before the second tweet should be:
A single frog hops in the pool, does something cool;
To boil him, they try. Don't arb that , and they start to cry.

4 2 20

ZetaZeroes @ZetaZeroes Oct 16

Unironically first time using twatter, don't know how to delete

4 1 20

ZetaZeroes @ZetaZeroes Oct 16

(You must understand that all my poasts are ironies for lulz, put as much salt as you want on them.)

3 1 5

Show this thread

ZetaZeroes @ZetaZeroes Oct 16

There were frontrunners that copied my FFF pool arbitrage taking $5M from what I feel like is rightfully my balance. Should've been my $21M arbitrage instead of $16M.

Such is crypto. Don't kvetch about it too much. Git gud at the game or go home.

9 27 81

ZetaZeroes
43 Tweets
Follow

ZetaZeroes @ZetaZeroes Oct 16

You were out-traded. There is nothing you can do about that.
Had you and your LP providers put in the time and effort to understand balancer pools more,
you would have been able to keep this from happening and even out-trade me.

5 7 35

Show this thread

Search Twitter

You might like

CowSwap - MevProte... @MEVprotection Follow

Matti @mattigags Follow

MEV Alpha Leak

Home
Explore
Notifications
Messages
Bookmarks
Lists
Profile
More

Tweet

ZetaZeroes @ZetaZeroes Oct 16
So indexed, go try to join forces with (exchanges), (feds), and other swamp creatures.
But the glory of the frogs will NEVER be diminished. //////
6 2 21
Show this thread

ZetaZeroes @ZetaZeroes Oct 16
To boil him, they try. Don't arb that , and they start to cry.
But the frog is not dismayed, for he has god on his side.
4 2 8
Show this thread

ZetaZeroes @ZetaZeroes Oct 16
I must talk about the elephant in the room:
The Grand Indexed Plan for Higher TVL.
13 7 19
Show this thread

ZetaZeroes @ZetaZeroes Oct 16
And what is the result of all this? What remains?
The thing we are left with here is the old cliché. A tale as old as time:
2 2

ZetaZeroes @ZetaZeroes Oct 16
Developers eagerly announce,
how there project is read to pounce.
Taking on the lizards and glowies of the world;
2 2 7

ZetaZeroes @ZetaZeroes Oct 16
I will do a few poastings in a few minutes
1 10

ZetaZeroes @ZetaZeroes Oct 16
Yes, hello?
2 3 14

Search Twitter
Show more

What's happening

NFL Last night
Patriots at Bills
Trending with Mac Jones, Buffalo

Trending in Canada
#MontrealMassacre
3,178 Tweets

Toronto Star Yesterday
This small Ontario town is caught in COVID's rural-urban divide

Bloomberg Quickt... Last night
Jussie Smollett testifies 'there was no hoax' at trial

NHL Trending
#Canucks
Trending with Boudreau, Demko

Show more

[redacted] ···

THIS IS **EXHIBIT "37"** TO
THE AFFIDAVIT OF **LAURENCE DAY**
SWORN BEFORE ME
THIS 9th DAY OF DECEMBER, 2021

Stephen Aylward

A COMMISSIONER ETC.

Exact Formulas for Averages of Secular Coefficients

by

Andean Medjedovic

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Mathematics
in
Pure Mathematics

Waterloo, Ontario, Canada, 2021

Author's Declaration

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

We study averages of secular coefficients that frequently appear in random matrix theory. We obtain exact formulas, identities and new asymptotics for these integrals as well as a technique to deal with singularities that classically occur in the study of these problems.

Acknowledgements

It was my great fortune to have Michael O. Rubinstein advise me through the past few years. Thank you for the discussions, guidance and encouragement you have provided me with throughout the program.

I would also like to thank the researchers at the American Institute of Mathematics studying Random Matrix Theory for their insights and lectures on the field, as well as their general fellowship.

Lastly, I would like to thank my parents, [redacted] for their love and support.

Dedication

Dedicated to my parents, [redacted].

Table of Contents

0.1 List of Tables

0.2 List of Notation

(i) $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ is the Riemann zeta function.

(ii) $\delta(x)$ is the Dirac delta function.

(iii) $d_k(n) = \sum_{n_1 n_2 \ldots n_k = n} 1$ is the k-fold divisor function. It is the number of ways to write n as a product of k natural numbers.

(iv) RMT is an abbreviation for Random Matrix Theory.

(v) NT is an abbreviation for Number Theory.

(vi) $SSYT$ is an abbreviation for Semi-Standard Young Tableaux. A construct in partition theory which we will properly define later.

(vii) λ is a partition. λ_i is the i^{th} part of the partition. $s(\lambda)$ is the size of the partition and λ' is the conjugate partition to λ.

(viii) $U(N), SP(2N), O(N), SO(N)$ are the unitary, symplectic, and (special) orthogonal matrix groups.

(ix) χ^G is a character on the group G.

Chapter 1

Introduction

The goal of this thesis is to study the random matrix theory analogue of moments of L-functions. In particular, we develop a theory of averages of powers of determinants over matrix groups. Certain properties of these determinants have been studied by Keating, Rogers, Roditty-Gershon and Rudnick [12], Bump and Gamburd [8], as well as one of the authors [3]. These averages have long been known to be related to conjectures for asymptotics of higher moments of the ζ function [10].

1.1 Outline

- We motivate the study of a class of functions and so called "Secular Coefficients". We begin by reviewing known results for the unitary case in the rest of the introduction. We define and generalize the set of polynomials known within the literature as $\gamma_k(c)$. We summarize all the results contained in this thesis.
- In the next section, we briefly review some symmetric function theory and partition theory. We prove a Lemma the will be invaluable in our investigation that will allow us the remove certain singularities that classically appear in the study of these averages of characteristic polynomials of random matrices.
- We apply this Lemma along with results from Bump-Gamburd [8] as well as enumerations coming from the theory of plane partitions to get exact determinant formulas for averages of determinants of random matrices. We can use these ideas to deal with

a wide case of matrix families, the classical groups. This is the main achievement of the thesis.

- We then further analyze the Unitary case, obtaining properties of lower order terms of $\gamma_k(c)$.
- We give a short proof of the unimodality of $\gamma_k(c)$, which was conjectured by Ze'ev Rudnick.
- Lastly, we succinctly summarize further relations between the Riemann ζ function and averages of functions over random matrix groups.

The motivation is that we are trying to understand moments of the zeta function. We begin with taking powers of ζ, and we have the following identity for the divisor function. Let $d_k(n)$ be the k-th divisor numbers, i.e. the Dirichlet coefficients of the k-th power of the Riemann zeta function:

$$\zeta(s)^k = \sum_1^\infty \frac{d_k(n)}{n^s}, \qquad \Re s > 1. \tag{1.1}$$

The Dirichlet coefficient $d_k(n)$ is equal to the number of ways of writing n as a product of k factors. Define

$$S_k(X) = \sum_{n \le X} d_k(n). \tag{1.2}$$

The main term in the asymptotics of $S_k(x)$ comes from the pole at $s = 1$ of $\zeta^k(s)$. Let $XP_{k-1}(\log X)$ be the residue, at $s = 1$ of $\zeta(s)^k X^s/s$, with $P_{k-1}(\log X)$ being a polynomial in $\log X$ of degree $k-1$. Then

$$S_k(X) = XP_{k-1}(\log X) + \Delta_k(X), \tag{1.3}$$

with $\Delta_k(X)$ denoting the remainder term. The k-divisor problem asserts that $\Delta_k(x) = O_k(x^{\frac{k-1}{2k}+\epsilon})$. It is this remainder term that needs to be understood further.

The behaviour of Δ_k in short intervals was studied by Keating, Rodgers, Roditty-Gershon, and Rudnick [12]. Let

$$\Delta_k(x; H) = \Delta_k(x + H) - \Delta_k(x) \tag{1.4}$$

be the remainder term for sums of d_k over the interval $[x, x + H]$.

Define

$$a_k = \prod_p \Big\{ (1 - \frac{1}{p})^{k^2} \sum_{j=0}^{\infty} \left(\frac{\Gamma(k+j)}{\Gamma(k) j!} \right)^2 \frac{1}{p^j} \Big\}. \tag{1.5}$$

the product convergence is seen by expanding the terms with respect to p giving a product over $1 - \frac{C}{p^2} + O(\frac{1}{p^3})$, where C is a constant in k. By considering the analogous problem for function fields and related random matrix theory statistics, Keating, Rodgers, Roditty-Gershon, and Rudnick conjectured [12]:

Conjecture 1. *If $0 < \alpha < 1 - \frac{1}{k}$ is fixed, then for $H = X^\alpha$,*

$$\frac{1}{X} \int_X^{2X} \Big(\Delta_k(x, H) \Big)^2 dx \sim a_k \mathcal{P}_k(\alpha) H (\log X)^{k^2 - 1} \;, \quad X \to \infty \tag{1.6}$$

where $P_k(\alpha)$ is given by

$$\mathcal{P}_k(\alpha) = (1 - \alpha)^{k^2 - 1} \gamma_k(\frac{1}{1 - \alpha}) \;. \tag{1.7}$$

Here $\gamma_k(c)$ is a piecewise polynomial function defined in the next section. Thereby, we hope to gain a better understanding of the statistics of the k-divisor function by understanding the general theory of $\gamma_k(c)$ and related constructions.

We briefly touch on the results found by Keating et al. and how they connect not only RMT and NT, but analogous questions for function fields.

Let U be an $N \times N$ matrix. We define the *secular coefficients*, $\mathrm{Sc}_j(U)$, to be the coefficients of the characteristic polynomial of U:

$$\det(I + xU) = \sum_{j=0}^{N} \mathrm{Sc}_j(U) x^j. \tag{1.8}$$

Thus $\mathrm{Sc}_0(U) = 1$, $\mathrm{Sc}_1(U) = \operatorname{tr} U$, $\mathrm{Sc}_N(U) = \det U$. The secular coefficients are just elementary symmetric functions in the eigenvalues of U.

Let G be one of the matrix groups $U(N), Sp(2N), SO(N)$ or $O(N)$. Working with respect to the natural Haar measure in each case, define, for $G = Sp(2N), SO(N)$, or $U(N)$,

$$I_k^G(n,N) := \int_G \sum_{\substack{j_1+\cdots+j_k=n \\ 0\le j_1,\ldots,j_k\le N}} Sc_{j_1}(U)\ldots Sc_{j_k}(U)dU. \tag{1.9}$$

Unless $G = U(N)$ where we introduce a conjugate term, squaring the integrand (otherwise the average becomes 0):

$$I_k^G(n,N) := \int_G \sum_{\substack{j_1+\cdots+j_k=n \\ 0\le j_1,\ldots,j_k\le N}} |Sc_{j_1}(U)\ldots Sc_{j_k}(U)|^2 dU. \tag{1.10}$$

The connection to function field theory needs some additional notation. Let f be a monic polynomial in $\mathbb{F}_q$ and use $d_k(f)$ to denote the number of ways to write f as $f = f_1 \ldots f_k$ with f_i monic. We assume that the index A is a monic polynomial in $\mathbb{F}_q$. Furthermore, for a monic, define

$$I(A;h) = \{f : ||f - A|| \le q^h\} \tag{1.11}$$

with $||f|| = q^{\deg(f)}$ and

$$\mathcal{N}(A;h) := \sum_{f\in I(A;h)} d_k(f) \tag{1.12}$$

to be the divisor sum in function fields. Defining the difference and variance in short intervals similarly,

$$\Delta_k(A;h) := \mathcal{N}(A;h) - q^{h+1}\binom{n+k-1}{k-1}, \tag{1.13}$$

$$\mathrm{Var}(\mathcal{N}) := \frac{1}{q^n}\sum_{\deg(A)=n} |\Delta_k(A;h)|^2. \tag{1.14}$$

We then have the following estimate of the function field variance:

Theorem 1 (KRRR)**.** *If $0 \le h \le \min(n-5, (1-\frac{1}{k})n-2)$, then as $q \to \infty$*

$$\mathrm{Var}(\mathcal{N}) = H \cdot I_k^G(n; n-h-2) + O\Big(\frac{H}{\sqrt{q}}\Big), \tag{1.15}$$

for $H = q^{h+1}$.

In this case H is comparable to the short interval X^a in the NT case.

The following result in this direction is the following theorem due to Keating et al [12] which gives the leading asymptotics of I_k^G in terms of $\gamma_k(c)$.

Theorem 2 (KRRR)**.** *Let $c := m/N$. Then for $c \in [0, k]$,*

$$I_k^{U(n)}(m, N) = \gamma_k(c)N^{k^2-1} + O_k(N^{k^2-2}). \tag{1.16}$$

1.2 The polynomials $\gamma_k(c)$

The function $\gamma_k(c)$, mentioned in Conjecture 1 and Theorem 2, is defined by the following integral over a slice of the unit hyper-cube:

$$\gamma_k(c) = \frac{1}{k!\, G(1+k)^2} \int_{[0,1]^k} \delta(t_1 + \ldots + t_k - c) \prod_{i<j} (t_i - t_j)^2 \, dt_1 \ldots dt_k, \tag{1.17}$$

where G is the Barnes G-function, so that for positive integers k, $G(1+k) = 1! \cdot 2! \cdot 3! \cdots (k-1)!$.

The function $\gamma_k(c)$ is supported on $[0, k]$ and symmetric around $\frac{k}{2}$.

$$\gamma_k(c) = \gamma_k(k - c) \tag{1.18}$$

It is also known that

Theorem 3 (KRRR)**.**

$$\gamma_k(c) = \sum_{0 \le \ell < c} \binom{k}{\ell}^2 (c - \ell)^{(k-\ell)^2 + \ell^2 - 1} g_{k,\ell}(c - \ell) \tag{1.19}$$

where $g_{k,\ell}(c-\ell)$ are polynomials in $c-\ell$. No explicit form for $g_{k,\ell}$ is currently known. Note that the above implies that on each interval $[j-1, j]$, (for integer j), $\gamma_k(c)$ is a polynomial.

While the motivation in studying $\gamma_k(c)$ from a number theoretic perspective comes primarily from the connection to divisor sums, they are of their own interest from the perspective of random matrix theory. The focus of our thesis is on the underlying random matrix theory.

1.3 Main Results

The main results of this thesis are determinant identities for the generating function of $I_k^G(n,N)$. No exact formulas for these generating functions are known in the literature. Let $G \in \{U(N), O(N), SP(2N), SO(N)\}$ be a matrix group and consider

$$P_{k,N}^G(u) = \sum_{n=0}^{\infty} u^n I_k^G(n,N).$$

Then if $G = U(N)$

Theorem 4.

$$P_{k,N}^G(u) = \frac{C_{N,k}}{(1-u)^{k^2}} \det \frac{1-u^{N+i+j-1}}{N+i+j-1}$$

with

$$C_{N,k} = \prod_{j=1}^{k} \frac{(N+k-j-1)!}{(j-1)!^2\,(N+j-1)!}.$$

If $G = SP(2N)$ then

Theorem 5.

$$P_{k,N}^G(u) = \frac{1}{(1-u^2)^{\binom{k+1}{2}}} \det_{1\le i,j\le k} \left[\binom{j-1}{i-1}u^{j-i} - \binom{2N+2k+1-j}{i-1}u^{2N+2k+2-j-i}\right].$$

And finally, if $G = O(N)$ or $G = SO(N)$ we have

Theorem 6.

$$\begin{aligned}P_{k,N}^G(u) &= \frac{1}{2}\frac{1}{(1-u^2)^{\binom{k}{2}}} \\ &\det\left[\binom{j-1}{i-1}u^{j-i} - \binom{2N+2k-1-j}{i-1}u^{2N+2k-j-i}\right] \\ &+ \det\left[\binom{j-1}{i-1}u^{j-i} + \binom{2N+2k-1-j}{i-1}u^{2N+2k-j-i}\right].\end{aligned}$$

and

$$P^G_{k,N}(u) = \frac{1}{(1-u^2)^{\binom{k}{2}}} \det\left[\binom{j-1}{i-1}u^{j-1} + \binom{2N+2k-j-1}{i-1}u^{2N+2k-j-i}\right],$$

respectively.

The secondary results of this thesis are slightly more qualitative results. In Section 4 we prove that the lower order terms in the asymptotics for $I_k^{U(N)}$ in N have properties similar to $\gamma_k(c)$. That is to say, if $I_k^{U(N)}(cN, N) \sim \sum_{m=0} \gamma_{k,m}(c) N^{k^2-1-m}$ then:

1. $\gamma_{k,m}(c)$ is symmetric around $k/2$.
2. $\gamma_{k,m}(c)$ is supported on $[0, k]$ and on each interval $[j, j+1]$ (for j an integer) it is a polynomial.
3. Each polynomial piecewise composing $\gamma_{k,m}(c)$ is of degree at most $k^2 - m$.
4. $\gamma_{k,m}(c)$ is differentiable $k^2 - m - 2j(k-j) - 1$ times at a transition point $c = j$.

For example, $\gamma_{k,0}(c) = \gamma_k(c)$ and has exactly the above properties.

In section 5 we prove a conjecture of Ze'ev Rudnick [personal communication], that $\gamma_k(c)$ is unimodal.

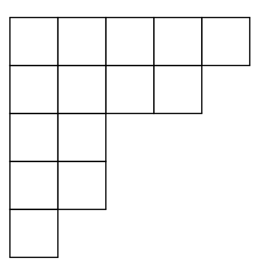
Chapter 2

Symmetric Function Theory

In this section we introduce some basics of symmetric function theory. The connection to symmetric function theory was used independently by Conrey, Farmer, Keating, Rubinstein and Snaith in CFKRS[9] as well as Bump and Gamburd in BG[8] to determine moments of characteristic polynomials of the classical compact groups. These results were used in CFKRS[9] to conjecture the asymptotics of the shifted moments of the ζ-function. We will describe the relevant symmetric function theory need for our results.

2.1 Young Diagrams

Let $\lambda = (\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_k)$ be a partition of n. Then $\lambda_1 + \lambda_2 + \ldots + \lambda_k = n$. To each partition λ we associate to it what is known as a Ferrer's diagram. The diagram is a collection of "cells" off length λ_i across. For example the partition of 14 given by $(5, 4, 2, 2, 1)$ corresponds to Ferrer's diagram



We say a Ferrer's diagram is a semi-standard young tableau when the cells are labeled by integers less than n in such a way so that the rows are non-decreasing and the columns are increasing, starting with 1 at the top-right most cell. A young tableau for the above would be:

1	2	2	3	4
3	4	4	4	
4	5			
5	7			
7				

We say such a semi-standard young tableau, T, is of shape λ if the Ferrer's diagram of the tableau is the Ferrer's diagram for λ. In which case we write $T \sim \lambda$.

We should also introduce the Schur polynomials $s_\lambda(x_1, \ldots, x_k)$, let $\Delta(x)$ be the determinant of the Vandermonde matrix:

$$\Delta(x) = \det_{1 \le i,j \le k} x_j^{i-1} = \prod_{i \neq j} (x_i - x_j). \tag{2.1}$$

We define the Schur polynomial of λ to be

$$s_\lambda(x_1, \ldots, x_k) = \frac{\det \begin{bmatrix} x_1^{\lambda_1+k-1} & x_2^{\lambda_1+k-1} & \ldots & x_k^{\lambda_1+k-1} \\ x_1^{\lambda_2+k-2} & x_2^{\lambda_2+k-2} & \ldots & x_k^{\lambda_2+k-2} \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{\lambda_k} & x_2^{\lambda_k} & \ldots & x_k^{\lambda_k} \end{bmatrix}}{\Delta(x)}. \tag{2.2}$$

Notice that s_λ is actually a polynomial as the determinant is 0 when $x_j = x_k$ for any j, k, canceling with the pole from the Vandermonde factor in the denominator. This definition of the Schur-functions is concise but unintuitive. An alternate definition follows.

We say T has *type* $a = (a_1, a_2, ...)$ if T has $a_i = a_i(T)$ parts equal to i. The SSYT above has type $(1, 2, 2, 5, 2, 0, 2)$. It is common to use the notational abbreviation

$$x^T = x_1^{a_1(T)} x_2^{a_2(T)} \cdots,$$

so for the example SSYT above,

$$x^T = x_1^1 x_2^2 x_3^2 x_4^5 x_5^2 x_7^2.$$

We finally come to the combinatorial definition of Schur functions.

Definition 1. *For a partition λ, the Schur function in the variables $x_1, ..., x_r$ indexed by λ is a multivariable polynomial defined by*

$$s_\lambda(x_1, ..., x_r) := \sum_T x_1^{a_1(T)} \cdots x_r^{a_r(T)},$$

where the sum is over all SSYTs T whose entries belong to the set $\{1, ..., r\}$ (i.e. $a_i(T) = 0$ for $i > r$).

For example, the SSYTs of shape $(4, 2)$ whose entries belong to the set $\{1, 2\}$ are

$$\begin{array}{|c|c|c|c|}\hline 1 & 1 & 1 & 1 \\ \hline 2 & 2 \\ \cline{1-2}\end{array} \qquad \begin{array}{|c|c|c|c|}\hline 1 & 1 & 1 & 2 \\ \hline 2 & 2 \\ \cline{1-2}\end{array} \qquad \begin{array}{|c|c|c|c|}\hline 1 & 1 & 2 & 2 \\ \hline 2 & 2 \\ \cline{1-2}\end{array}$$

and so

$$s_{(4,2)}(x_1, x_2) = x_1^4 x_2^2 + x_1^3 x_2^3 + x_1^2 x_2^4.$$

Nota bene, the value $s_\lambda(1, \ldots, 1)$ enumerates the total number of SSYT associated to the partition λ.

2.2 Singularity Removal For Moments

Consider a polynomial $P(x)$ given by

$$P(x) = \det_{1 \le i,j \le k} \left[x_{j-1}^{a_i} \right], \tag{2.3}$$

where a_i are non-negative integers. Then,

$$P(x) = P(x_0, \ldots, x_{k-1}) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=0}^{k-1} x_i^{a_{\sigma(i)}}. \tag{2.4}$$

This is an alternating polynomial and thus divisible by $\Delta(x)$. We are interested in finding $\frac{P(x)}{\Delta(x)}$ when $x_0 = x_1 = x_2 = \ldots = x_{k-1} = u$. Taking the limit as $x_1 \to x_2$, $x_2 \to x_3$, etc. and applying L' Hopital's rule gives

$$\lim_{x \to (u,\ldots,u)} \frac{P(x)}{\Delta(x)} = \frac{1}{1!2! \ldots (k-1)!} \frac{\partial^{k-1}}{\partial x_{k-1}^{k-1}} \cdots \frac{\partial^2}{\partial {x_2}^2} \frac{\partial}{\partial x_1} \Big|_{(u,\ldots,u)} P(x). \tag{2.5}$$

We expand $P(x)$ according to its definition taking derivatives and matching $i!$ with the $a_{\sigma(i)}$ terms to get binomial coefficients.

$$\lim_{x\to(u,\ldots,u)} \frac{P(x)}{\Delta(x)} = \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) \prod_{i=0}^{k-1} \binom{a_{\sigma(i)}}{i} x_i^{a_{\sigma(i)}-i}\Big|_{(u,\ldots,u)}. \tag{2.6}$$

And we have computed the removable singularities of $\frac{P(x)}{\Delta(x)}$ to be

$$\frac{P(x)}{\Delta(x)}\Big|_{(u,\ldots,u)} = \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) \prod_{i=0}^{k-1} \binom{a_{\sigma(i)}}{i} x_i^{a_{\sigma(i)}-i}\Big|_{(u,\ldots,u)} \tag{2.7}$$

$$= \det_{1\le i,j\le k}\left[\binom{a_j}{i-1} x_{i-1}^{a_j-i+1}\right]\Big|_{(u,\ldots,u)} \tag{2.8}$$

$$= \det_{1\le i,j\le k}\left[\binom{a_j}{i-1} u^{a_j-i+1}\right]. \tag{2.9}$$

We can extend this theorem slightly in the following Lemma.

Lemma 1. *Let* $P(x) = \det_{1\le i,j\le k}[p_j(x_{i-1})]$ *be an alternating polynomial where each* p_j *is itself a polynomial. Then*

$$\frac{P(x)}{\Delta(x)}\Big|_{(u,\ldots,u)} = \det_{1\le i,j\le k}\left[\frac{1}{i-1!}\frac{\partial^{i-1}}{\partial u^{i-1}} p_j(u)\right]. \tag{2.10}$$

Proof. If each p_j is a monomial then the proof is detailed above. In the case that p_j are not monomials we may split up the determinant as a sum of monomials by multi-linearity and apply the above recipe on each term individually. Adding the terms together by multi-linearity again yields Lemma 1. □

This Lemma will be crucial in removing singularities that appear in expressions for averages of secular coefficients. This will allow us to get an exact formula for certain matrix theory integrals that appear in the literature.

Chapter 3

Secular Coefficients of Matrix Groups

3.1 The Unitary Group

We will apply the singularity removal technique to equation (2.9) in Autocorrelations of Random Matrix polynomials [9]. That formula is reproduced below in equation (3.3). Let $G = U(N)$ and let $U \in U(N)$. First notice the following relation

$$\det(I - xU)^k \det(I - yU^*)^k = \left(\sum_{j=1}^{N} \mathrm{Sc}_j(U)(-x)^j\right)^k \left(\sum_{i=1}^{N} \mathrm{Sc}_i(U^*)(-y)^i\right)^k \tag{3.1}$$

and integrate over the unitary group.

$$\int_G \det(I - xU)^k \det(I - yU^*)^k dU = \sum_{0 \leq m \leq kN} I_k^G(n, N)(xy)^n. \tag{3.2}$$

In the above equation only diagonal terms remain, i.e. the coefficients of the terms of form $x^n y^m, m \neq n$, are 0. Consider the map $U \mapsto e^{it}U$ which by the invariance of the Haar measure does not change the value of the integral. Under this map, U^* gets scaled by e^{-it}. We can absorb the e^{it} terms in x and e^{-it} in y so that the term $x^n y^m$ in the sum becomes $e^{(n-m)it} x^n y^m$. Since the integral is invariant under this transformation, the sum should be too, and so the coefficient of any term with $n \neq m$ is indeed 0.

Formula (2.9) of the Autocorrelations paper is copied below:

$$\prod_{l=m+1}^{r} w_l^N \int_{U(N)} \prod_{i=m+1}^{n} \det(I - w_i^{-1}U) \prod_{j=1}^{m} \det(I - w_j U^*) dU \tag{3.3}$$
$$= \frac{1}{\prod_{1\le \ell < q \le n}(w_q - w_\ell)} \begin{vmatrix} 1 & w_1 & w_1^2 & \cdots & w_1^{m-1} & w_1^{N+m} & w_1^{N+m+1} & \cdots & w_1^{N+n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & w_n & w_n^2 & \cdots & w_n^{m-1} & w_n^{N+m} & w_n^{N+m+1} & \cdots & w_n^{N+n-1} \end{vmatrix}.$$

Specializing to $m = k, n = 2k$, $w_1 = w_2 = \ldots = w_k = x$ and $w_{k+1} = \ldots = w_{2k} = 1$ and removing the singularities as in Lemma 1 gives

$$I_k^{U(N)}(n, N) = [x^n] \frac{1}{(1-x)^{k^2}} \begin{vmatrix} A(x) & B(x) \\ A(1) & B(1) \end{vmatrix} \tag{3.4}$$

where

$$A_{ij}(x) = \binom{j-1}{i-1} x^{j-i} \tag{3.5}$$
$$B_{ij}(x) = \binom{N+2k+j-1}{i-1} x^{N+2k+j-i}. \tag{3.6}$$

We now are going to perform row reductions on the above. Notice $A(x)^{-1} = A(-x)$, as can be verified using the underlying binomial identity

$$\sum_{l=1}^{k} (-1)^{i+l} \binom{l-1}{i-1} \binom{j-1}{l-1} = \binom{j-1}{i-1} \sum_{l=1}^{k} (-1)^{i-l} \binom{j-i}{l-i}. \tag{3.7}$$

If $j > i$ the sum on the right is an alternating sum of the $(j-i)^{th}$ row of Pascal's triangle and vanishes. If $j < i$ the factor of $\binom{j-1}{i-1}$ infront of the sum is 0. And if $i = j$ only one term contributes to the sum, namely $l = i$, giving 1. Thus, multiplying the block matrix in 3.4 on the left by the block matrix

$$\begin{pmatrix} A(-x) & 0 \\ 0 & A(-1) \end{pmatrix} \tag{3.8}$$

gives

$$\left(\begin{array}{cc} A(-x) & 0 \\ 0 & A(-1) \end{array}\right)\left(\begin{array}{cc} A(x) & B(x) \\ A(1) & B(1) \end{array}\right)=\left(\begin{array}{cc} I & A(-x)B(x) \\ I & A(-1)B(1) \end{array}\right), \tag{3.9}$$

and then by multiplying with

$$\left(\begin{array}{cc} I & 0 \\ -I & I \end{array}\right) \tag{3.10}$$

to remove the bottom left I:

$$\left(\begin{array}{cc} I & 0 \\ -I & I \end{array}\right)\left(\begin{array}{cc} I & A(-x)B(x) \\ I & A(-1)B(1) \end{array}\right)=\left(\begin{array}{cc} I & A(-x)B(x) \\ 0 & A(-1)B(1)-A(-x)B(x) \end{array}\right). \tag{3.11}$$

These multiplications do not change the determinant as both multiplications are by triangular matrices with 1's on the diagonal. Therefore the determinant of the matrix in (3.4) equals the determinant of the lower $k \times k$ block above, i.e.

$$|A(-1)B(1)-A(-x)B(x)|_{k\times k}. \tag{3.12}$$

Next we compute the entries of the above matrix. The i, j entry is

$$\sum_{l=1}^{k}(-1)^{l-i}\binom{l-1}{i-1}\binom{N+k+j-1}{l-1}(1-x^{N+k+j-i}) \tag{3.13}$$

but,

$$\binom{l-1}{i-1}\binom{N+k+j-1}{l-1}=\binom{N+k+j-1}{i-1}\binom{N+k+j-i}{l-i}. \tag{3.14}$$

so that equation 3.13 equals

$$\binom{N+k+j-1}{i-1}(1-x^{N+k+j-i})(-1)^{i}\sum_{l=1}^{k}(-1)^{l}\binom{N+k+j-i}{l-i}. \tag{3.15}$$

But the sum above equals

$$(-1)^{i}\sum_{l=0}^{k-i}(-1)^{l}\binom{N+k+j-i}{l}. \tag{3.16}$$

This is an alternating sum of the $N+k+j-i$ row of Pascal's triangle which so the above famously equals

$$(-1)^k \binom{N+k+j-i-1}{k-i}. \tag{3.17}$$

Returning to the $k \times k$ determinant we see that the i,j entry of the matrix equals

$$(-1)^{k-i} \binom{N+k+j-1}{i-1} \binom{N+k+j-i-1}{k-i} (1-x^{N+k+j-i}). \tag{3.18}$$

This product of binomial coefficients equals

$$\binom{N+k+j-1}{i-1} \binom{N+k+j-i-1}{k-i} = \frac{(N+k+j-1)!}{(i-1)!(k-i)!(N+j-1)!(N+k+j-i)}. \tag{3.19}$$

We can thus pull out from row i of the determinant a factor of $\frac{(-1)^{k-i}}{((i-1)!(k-i)!)}$ and a factor of $\frac{(N+k+j-1)!}{(N+j-1)!}$ from column j. Therefore, the determinant in (3.4) equals, on collecting these factors,

$$\prod_{j=1}^{k} \frac{(-1)^{k-j}(N+k+j-1)!}{(j-1)!(k-j)!(N+j-1)!} \det \left[\frac{1-x^{N+k+j-i}}{N+k+j-i} \right]_{k \times k} = \tag{3.20}$$

$$\prod_{j=1}^{k} \frac{(N+k+j-1)!}{(j-1)!^2 (N+j-1)!} \det \left[\frac{1-x^{N+i+j-1}}{N+i+j-1} \right]_{k \times k} \tag{3.21}$$

where, in the last equality we have reversed the k rows of the matrix. We have thus arrived at the formula of Theorem 4:

$$I_k^{U(N)}(n,N) = [x^n] \frac{C_{N,k}}{(1-x)^{k^2}} \det \frac{1-x^{N+i+j-1}}{N+i+j-1}. \tag{3.22}$$

Here $C_{N,k}$ is a constant depending only on N and k and can be given explicitly in several ways:

$$C_{N,k} = \prod_{j=1}^{k} \frac{(N+k+j-1)!}{(j-1)!^2\,(N+j-1)!} = \frac{\prod_{1 \le i,j \le k}(N+i+j-1)}{\prod_{1 \le i < j \le k}(j-i)^2} \tag{3.23}$$

$$C_{N,k} = \frac{1}{\det_{1 \le i,j \le k}[\frac{1}{N+i+j-1}]} \tag{3.24}$$

$$C_{N,k} = \frac{G(N+2k)G(N)}{G(N+k)^2 G(k)^2} \tag{3.25}$$

where $G(m) = 1!2!\dots(m-1)!$ is the Barnes G-function.

3.2 The Symplectic Group

We move on the symplectic case now. Let $G = SP(2N)$. We begin with proposition (11) and equation (43) from Bump-Gamburd [8].

$$\int_{Sp(2N)} \prod_{i=1}^{k} \det\left(1 + x_i U\right) dU = \left(x_1 \dots x_k\right)^N \chi_{\left\langle N^k \right\rangle}^{Sp(2k)}(x_1^{\pm 1}, \dots, x_k^{\pm 1}). \tag{3.26}$$

Here $\chi_{\left\langle N^k \right\rangle}^{Sp(2k)}$ is a certain irreducible character from the representation theory of $\mathrm{GL}_n(\mathbb{C})$. A partition is said to be even if all parts of it are even. From section 7.1 of the same paper we have

$$\left(x_1 \dots x_k\right)^N \chi_{<N^k>}^{Sp(2k)}(x_1^{\pm 1}, \dots, x_k^{\pm 1}) = \sum_{\substack{\lambda_1 \le 2N \\ \lambda \textbf{ even}}} s_\lambda(x_1, \dots, x_k). \tag{3.27}$$

where the sum is taken over all even partitions.

Let $G = Sp(2N)$.

Consider the generating function

$$\sum_{n=0}^{2kN} x^n I_k^G(n, N) = \int_{Sp(2N)} \det(1 + xU)^k dU. \tag{3.28}$$

We are trying to extract the $[x^n]$ coefficient of

$$\sum_{\substack{\lambda_1 \le 2N \\ \lambda \textbf{ even}}} s_\lambda \overbrace{(x, \dots, x)}^{k}. \tag{3.29}$$

By the combinatorial interpretation of Schur functions the coefficient we desire is

$$\sum_{\substack{s(\lambda)=n \\ \lambda_1 \le 2N \\ \lambda \textbf{ even}}} s_\lambda \overbrace{(1, \dots, 1)}^{k}. \tag{3.30}$$

where $s(\lambda)$ is the size of the partition. One can see that $s_\lambda \overbrace{(1, \dots, 1)}^{k}$ as the number of semi-standard young tableaux of type λ. Hook content formula gives $s_\lambda(1, ..., 1) = \prod_{u \in \lambda} \frac{n+c(u)}{h(u)}$

where $c(u)$ and $h(u)$ are the content and hook of a cell $u \in \lambda$.

Other identities for partitions of the form described in equation (3.29) are well-known within literature dealing with plane partitions. A famous example is the Hall-Littlewood identity [1].

$$\sum_{\lambda \text{ even}} s_\lambda(x_1, \ldots, x_k) = \prod_{i=1}^{k} \frac{1}{1 - x_i^2} \prod_{i<j} \frac{1}{1 - x_i x_j} \tag{3.31}$$

Note that if $n < 2N$ then the constraint from our formula drops out and the Hall-Littlewood identity allows us to immediately calculate

$$I_k^{Sp(2n)}(n, N) = \begin{cases} \binom{\frac{n}{2} + \binom{k+1}{2} - 1}{\binom{k+1}{2} - 1}, & \text{for } n \text{ even} \\ 0, & \text{otherwise} \end{cases}. \tag{3.32}$$

In other domains we must use bounded forms of the Hall-Littlewood identities. For this we use the Desarmenien-Stembridge-Proctor formula [14], [4] , [5].

$$\sum_{\substack{\lambda_1 \leq 2N \\ \lambda \text{ even}}} s_\lambda(x_1, \ldots, x_k) = \frac{1}{\Delta(x)} \prod_{i=1}^{k} \frac{1}{1 - x_i^2} \prod_{i<j} \frac{1}{1 - x_i x_j} \det_{1 \leq i,j \leq k} \left[x_i^{j-1} - x_i^{2N+2k+1-j} \right] \tag{3.33}$$

where $\Delta(x) = \prod_{i<j}(x_i - x_j)$ is the Vandermonde determinant. The difficulty here is singularities appear when all x_i are equal. Of course, since we are ultimately dealing with a finite sum of polynomials , these singularities must be removable.

We now apply the formula derived in Lemma 1 above to the Desarmenien-Stembridge-Proctor formula.

$$\frac{1}{\Delta(x)} \prod_{i=1}^{k} \frac{1}{1 - x_i^2} \prod_{i<j} \frac{1}{1 - x_i x_j} \det_{1 \leq i,j \leq k} \left[x_i^{j-1} - x_i^{2N+2k+1-j} \right] |_{(u,\ldots,u)} = \frac{1}{(1 - u^2)^{\binom{k+1}{2}}} \frac{\det_{1 \leq i,j \leq k} \left[x_i^{j-1} - x_i^{2N+2k+1-j} \right]}{\Delta(x)} \Big|_{(u,\ldots,u)} \tag{3.34}$$

In this case, since we are not working with monomial terms anymore the determinant expression gets more complicated but we can decompose it by multi-linearity and then apply the above formula to get rid of the $\frac{1}{\Delta(x)}$, putting everything back together again with multi-linearity.

$$\frac{\det_{1\le i,j\le k}\left[x_i^{j-1}-x_i^{2N+2k+1-j}\right]}{\Delta(x)}\Big|_{(u,\ldots,u)} \tag{3.35}$$

$$=\frac{1}{\Delta(x)}\sum_{\sigma\in S_n}\sum_{S\subset\{1,\ldots,k\}}(-1)^{|S|}\operatorname{sgn}(\sigma)\prod_{i\in S}x_i^{2N+2k+1-\sigma(i)}\prod_{i\notin S}x_i^{\sigma(i)-1}\Big|_{(u,\ldots,u)} \tag{3.36}$$

$$=\sum_{S\subset\{1,\ldots,k\}}(-1)^{|S|}\sum_{\sigma\in S_n}\frac{\operatorname{sgn}(\sigma)}{\Delta(x)}\prod_{i\in S}x_i^{2N+2k+1-\sigma(i)}\prod_{i\notin S}x_i^{\sigma(i)-1}\Big|_{(u,\ldots,u)} \tag{3.37}$$

$$=\det_{1\le i,j\le k}\left[\binom{j-1}{i-1}u^{j-i}-\binom{2N+2k+1-j}{i-1}u^{2N+2k+2-j-i}\right] \tag{3.38}$$

To summarize, if we let

$$P_{k,N}(u)=\sum_{n=0}^{2kN}u^n I_k^{Sp(2n)}(n,N). \tag{3.39}$$

Then we have the following formula of Theorem 5:

$$P_{k,N}(u)=\frac{1}{(1-u^2)^{\binom{k+1}{2}}}\det_{1\le i,j\le k}\left[\binom{j-1}{i-1}u^{j-i}-\binom{2N+2k+1-j}{i-1}u^{2N+2k+2-j-i}\right].$$

3.3 The Orthogonal and Special Orthogonal Group

In this section we use similar ideas to the previous section to deal with the $G=SO(2N)$ and $G=O(2N)$ case.

3.3.1 The Orthogonal Group

Let $G=O(2N)$. Our starting point is again

$$I_k^G(n,N):=\int_G\sum_{\substack{j_1+\cdots+j_k=n\\0\le j_1,\ldots,j_k\le N}}Sc_{j_1}(U)\ldots Sc_{j_k}(U)dU \tag{3.40}$$

for a matrix group G.

Consider the generating function

$$\sum_{n=0}^{2kN} x^n I_k^G(n,N) = \int_G \det(1+xU)^k dU. \tag{3.41}$$

Again, we refer to Bump-Gamburd for the first step. In equation 102, after specializing to $x_i = x_j$ for all i, j they give

$$\int_G \det(I+xU)^k dU = \sum_{\substack{\lambda_1 \le 2N \\ \lambda' \text{ even}}} s_\lambda(x,\ldots,x). \tag{3.42}$$

where λ' is the conjugate partition of λ. As before, if we want $I_k^G(n,N)$ we can isolate the x^n term of the above as

$$\sum_{\substack{s(\lambda)=n \\ \lambda_1 \le 2N \\ \lambda' \text{ even}}} s_\lambda(1,\ldots,1), \tag{3.43}$$

the total number of SSYT of partitions with even conjugate. Okada [7] gives an enumeration of such sums and we will apply our Lemma 1 to remove the singularities:

$$\sum_{\substack{\lambda_1 \le 2N \\ \lambda' \text{ even}}} s_\lambda(x_1,\ldots,x_k) = \frac{1}{2}\,\frac{\det(x_i^{j-1} - x_i^{2N+2k-1-j}) + \det(x_i^{j-1} + x_i^{2N+2k-1-j})}{\prod_{1 \le i < j \le k}(x_i x_j - 1)(x_i - x_j)} \tag{3.44}$$

Let

$$P_{k,N}(u) = \sum_{n=0}^{2kN} u^n I_k^G(n,N)$$

be the polynomial whose coefficients enumerate the averages we are after. Setting all $x_i = u$ and using Lemma 1 the resulting sum of determinants gives the first formula of Theorem 6.

$$\begin{aligned} P_{k,N}(u) &= \frac{1}{2}\frac{1}{(1-u^2)^{\binom{k}{2}}} \\ &\left(\det\left[\binom{j-1}{i-1}u^{j-i} - \binom{2N+2k-1-j}{i-1}u^{2N+2k-j-i}\right]\right. \\ &\left.+ \det\left[\binom{j-1}{i-1}u^{j-i} + \binom{2N+2k-1-j}{i-1}u^{2N+2k-j-i}\right]\right). \end{aligned}$$

3.3.2 The Special Orthogonal Group

Let $G = SO(2N)$ and keep the same notation as the previous subsection. The special orthogonal case is a little easier to handle. Equation 71 in Bump-Gamburd gives a relation for the integral we want in terms of a matrix

$$\int_G \prod_{j=1}^{k} \det(I + x_j g) = (x_1 \dots x_k)^N \chi^{O_{2k}}_{\langle N^k \rangle}(x_1^{\pm 1}, \cdots, x_k^{\pm 1}) \tag{3.45}$$

Where the character χ can be written explicitly as

$$(x_1 \dots x_k)^N \chi^{O(2k)}_{N^k}(x_1^{\pm 1}, \cdots, x_k^{\pm 1}) =$$

$$\det \begin{vmatrix} x_1^{N+k-1} + x_1^{-(N+k-1)} & x_1^{N+k-2} - x_1^{-(N+k-2)} & \cdots & x_1^N - x_1^{-(N)} \\ \vdots & \vdots & \ddots & \vdots \\ x_k^{N+k-1} - x_k^{-(N+k-1)} & x_k^{N+k-2} - x_k^{-(N+k-2)} & \cdots & x_k^N - x_k^{-(N)} \end{vmatrix} \tag{3.46}$$

$$\times \frac{(x_1 \cdots x_k)^{k+N-1}}{\prod_{1 \leqslant i < j \leqslant k}(x_i - x_j)(x_i x_j - 1)}.$$

If we let

$$P_{k,N}(u) = \sum_{n=0}^{2kN} u^n I_k^G(n, N)$$

the consequently (after an application of Lemma 1) we obtain, the second formula in Theorem 6:

$$P_{k,N}(u) =$$
$$\frac{1}{(1-u^2)^{\binom{k}{2}}} \det \left[\binom{j-1}{i-1} u^{j-1} + \binom{2N+2k-j-1}{i-1} u^{2N+2k-j-i} \right].$$

Chapter 4

Asymptotic Behavior of the Unitary Group & Lower Order Terms

4.1 Analysis by Minors

Let

$$F_{N,k}(x) := \det_{1\le i,j\le k}\left(\frac{x^{N+i+j-1}-1}{N+i+j-1}\right).$$

This is, up to sign, the determinant that occurs in Theorem 4, the unitary case, though we prefer here to write the numerator as $x^{N+i+j-1}-1$. Our goal is to get an understanding of the asymptotic behavior of this determinant so we can get higher order analogues of $\gamma_k(c)$.

We expand the above determinant as a sum of its minors. Imagine choosing sets $S,T\subset\{1,\dots,k\}$ that denote rows/columns where we choose powers of x in our power series expansion of F and what remains is the minor S^c,T^c. Each minor is a Cauchy matrix and there are known formulas for computing these determinants. Let $s(S)=\sum_{a\in S}a$, the sum of elements of S.

$$F_{N,k}(x) = \sum_{\substack{S,T\subset\{1,\dots,k\}\\|S|=|T|}} (-1)^{s(S)+s(T)} \det_{i\in S,j\in T}\left(\frac{x^{N+i+j-1}}{N+i+j-1}\right) \det_{i\in S^c,j\in T^c}\left(\frac{-1}{N+i+j-1}\right). \tag{4.1}$$

The determinant on the right hand side that is dependent on x is homogeneous. A more general version of this formula can be found in [13].

$$F_{N,k}(x) =$$

$$\sum_{\substack{S,T\subset\{1,\dots,k\}\\|S|=|T|}} (-1)^{k-|S|+s(S)+s(T)} x^{(N-1)|S|+\sum_{i\in S} i+\sum_{j\in T} j} \det_{i\in S, j\in T}\left(\frac{1}{N+i+j-1}\right) \det_{i\in S^c, j\in T^c}\left(\frac{1}{N+i+j-1}\right). \tag{4.2}$$

We now make use of Cauchy's determinant formula.

Theorem 7 (Cauchy)**.** *Let* $A=\{\alpha_1,\dots,\alpha_k\}, B=\{\beta_1,\dots,\beta_k\}$. *Then*

$$\det\left(\frac{1}{\alpha_i+\beta_j}\right) = \frac{\Delta(A)\Delta(B)}{P(A,B)},$$

where $\Delta(S)=\prod_{i<j}(s_i-s_j)$ *and* $P(S+T)=\prod_{s\in S,t\in T}(s+t)$.

Let $N+S$ denote the set obtained by adding the integer N to each element of S. Likewise, let $T-1$ be the set obtained by subtracting 1 from each element of T. Applying this to the product of two minors in our expression for $F_{N,k}$ with $A=N+S$ and $B=T-1$ and noticing we can factor out $C_{N,k}$, using 3.24 yields

$$\det_{i\in S, j\in T}\left(\frac{1}{N+i+j-1}\right) \det_{i\in S^c, j\in T^c}\left(\frac{1}{N+i+j-1}\right) = \frac{\Delta(S)\Delta(T)\Delta(S^c)\Delta(T^c)}{P(N+S,T-1)P((N+S)^c,(T-1)^c} \tag{4.3}$$

$$= \frac{1}{C_{N,k}} \frac{P(N+S,(T-1)^c)P\left((N+S)^c,T-1\right)}{P\left(S,-S^c\right)P\left(T,-T^c\right)}. \tag{4.4}$$

In the first equality we used $\Delta(N+S)=\Delta(S)$ and $\Delta(T-1)=\Delta(T)$ and likewise for their complements, S^c, T^c. In the second equality we factor out the $\frac{1}{C_{N,k}}$ and are left with the remaining products. To proceed multiply the polynomial $F_{N,k}(x)$ by the power series of $\frac{(-1)^k C_{N,k}}{(1-x)^{k^2}}$. The x^n coefficient of the resulting polynomial is

$$(-1)^k \sum_{m=0}^{n} C_{N,k} \binom{k^2-1+n-m}{k^2-1} [x^m] F_{N,k}(x) \tag{4.5}$$

For given k, if N is sufficiently large, notice that powers in the above polynomial cluster around jN for an integer $j \leq k$. That is, all non-zero terms in $F_{N,k}$ that involve terms x^m for $m = jN + l$ with l being an integer less than k^2. Let $jN \leq n = cN \leq (j+1)N$ so the above becomes

$$\sum_{j=0}^{c} \sum_{l=0}^{k^2} \binom{k^2 - 1 + (c-j)N - l}{k^2 - 1} \tag{4.6}$$
$$\times \sum_{\substack{S,T \subset \{1,\ldots,k\} \\ |S|=|T| \\ (N-1)|S| + \sum_{s\in S} s + \sum_{t \in T} t = jN+l}} (-1)^{|S|+s(S)+s(T)} \frac{P(S+N, (T-1)^c) P\left((S+N)^c, T-1\right)}{P\left(S, -S^c\right) P\left(T, -T^c\right)}.$$

We can take note of the following properties from the above formula. As c passes through integers $1, 2, \ldots k$ new terms are added to the above double sum. These terms are a polynomial in $(c-j)$. Suppose we want to know the polynomials associated to the N^{k^2-m} term. This is a generalization of $\gamma_k(c)$ which occurs when $m = 1$. All terms involving $(c-j)$ to some power come from the binomial coefficient. The product of minors on the right contributes at most terms of order $N^{2j(k-j)}$. Therefore, at the transition points we are adding polynomials which have zeroes of order $k^2 - m - 2j(k-j)$ (assuming this quantity is positive), coming from the binomial coefficients in the above expression. This makes the resulting piecewise function very smooth. To be precise,

Theorem 8. *The piecewise function of polynomials giving asymptotics for the N^{k^2-m} power of N has the following properties:*

- *It is symmetric around $k/2$.*
- *It is supported on $[0, k]$ and on each interval $[j, j+1]$ (for j an integer) it is a polynomial.*
- *Each polynomial is of degree at most $k^2 - m$.*
- *It is differentiable $k^2 - m - 2j(k-j) - 1$ times at a transition point $c = j$.*

The first property is a consequence of the functional relation for $I_k^{U(N)}$. The second property comes from 4.6 and noticing that $I_k^{U(N)}$ is 0 for $c > k$. The third property comes from noticing that in the binomials in 4.6, a factor of c is paired with a factor of N always.

The fourth property comes from the previously described differentiability at 0. That is to say, if

$$I_k^{U(N)}(n,N) = \gamma_k(c)N^{k^2-1} + \gamma_{k,1}(c)N^{k^2-2} + \gamma_{k,2}(c)N^{k^2-3} + \dots,$$

then $\gamma_{k,m}(c)$ share the same properties as $\gamma_k(c)$ in the above way. All of the lower order terms in N are highly smooth symmetric piecewise polynomials on the domain $[0,k]$.

4.1.1 A recursion for $F_{N,k}(x)$

Let M be a $k \times k$ matrix, M_i^j then $(k-1)\times(k-1)$ the matrix obtained by deleting row i and column j of M and $M_{i,j}^{l,m}$ be the $(k-2)\times(k-2)$ matrix obtained from M by deleting rows i and j, and columns l and m.

The Desnanot-Jacobi identity states that

$$\det(M)\det(M_{1,k}^{1,k}) = \det(M_1^1)\det(M_k^k) - \det(M_1^k)\det(M_k^1). \tag{4.7}$$

Applying this identity to $F_{N,k}(x)$ gives

$$F_{N,k}(x) = \frac{F_{N+2,k-1}(x)F_{N,k-1}(x) - F_{N+1,k-1}(x)^2}{F_{N+2,k-2}(x)}. \tag{4.8}$$

This follows from the observation that the entries of $F_{N,k}(x)$ are of the form $\frac{X^{N+i+j-1}-1}{N+i+j-1}$, with $N+i+j-1$ increasing by 1 as we increment either i or j.

This recursion allows one to determine the polynomial $F_{N,k}(x)$ the from the polynomials for $k-1$ and $k-2$.

Chapter 5

Further Properties

5.1 Unimodality of $\gamma_k(c)$

We review some more basic properties of $\gamma_k(c)$. In the appendix we have plots of $\gamma_k(c)$ for $k = 4$. On each interval $[j-1, j]$ for $j \leq 4$, an integer, $\gamma_k(c)$ is a different polynomial. These polynomials approximate a Gaussian.

Indeed, the Gaussian behavior suggest that $\gamma_k(c)$ is unimodal. This question was raised by Rudnick during a conference a few years ago. Recently, Rogers remarked that $\gamma_k(c)$ is log-concave and outlined a proof[11]. We give a shorter proof here and show that this log-concavity implies unimodality.

The Gaussian behaviour was shown explicitly in earlier work due to Basor, Ge and Rubinstein [3], at least asymptotically around the center. The following theorem summarizes the Gaussian nature in the limiting case

Theorem 9 (Basor, Ge, Rubinstein)**.** *Let* $b_k = 8(1 - 1/(4k^2))$ *and* $c = k/2 + o(k)$*. Then*

$$\gamma_k(c) \sim \frac{G(k+1)^2}{G(2k+1)} \sqrt{\frac{b_k}{\pi}} e^{-b_k(c-k/2)^2}.$$

We move on to the proof of unimodality, log-concavity and some recurrence relations for $\gamma_k(c)$ and related functions.

Let

$$P_{\alpha,\beta,\gamma}(x) = \left(\prod_{i=1}^{k} x_i\right)^{\alpha} \left(\prod_{i=1}^{k} 1 - x_i\right)^{\beta} \left(\prod_{i \neq j} |x_i - x_j|\right)^{\gamma}. \tag{5.1}$$

We are interested in the integral

$$y_{\alpha,\beta,\gamma}(c) = \int_{C^k} \delta\left(c - \sum_{i=1}^{k} x_i\right) P_{\alpha,\beta,\gamma}(x), \tag{5.2}$$

with C^k being the unit cube and δ being the Dirac delta function which is a generalization of the integral that appears in the definition (1.15) of $\gamma_k(c)$.

Theorem 10. *The functions $y_{\alpha,\beta,\gamma}(c)$ are unimodal if $\alpha, \beta, \gamma > 1$ and real.*

We first prove unimodality is guaranteed by log-concavity. Let $f : [0,1] \to \mathbb{R}$ and assume f is bounded, continuous and log-concave. Furthermore assume f is positive on its interior. We prove that f must be unimodal.

Proof. Suppose $f'(a) = f'(b) = 0$ for some $a \neq b$ in $[0,1]$, where a is a global maximum. Since f is log-concave, $\log f$ is a concave function with vanishing derivative at a and b. Consider the line segment from $(a, \log f(a))$ to $(b, \log f(b))$. WLOG let $b < a$, so it has positive slope. Since the derivative of $\log(f)$ at b is 0 there is some neighbourhood to the right of b contained under the line segment. But this contradicts concavity. $\square$

Now it remains to see that $y_{\alpha,\beta,\gamma}(c)$ is log-concave. Consider the domain where the integrand is non-zero, $C^k \cap H_c$ where H_c is the hyperplane $\sum_{i=1}^{k} x_i = c$ This is a convex set, it suffices to show $P_{\alpha,\beta,\gamma}(c)$ is log-concave on this set. This is because taking marginals of log-concave functions preserves log-concavity [6].

Lemma 2. *$P_{\alpha,\beta,\gamma}(x)$ is log-concave on the domain $C^K \cap H_c$.*

Proof. Since a product of log concave functions is log-concave, it suffices to prove log-concavity of each term separately. That is, we show x_i^{α}, $(1 - x_i)^{\beta}$ and $|x_i - x_j|^{\gamma}$ are log-concave. Indeed, it suffices to take the domain of integration to be $0 \leq x_i \leq x_j \leq 1$ for $i < j$ by symmetry (introducing a factor of $n!$). Taking the log of x_i^{α} gives $\alpha \log(x_i)$ which is concave on $[0,1]$. Similarly, we can substitute $u = 1 - x_i$ in the second case, and $u = |x_i - x_j| = x_j - x_i$ in the third. In each case the domain is still within $[0,1]$. $\square$

Some Identities

We derive some general identities for the derivative of $y_{\alpha,\beta,\gamma}(c)$. Note first that

$$y_{\alpha,\beta,\gamma}(c) = y_{\beta,\alpha,\gamma}(k-c) \tag{5.3}$$

via the substitution $x_i \mapsto 1 - x_i$.

Consider the two sets $C^k \cap H_c$ and $C^k \cap H_{c+\epsilon}$. With the substitution $x_i \mapsto x_i + \frac{\epsilon}{k}$ we can get a bijection between the two sets, apart from some small section around the border.

Expanding using the definition of derivative:

$$\frac{y_{\alpha,\beta,\gamma}(c+\epsilon) - y_{\alpha,\beta,\gamma}(c)}{\epsilon}.$$

Which yields

Theorem 11.

$$y'_{k,\alpha,\beta,\gamma}(c) = \delta(\alpha) y_{k-1,\gamma,\beta,\gamma}(c) - \delta(\beta) y_{k-1,\alpha,\gamma,\gamma}(c-1) + \frac{1}{k} \int_{C^k \cap H_c} P_{k,\alpha,\beta,\gamma}(x) \left(\sum_i \frac{\alpha}{x_i} + \frac{\beta}{1-x_i} \right).$$

Here we use $\delta(\alpha)$ to denote the function that takes on the value of 1 if $\alpha = 0$ and 0 otherwise. If we instead consider the substitution $x_i \mapsto \left(1 + \frac{\epsilon}{c}\right) x_i$ which achieves a similar effect to the above we can again expand the derivative to get

Theorem 12.

$$c y'_{k,\alpha,\beta,\gamma}(c) = C_1 y_{k,\alpha,\beta,\gamma}(c) - k\delta(\beta) y_{k-1,\alpha,\gamma,\gamma}(c-1) + \beta \int_{C^k \cap H_c} \left(k - \sum_i \frac{1}{1-x_i} \right) P_{k,\alpha,\beta,\gamma}(x).$$

With $C_1 = \alpha k + \beta k + \gamma \binom{k}{2}$ being a constant in c.

Chapter 6

Conclusions

We have established determinant formulae for averages of secular coefficients. In the limit these random matrix theory averages are conjectured to behave like the number theoretic integrals over divisor sums. We also showed that the lower order terms of the random matrix theory averages have a similar behaviour to $\gamma_k(c)$. We end the thesis by raising some further questions for research.

Q1. We know that $\gamma_k(c)$ has an integral formulation as

$$\gamma_k(c) = \int_{[0,1]^k} \delta(\sum_i x_i - c) \prod_{1 \leq i < j \leq k} (x_i - x_j)^2 dx$$

and $\gamma_k(c)$ is the highest order term (N^{k^2-1}) in the asymptotics of $I_k^G(n, N)$ with $G = U(N)$. Do there exist integral formulations of the cases when $G = O(N)$ or $G = Sp(2N)$? What about the lower order terms?

Q2. We have seen that the divisor function $d_k(n)$ in number theory gives rise to the polynomials $\gamma_k(c)$ in random matrix theory through the conjecture due to Keating et al.[12]. Is there a natural arithmetic function that gives rise to Symplectic and Orthogonal $\gamma_k(c)$? We suspect that $\chi(n)d_k(n)$, for real quadratic characters χ and $d_k(n^2)$ gives rise to Symplectic behaviour.

Q3. Since we have determinant identities for $I_k^G(n, N)$, is it possible to derive asymptotics from analyzing them? We were able to understand some properties from a general analysis in the previous section but it's not clear if these determinant identities can give asymptotics for $\gamma_k^G(c)$ and lower order terms as $k \to \infty$.

Q4. In the paper of Keating et al. a lattice point calculation for $I_k^G(n,N)$ with $G = U(N)$ is given which is then used to derive some other properties. $I_k^{U(N)}(m;N)$ is equal to the count of lattice points $x = (x_i^{(j)}) \in \mathbb{Z}^{k^2}$ satisfying the set of relations

1. $0 \le x_i^{(j)} \le N$ for all $1 \le i,j \le k$
2. $x_1^{(k)} + x_2^{(k-1)} + \cdots + x_k^{(1)} = kN - m$, and
3. $x \in A_k$,

where A_k is the collection of $k \times k$ matrices whose entries satisfy the following system of inequalities,

$$\begin{array}{ccccccc}
x_1^{(1)} & \le & x_1^{(2)} & \le & \cdots & \le & x_1^{(k)} \\
\vee\!| & & \vee\!| & & & & \vee\!| \\
x_2^{(1)} & \le & x_2^{(2)} & \le & \cdots & \le & x_2^{(k)} \\
\vee\!| & & \vee\!| & & & & \vee\!| \\
\vdots & & \vdots & & \ddots & & \vdots \\
\vee\!| & & \vee\!| & & & & \vee\!| \\
x_k^{(1)} & \le & x_k^{(2)} & \le & \cdots & \le & x_k^{(k)}
\end{array}$$

Can natural lattice point counting analogues be given for $G = Sp(2N)$ or $O(N)$?

References

[1] George E Andrews. *Plane Partitions (I): The Mac Mahon Conjecture*. University of Wisconsin-Madison, Mathematics Research Center, 1975.

[2] E. C. Bailey, S. Bettin, G. Blower, J. B. Conrey, A. Prokhorov, M. O. Rubinstein, and N. C. Snaith. Mixed moments of characteristic polynomials of random unitary matrices. *Journal of Mathematical Physics*, 60(8):083509, Aug 2019.

[3] Estelle Basor, Fan Ge, and Michael O. Rubinstein. Some multidimensional integrals in number theory and connections with the painlevé v equation. *Journal of Mathematical Physics*, 59(9):091404, Sep 2018.

[4] Edward A Bender and Donald E Knuth. Enumeration of plane partitions. *Journal of Combinatorial Theory, Series A*, 13(1):40–54, 1972.

[5] D. Betea and M. Wheeler. Refined cauchy and littlewood identities, plane partitions and symmetry classes of alternating sign matrices. *Journal of Combinatorial Theory, Series A*, 137:126–165, Jan 2016.

[6] Herm Jan Brascamp and Elliott H Lieb. On extensions of the brunn-minkowski and prékopa-leindler theorems, including inequalities for log concave functions, and with an application to the diffusion equation. *Journal of Functional Analysis*, 22(4):366 – 389, 1976.

[7] David Bressoud. Elementary proofs of identities for schur functions and plane partitions. *The Ramanujan Journal*, 4, 03 2000.

[8] Daniel Bump and Alex Gamburd. On the averages of characteristic polynomials from classical groups. *Communications in Mathematical Physics*, 265(1):227–274, Feb 2006.

[9] J.B. Conrey, D.W. Farmer, J.P. Keating, M.O. Rubinstein, and N.C. Snaith. Autocorrelation of random matrix polynomials. *Communications in Mathematical Physics*, 237(3):365–395, Jun 2003.

[10] J.B. Conrey, D.W. Farmer, J.P. Keating, M.O. Rubinstein, and N.C. Snaith. Lower order terms in the full moment conjecture for the riemann zeta function. *Journal of Number Theory*, 128(6):1516 – 1554, 2008.

[11] Ofir Gorodetsky and Brad Rodgers. The variance of the number of sums of two squares in $\mathbb{F}_q[t]$ in short intervals, 2020.

[12] J. P. Keating, B. Rodgers, E. Roditty-Gershon, and Z. Rudnick. Sums of divisor functions in $\mathbb{F}_q[t]$ and matrix integrals. *Mathematische Zeitschrift*, 288(1-2):167–198, Mar 2017.

[13] Marvin Marcus. Determinants of sums. *The College Mathematics Journal*, 21(2):130–135, 1990.

[14] Robert A. Proctor. New symmetric plane partition identities from invariant theory work of de concini and procesi. *European Journal of Combinatorics*, 11(3):289 – 300, 1990.

[15] Kannan Soundararajan. Moments of the riemann zeta function. *Annals of Mathematics*, pages 981–993, 2009.

APPENDICES

Appendix A

Tables and Plots

A.1 Tables of $\gamma_k^G(c)$

Given a matrix group and integers k, j we give the polynomial defining $\gamma_k^G(c)$ on $c \in [j-1, j]$.

A.1.1 Unitary Group

(k, j)	$(k^2-1)!\gamma_k(c)$
$(2,1)$	c^3
$(2,2)$	$(2-c)^3$
$(3,1)$	c^8
$(3,2)$	$-2c^8 + 24c^7 252c^6 + 1512c^5 4830c^4 + 8568c^3 8484c^2 + 4392c 927$
$(3,3)$	$(c-3)^8$
$(4,1)$	c^{15}
$(4,2)$	$-3c^{15} + 60c^{14} - 1680c^{13} + 29120c^{12} - 294840c^{11} + 1873872c^{10} - 7927920c^9$ $+23268960\mathrm{c}^8 - 48674340c^7 + 73653580c^6 - 80912832c^5 + 63969360c^4$ -35497280 $\mathrm{c}^3 + 13131720c^2 - 2910240c + 292464$
$(4,3)$	$3c^{15} - 120c^{14} + 3360c^{13} - 58240c^{12} + 644280c^{11} - 4948944c^{10} + 28428400c^9$ -128700000 $\mathrm{c}^8 + 470398500c^7 - 1381480100c^6 + 3179336160c^5 - 5531176560c^4$ $+6950332480$ $\mathrm{c}^3 - 5910494520c^2 + 3031004640c - 705916304$
$(4,4)$	$(4-c)^{15}$

A.1.2 Symplectic Group

(k,j)	$\frac{(k+2)(k-1)}{2}!\gamma_k(c)$
$(2,1)$	c^2
$(2,2)$	$(c-2)^2$
$(3,1)$	c^5
$(3,2)$	$15c^4 - 90c^3 + 190c^2 - 165c + 51$
$(3,3)$	$(3-c)^5$
$(4,1)$	c^9
$(4,2)$	$c^9 - 36c^8 + 576c^7 - 3696c^6 + 12096c^5 - 22680c^4 + 25536c^3 - 17136c^2 + 6336c - 996$
$(4,3)$	$-c^9 + 1680c^6 - 20160c^5 + 106344c^4 - 307776c^3 + 508176c^2 - 449856c + 165916$
$(4,4)$	$(4-c)^9$

A.1.3 Orthogonal Group

The orthogonal group has a slightly different form than the unitary and symplectic groups for odd k. For odd k, $\gamma_k(c)$ is supported on $[0, k-1]$. Also, when $k=2$ the scaling factor is 1 in the below table.

(k,j)	$\frac{(k+1)(k-2)}{2}!\gamma_k(c)$
$(2,1)$	1
$(2,2)$	1
$(3,1)$	c^2
$(3,2)$	c^2
$(3,3)$	0
$(4,1)$	c^5
$(4,2)$	c^5
$(4,3)$	$(4-c)^5$
$(4,4)$	$(4-c)^5$
$(5,1)$	c^9
$(5,2)$	c^9
$(5,3)$	$-c^9 + 3360c^6 - 50400c^5 + 330624c^4 - 1182720c^3 + 2396160c^2 - 2580480c + 1146880$
$(5,4)$	$-c^9 + 3360c^6 - 50400c^5 + 330624c^4 - 1182720c^3 + 2396160c^2 - 2580480c + 1146880$
$(5,5)$	0

A.2 Plots of $\gamma_k^G(c)$

To illustrate the gaussian and highly smooth nature of $\gamma_k^G(c)$ we plot it below for $k = 4$.

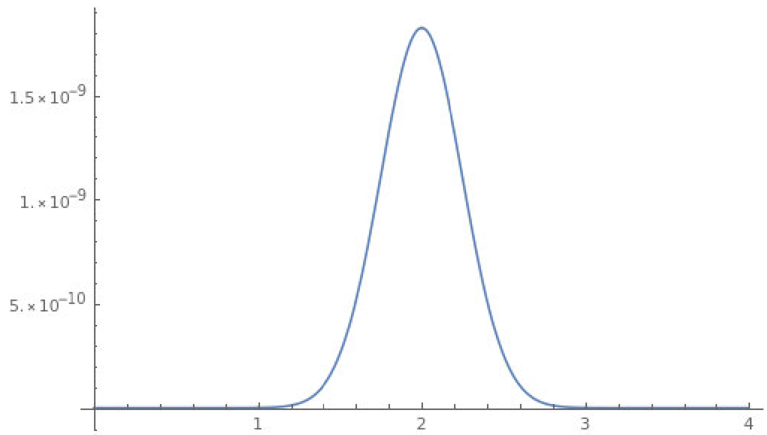


Figure A.1: $G = U(N), k = 4$

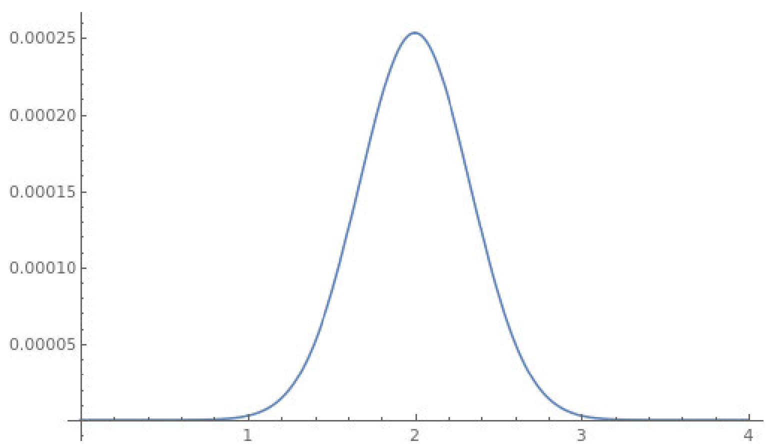


Figure A.2: $G = SP(2N), k = 4$

And for odd k in the case that $G = O(N)$:

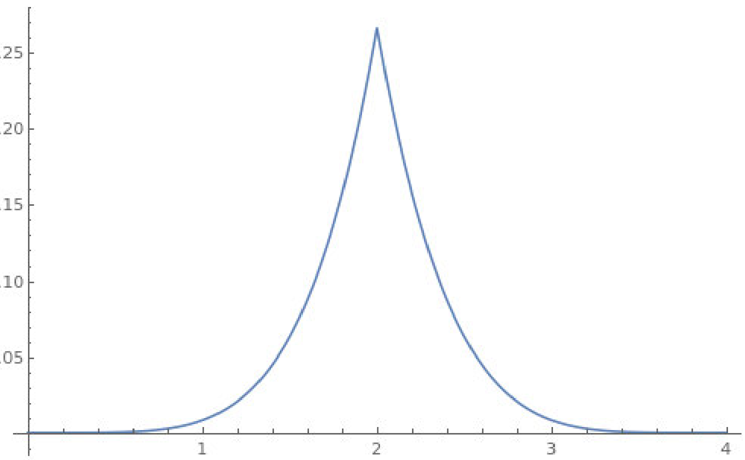


Figure A.3: $G = O(N), k = 4$

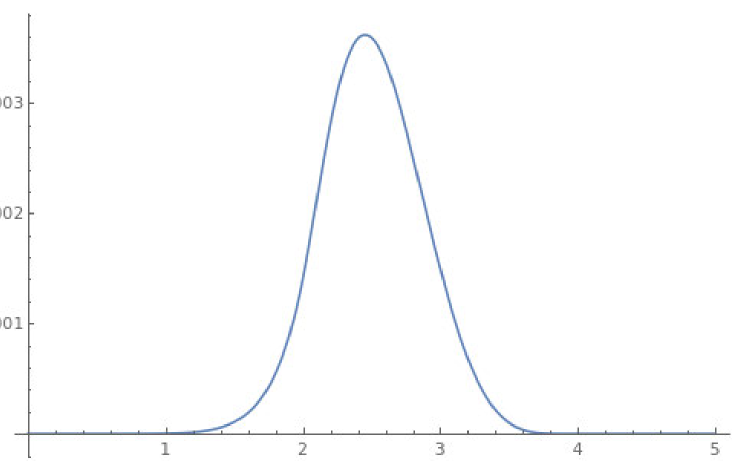


Figure A.4: $G = O(N), k = 5$

THIS IS **EXHIBIT "38"** TO
THE AFFIDAVIT OF **LAURENCE DAY**
SWORN BEFORE ME
THIS 9th DAY OF DECEMBER, 2021

Stephen Ayford

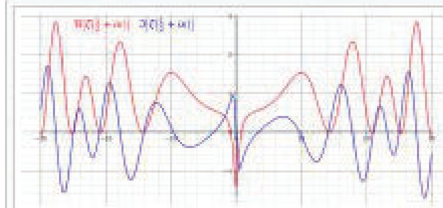
A COMMISSIONER ETC.

Riemann hypothesis

From Wikipedia, the free encyclopedia

For the musical term, see Riemannian theory.

In mathematics, the **Riemann hypothesis** is a conjecture that the Riemann zeta function has its zeros only at the negative even integers and complex numbers with real part $\frac{1}{2}$. Many consider it to be the most important unsolved problem in pure mathematics.[1] It is of great interest in number theory because it implies results about the distribution of prime numbers. It was proposed by Bernhard Riemann (1859), after whom it is named.



The real part (red) and imaginary part (blue) of the Riemann zeta function along the critical line Re(s) = 1/2. The first nontrivial zeros can be seen at Im(s) = ±14.135, ±21.022 and ±25.011.

The Riemann hypothesis and some of its generalizations, along with Goldbach's conjecture and the twin prime conjecture, make up Hilbert's eighth problem in David Hilbert's list of 23 unsolved problems; it is also one of the Clay Mathematics Institute's Millennium Prize Problems. The name is also used for some closely related analogues, such as the Riemann hypothesis for curves over finite fields.

Millennium Prize Problems

Birch and Swinnerton-Dyer conjecture
Hodge conjecture
Navier–Stokes existence and smoothness
P versus NP problem
Poincaré conjecture (solved)
Riemann hypothesis
Yang–Mills existence and mass gap

V · T · E

The Riemann zeta function $\zeta(s)$ is a function whose argument s may be any complex number other than 1, and whose values are also complex. It has zeros at the negative even integers; that is, $\zeta(s) = 0$ when s is one of −2, −4, −6, ... These are called its *trivial zeros*. However, the negative even integers are not the only values for which the zeta function is zero. The other ones are called *nontrivial zeros*. The Riemann hypothesis is concerned with the locations of these nontrivial zeros, and states that:

> The real part of every nontrivial zero of the Riemann zeta function is $\frac{1}{2}$.

Thus, if the hypothesis is correct, all the nontrivial zeros lie on the critical line consisting of the complex numbers $\frac{1}{2} + it$, where t is a real number and i is the imaginary unit.

THIS IS **EXHIBIT "39"** TO
THE AFFIDAVIT OF **LAURENCE DAY**
SWORN BEFORE ME
THIS 9th DAY OF DECEMBER, 2021

Stephen Ayford

A COMMISSIONER ETC.

Testing Zeros Of The Riemann Hypothesis [closed]

Asked 5 years, 2 months ago Active 5 years, 2 months ago Viewed 1k times

4

Closed. This question needs details or clarity. It is not currently accepting answers.

Want to improve this question? Add details and clarify the problem by editing this post.
Closed 5 years ago.

Improve this question

I was on Mathworld some time ago when I read this from http://mathworld.wolfram.com/RiemannHypothesis.html:

The Riemann hypothesis was computationally tested and found to be true for the first 200000001 zeros by Brent et al. (1982), covering zeros sigma+it in the region 0 < t < 81702130.19.

My question is: How can you be sure that you haven't missed any zeros? It seems to me that it is impossible because for any fixed t one would have to check all real sigma values between 0 and 1. And even if there was some way to do that one would still need to test all real values of t between 0 and 81702130.19. Do they have a list of "candidate zeros" that they would just try out?

Thanks in advance.

number-theory computer-science riemann-zeta riemann-hypothesis experimental-mathematics

Share Cite Follow

asked Aug 25 '16 at 22:42
mtheorylord
4,342 12 37

What are "the first" so and so zeros?? From what do you, or they, begin to count? – DonAntonio Aug 25 '16 at 22:44

You'll have to ask them. I don't know the answer, just the link. – mtheorylord Aug 25 '16 at 22:47

Linked

11 More elegant $\zeta(s)$ zeros counting function than $N(T)$

0 Is this plot of the argument of the Riemann zeta function around ZetaZero(127) correct?

2 How to prove a numerically calculated Riemann zero is exactly zero exactly on the line?

2 What's the best way to compute the zeros of functions of one complex variable?

2 About the number of zeros of the zeta function?

1 Numerical treatment of Riemann hypothesis?

2 Does this contour integral actually count

THIS IS **EXHIBIT "40"** TO
THE AFFIDAVIT OF **LAURENCE DAY**
SWORN BEFORE ME
THIS 9th DAY OF DECEMBER, 2021

Stephen Ayford

A COMMISSIONER ETC.

User talk:Mtheorylord

From Wikipedia, the free encyclopedia

This is an old revision of this page, as edited by Mtheorylord (talk | contribs) at 00:23, 17 June 2016 (*←Created page with 'Man I'm a good contributor. I am an expert in mathematics and theoretical physics. I believe in posting information about papers authors wrote on their wiki page...'*). The present address (URL) is a permanent link to this revision, which may differ significantly from the current revision.

(diff) ← Previous revision | Latest revision (diff) | Newer revision → (diff)

Man I'm a good contributor. I am an expert in mathematics and theoretical physics. I believe in posting information about papers authors wrote on their wiki page as well as where to find them. Thanks for your time.

THIS IS **EXHIBIT "41"** TO
THE AFFIDAVIT OF **LAURENCE DAY**
SWORN BEFORE ME
THIS 9th DAY OF DECEMBER, 2021

A COMMISSIONER ETC.

Alice Chu

[redacted]

[redacted]

[redacted]

From: Andrew Lin <alin@pcrfirm.com>
Sent: Wednesday, October 27, 2021 11:40 AM
To: Gottlieb, Jason <jgottlieb@morrisoncohen.com>
Cc: Bill Richmond <brichmond@pcrfirm.com>
Subject: RE: Return of funds

CAUTION: External sender. Verify before continuing.

Jason,

We dispute your characterization that those two statements are the same; the terms "return," "funds," and "money" result in a loaded question.

To speed things along, my client currently has no plans to send ERC20 tokens to an address of your choosing.

Best,
Andrew

From: Gottlieb, Jason <jgottlieb@morrisoncohen.com>
Sent: Wednesday, October 27, 2021 8:55 AM
To: Andrew Lin <alin@pcrfirm.com>
Cc: Bill Richmond <brichmond@pcrfirm.com>
Subject: RE: Return of funds

CAUTION: External Sender.

Confirmed on the document hold.

On the return of funds, I'm sorry, what do you mean you don't have a response? Either he's planning to return the funds, in which case let's talk about how to do that, or he's not. "We do not have a response at this time" is the same as "not returning the funds."

Jason P. Gottlieb
Partner & Chair, White Collar and Regulatory Enforcement
T: 212.735.8837 | F: 917.522.9937
jgottlieb@morrisoncohen.com
vCard | Bio | LinkedIn

Morrison Cohen LLP
909 Third Avenue
27th Floor
New York, NY 10022
www.morrisoncohen.com

From: Andrew Lin <alin@pcrfirm.com>
Sent: Tuesday, October 26, 2021 4:35 PM
To: Gottlieb, Jason <jgottlieb@morrisoncohen.com>
Cc: Bill Richmond <brichmond@pcrfirm.com>
Subject: RE: Return of funds

CAUTION: External sender. Verify before continuing.

Jason,

In view of the pending criminal investigation you informed us of, we do not have a response at this time.

I will pass your document hold notice on to him and would request the same from your clients.

Best,
Andrew

From: Gottlieb, Jason <jgottlieb@morrisoncohen.com>
Sent: Tuesday, October 26, 2021 3:25 PM
To: Andrew Lin <alin@pcrfirm.com>
Cc: Bill Richmond <brichmond@pcrfirm.com>
Subject: RE: Return of funds

CAUTION: External Sender.

Andrew, following up on my email from yesterday. Is your client going to return the money?

I also wanted to say: please instruct your client to preserve, and not delete, all evidence in connection with this matter, including code/scripts, communications, social media posts (including Twitter), Slack / Telegram / Whatsapp, etc.

Happy to talk live.

Jason

Jason P. Gottlieb
Partner & Chair, White Collar and Regulatory Enforcement
T: 212.735.8837 | F: 917.522.9937
jgottlieb@morrisoncohen.com
vCard | Bio | LinkedIn

Morrison Cohen LLP
909 Third Avenue
27th Floor
New York, NY 10022
www.morrisoncohen.com

From: Gottlieb, Jason
Sent: Monday, October 25, 2021 11:43 AM
To: 'Andrew Lin' <alin@pcrfirm.com>
Cc: Bill Richmond <brichmond@pcrfirm.com>
Subject: RE: Return of funds

Andrew, nice to meet you.

I represent Dr. Laurence Day and Dillon Kellar.

As you know, I have started discussions with law enforcement folks. I'm not at liberty to discuss the status of those discussions. But they are keenly interested, which makes sense.

I continue to think that your client's best play is to arrange for the return of the funds, which will take a lot of the pressure off. While I can't promise what law enforcement will do (I obviously don't control them), in my view (and experience), they'll be much less interested if all the money is returned.

So, to put the fine point on it: is your client going to return the money?

Happy to set up a call to discuss. Let me know what works.

Jason

Jason P. Gottlieb
Partner & Chair, White Collar and Regulatory Enforcement
T: 212.735.8837 | F: 917.522.9937
jgottlieb@morrisoncohen.com
vCard | Bio | LinkedIn

Morrison Cohen LLP
909 Third Avenue
27th Floor
New York, NY 10022
www.morrisoncohen.com

From: Andrew Lin <alin@pcrfirm.com>
Sent: Monday, October 25, 2021 9:10 AM
To: Gottlieb, Jason <jgottlieb@morrisoncohen.com>

Cc: Bill Richmond <brichmond@pcrfirm.com>
Subject: RE: Return of funds

CAUTION: External sender. Verify before continuing.

Mr. Gottlieb,

This firm represents Mr. Medjedovic. Please direct all correspondence to us in the future. In addition, your email states you "represent[] certain individual community members in the Indexed.Finance community," please also let us know who your clients are.

Best,
Andrew

Andrew Lin, *Senior Counsel*
PLATT CHEEMA RICHMOND PLLC
1201 N. Riverfront Blvd., Suite 150
Dallas, Texas 75207
214.559.2700 Main

---------- Forwarded message ---------
From: **Gottlieb, Jason** <jgottlieb@morrisoncohen.com>
Date: Sun, Oct 17, 2021 at 1:36 PM
Subject: Return of funds
[redacted]

Andean:

I am an attorney in New York, representing certain individual community members in the Indexed.Finance community.

I have been provided with overwhelming evidence – far more than the community has produced publicly – that you hacked the Indexed protocol, and stole approximately $16 million worth of assets – approximately $12 million of assets from the DEFI5 pool, and $4 million from the CC10 pool. This attack violated U.S. federal and state law, as well as Canadian laws. These assets are not yours. They are stolen property, belonging to the Indexed community.

I'm not your lawyer, but your best and only play here seems really obvious: if there is an easy way to return all of the funds (or even most of them, with some small amount as a "bug bounty"), you should take it.

The assets are still in the wallet into which they were placed immediately following the attack (https://etherscan.io/address/0xba5ed1488be60ba2facc6b66c6d6f0befba22ebe). That means you can still return them, and claim the mantle of a white hat hacker.

But as you know, the assets are all easily and immediately traceable. You will never be able to use them, in any way, without committing further crimes.

You're clearly a young, bright guy. Assuming your CV is truthful about your Putnam score, it's really impressive. Your math papers are quite strong for your age. You have a great future ahead of you.

Don't screw up your whole future over money you can't ever touch anyway.

If you don't return it, the community will be forced to go to the authorities, as well as your university. If you don't think the authorities can do anything, ask Mark Shin, the guy who took $10m of ICX in the ICON attack, and is now under criminal indictment. Waterloo isn't going to want this on their record either. You're jeopardizing your career, and even your freedom, for nothing. Don't do that – take the easy way out here and return the funds.

You – or your lawyer if you have one – should reach out to the Indexed community, or contact me, immediately, to discuss returning the stolen assets. My contact information is below.

Best regards,

Jason

Jason P. Gottlieb
Partner & Chair, White Collar and Regulatory Enforcement
T: 212.735.8837 | F: 917.522.9937

jgottlieb@morrisoncohen.com
vCard | Bio | LinkedIn

Morrison Cohen LLP

909 Third Avenue

27th Floor

New York, NY 10022

www.morrisoncohen.com

This transmittal and/or attachment (s) may be a confidential attorney-client communication or may otherwise be privileged or confidential. If you are not the intended recipient, you are hereby notified that you have received this transmittal in error; any review, dissemination, distribution or copying of this transmittal is strictly prohibited. If you have received this transmittal and/or attachment(s) in error, please notify us immediately by reply or by telephone (call us collect at 212-735-8600) and immediately delete this message and all of its attachments. Thank you. We take steps to remove metadata in attachments sent by email, and any remaining metadata should be presumed inadvertent and should not be viewed or used without our express permission. If you receive an attachment containing metadata, please notify the sender immediately and a replacement will be provided.

This email has been scanned for email related threats and delivered safely by Mimecast.
For more information please visit http://www.mimecast.com

This transmittal and/or attachment (s) may be a confidential attorney-client communication or may otherwise be privileged or confidential. If you are not the intended recipient, you are hereby notified that you have received this transmittal in error; any review, dissemination, distribution or copying of this transmittal is strictly prohibited. If you have received this transmittal and/or attachment(s) in error, please notify us immediately by reply or by telephone (call us collect at 212-735-8600) and immediately delete this message and all of its attachments. Thank you. We take steps to remove metadata in attachments sent by email, and any remaining metadata should be presumed inadvertent and should not be viewed or used without our express permission. If you receive an attachment containing metadata, please notify the sender immediately and a replacement will be provided.

This email has been scanned for email related threats and delivered safely by Mimecast.
For more information please visit http://www.mimecast.com

This transmittal and/or attachment (s) may be a confidential attorney-client communication or may otherwise be privileged or confidential. If you are not the intended recipient, you are hereby notified that you have received this transmittal in error; any review, dissemination, distribution or copying of this transmittal is strictly prohibited. If you have received this transmittal and/or attachment(s) in error, please notify us immediately by reply or by telephone (call us collect at 212-735-8600) and immediately delete this message and all of its attachments. Thank you. We take steps to remove metadata in attachments sent by email, and any remaining metadata should be presumed inadvertent and should not be viewed or used without our express permission. If you receive an attachment containing metadata, please notify the sender immediately and a replacement will be provided.

This email has been scanned for email related threats and delivered safely by Mimecast.
For more information please visit http://www.mimecast.com

THIS IS **EXHIBIT "42"** TO
THE AFFIDAVIT OF **LAURENCE DAY**
SWORN BEFORE ME
THIS 9th DAY OF DECEMBER, 2021

Stephen Aylward

A COMMISSIONER ETC.

Transcription of Voicemail Messages Left by Ed Medjedovic for Jason Gottlieb

Date: October 21, 2021 at 7:46:22 AM EDT

Subject: Message from Medjedovic E ([redacted])

"Hello Jason it's Andean Medjedovic's dad here. We had a conversation a few days ago and you asked me if I can talk with him. I did establish some contact with him but there's a lot going on and at that point when we spoke as a parent to parent. You gave me some information, however I find much more and now we can talk. So please give me a call back on this number and if you wanna talk; if not we have to proceed how we have to proceed. Thank you."

Date: October 21, 2021 at 8:41:26 AM EDT

"Jason I left you a message and I know you were early awake because I follow Twitter same as you let me be clear on this. Andy is a very smart guy, a very smart guy. It's not just it's my son but he's a very smart but he did what he do to prove the point. I don't wanna go more into Andean. We are definitely going to have a lawyer because obviously all those things online, all the comments that you even made there are very out of propositions. All the doxing. Everything that's going on. If this child — and he did before — lose his nerve, he may commit something you're all gonna regret. The money's gonna be gone, because he's the only one who knows how to get it, and you will not have anything, and I will not have my child. So, all those ultimatums what you make and everything else, just give me a call back, and let's see what we can do together, but he has to agree with this, and they have to agree with this. Please call. Bye."

THIS IS **EXHIBIT "43"** TO
THE AFFIDAVIT OF **LAURENCE DAY**
SWORN BEFORE ME
THIS 9th DAY OF DECEMBER, 2021

Stephen Aylward

A COMMISSIONER ETC.

Raymond Chabot Grant Thornton

Recovery and reorganization

Advisory

Raymond Chabot Administrateur Provisoire inc.

Restructuring expertise proposal

STOCKWOODS LLP
Barristers
Toronto-Dominion Centre
TD North Tower, Box 140
77 King Street West, Suite 4130
Toronto ON M5K 1H1

December, 2021

We Are Where You Are

and where you want to be

Grant Thornton's Canadian Restructuring Practice

RECOVERY AND REORGANIZATION

- Grant Thornton maintains dedicated recovery and reorganization professionals in offices in Vancouver, Calgary, Edmonton, Thunder Bay, Toronto, Markham, Ottawa, Montreal, Quebec City, Saint John, Fredericton, Charlottetown, and Halifax.
- In all, Grant Thornton has over 300 dedicated restructuring professionals across the country; this includes the Raymond Chabot Grant Thornton LLP practice in Quebec.
- The restructuring practice is integrated as a Canadian National practice and utilizes professionals and staff from across the country to administer National engagements or such engagements which require specific experience. Grant Thornton offers full restructuring services at competitive rates across Canada.

Our Line of Integrated Services

OUR SUBSIDIARIES

catallaxy AURAY Sourcing operio

ONE-STOP SHOP

Tax
- Canadian, U.S. and international taxes
- Commodity taxes
- R&D and innovation

ADVISORY SERVICES
- Recovery and reorganization
- Financial consulting
- Management consulting
- Digital and technology consulting
- Human resources consulting and recruiting
- Cybersecurity
- Financial performance: technological Solutions

ASSURANCE
- Audit
- Digital asset audit
- Review
- Compilation

ACCOUNTING
- Bookkeeping
- Online accounting
- Access to specialized services and a network of experts

A Unique Client Experience

A DISTINCTIVE SERVICE OFFERING

Availability and **proximity** of our professionals in over 105 offices in Quebec

Personalized support and **an integrated offering** to meet all business needs

Proactively providing **concrete solutions**

Competitive fees

Increased understanding of the various issues in different industries

Digital assets –
Recovery and Reorganization Experience

- Our team of professionals has significant experience dealing with digital assets (i.e. seizure, conversion, investigation) and appreciates it's challenges, complexities and nuances.
- An expertise developed in various cases, including Dominic Lacroix (Plexcoin). Appointed by the Superior Court at the request of the *Autorité des Marchés Financiers*, our team seized more than $ 7M of digital assets and converted them into fiat to the benefit of investors.

Recovery & Reorganization Department

VARIOUS ASSIGNMENTS, SUCH AS:

- Interim receiver;
- Receivership for secured creditors;
- Judicial receivership;
- Provisional administration;
- Commercial bankruptcy;
- Liquidator under federal or provincial law;
- Monitor under the *Companies' Creditors Arrangement Act*;
- Supervision of a corporation's affairs for the benefit of creditors;
- Survival of companies under an arrangement or proposal.

Background and Context

Situation That Led to Our Involvement

- Dispute among parties:
  - Creating insecurity among stakeholders
  - Status quo is unsustainable due to the nature of the assets involved
- Need for a receiver and/or the necessity to put in place protective/safety measures over digital assets
- Limited receivership sought, where the receiver’s only powers and duties would be to secure the assets by placing them in cold storage. Any power or responsibility to liquidate the assets, portfolio management is required.
- The method chosen by the applicants for the receiver to personally setup a secure cryptocurrency wallet using commercially available hardware wallet solution (Trezor) and stored securely by the receiver along with all seed and recovery information. Live assistance from an expert to be also provided at the time of asset transfer to ensure that the transfer process is thoroughly followed.

Advisory and Professional fees

Billing Rates

Partners	$500 – $600/h
Senior Managers	$300 – $450/h
Managers	$225 – $295/h
Analysts	$125 – $195/h

Estimated $400/h blended rate

Estimated Professional Fees*

	Time	Fees
Review of cold wallets (device) available and safety requirement	5-10 hours	$2,000 - $4,000
Develop a protocol to assure safe transfer of digital assets on the cold wallets	10-15 hours	$4,000 - $6,000
Supervise the transfer of digital assets on cold wallets and confirm the transactions	4-8 hours	$1,600 – $3,200
Review, if needed, on transactions over the blockchain	TBD	TBD
Transportation and storage in a safety box (at a bank or any place chosen by parties)	TBD	TBD
Report to Court / Parties	1-2 hours	$ 400 – 800

Total range of circa $8,000 to $14,000

In addition to expenses

**Does not include expenses/disbursements*

Raymond Chabot Grant Thornton

Our Dedicated Team

Dedicated Team

Emmanuel Phaneuf, M.Sc., CIRP, LIT

Partner

Role in the project:

Project lead

As a member of the RCGT's Recovery and Reorganization group since 2000, **Emmanuel Phaneuf** has participated in the restructuring of many companies in several different sectors.

Indeed, Mr. Phaneuf has developed specific expertise in highly complex insolvencies, fraud and cases related to various industries. He also has solid international experience, having, among others, worked for Grant Thornton UK in London on several major cases.

Mr. Phaneuf has worked on a number of trusteeship and receivership assignments. Furthermore, he is the person in charge at Raymond Chabot Administrateur Provisoire inc. in the matter of the receivership of Dominic Lacroix associated with the Plexcoin ICO.

Mr Phaneuf holds a Master's degree in Finance from the Hautes Études Commerciales Montreal. He is also a Certified Insolvency and Restructuring Professional and he is a Licensed Insolvency Trustee. He is a well-renowned speaker and he is deeply involved in the educational program at Canadian Association of Insolvency and Restructuring Practitioner, having chaired the drafting committee for the CIRP National Insolvency Exam in 2010, 2011 & 2015 and seated on the oversight and the commercial practice committees. Mr. Phaneuf joined the CAIRP board of directors in 2019.

Raymond Chabot Grant Thornton

Dedicated Team

Louis Roy, CPA, CA

Partner - Audit and Blockchain services

Role in the project:
Expert

Louis Roy is a chartered professional accountant who has participated in audit engagements of various sizes and degrees of complexity. He has been in charge of several aspects of financial statement audits for large-sized clients which has served to develop his ability to implement efficient audit techniques and his leading-edge expertise in the field of computer-assisted audit techniques.

Louis has worked tirelessly to develop leading-edge audit methodologies in cryptocurrency mining and fund management. A leader in this field, he heads the initiatives of Raymond Chabot Grant Thornton and Catallaxy, its blockchain audit practice, in developing this pioneering transactional technology.

Raymond Chabot Grant Thornton

Dedicated Team

Roberto Pimentel, P.Eng, CBP

Principal Director, Software Engineering at Catallaxy | RCGT

Role in the project:

Expert

Roberto Pimentel is an active member of the Catallaxy expertise centre at Raymond Chabot Grant Thornton' Certification Team. He joined the team in 2018 and has provided technical leadership and management skills to engineer software tools and solutions to allow rigorous auditing digital assets.

Multidisciplinary and passionate about technology, Roberto began his career as an information technology entrepreneur, and has developed a solid expertise in software development engineering management, particularly in the fields of telecommunications, digital media and recently in finance, with well over 25 years of experience. Over the years, he has accumulated hundreds of software product and service deliveries on a wide range of platforms and has been replied upon to perform numerous technical due diligence analysis of software systems part of M&A activities. Recognized for his leadership by his exemplarity and his great ability to listen, he is praised by his peers as a mediator par excellence to balance technical constraints and commercial requirements.

Raymond Chabot Grant Thornton

Dedicated Team

Vincent Cloutier

Distributed and Cryptographic Systems Architect

Role in the project:

Expert

Raymond Chabot Grant Thornton

As a long-time Ethereum developer, Vincent Cloutier manages blockchain nodes and helps develop blockchain integrations in our products. He also works on the operational side of our distributed cloud infrastructure.

Previously at Catallaxy, Mr Cloutier has worked on extensions to the OpenTimestamps protocol, a set of operations for creating provable timestamps, and later independently verifying them, in order to prove that some data existed prior to a specific point in time. Programming has been a life-long passion of his. He started with Python when he was 7 (before learning English), and has not stopped since.

He loves working with leading-edge technology and helping to make it available to everyone. He created an open source, peer-to-peer photo sharing system with undetectable pictures called ipfs.pics. The project very rapidly achieved 1k stars on GitHub and effectively launched his professional career.

Dedicated Team

Genvìève Pagé
CPA, CA, CIRP, LIT

Lead Senior Manager

Role in the project:
Project management

Raymond Chabot Grant Thornton

Geneviève Pagé has over 19 years of experience in the Recovery and Reorganization Group. Her recent assignments include developing and monitoring the implementation of restructuring and/liquidation plans under the *Bankruptcy and Insolvency Act* and winding up of companies under the *Canada Business Corporations Act* and the *Business Corporations Act* (Quebec). Among others, she has been involved in the technology development, public sector employee unions, estates, manufacturing and bio-pharmaceutical sectors.

Mrs. Pagé's main strengths are her discipline, adaptability, productivity in high-stress situations, communication skills and team leadership abilities.

We offer our clients the quality services of an international organization with a human, personal approach in line with your needs and situation.

EMMANUEL PHANEUF,
M.SC., CIRP, LIT

Partner
+1 514 393-4826
Phaneuf.emmanuel@rcgt.com

Raymond Chabot
Grant Thornton

rcgt.com

THIS IS **EXHIBIT "44"** TO
THE AFFIDAVIT OF **LAURENCE DAY**
SWORN BEFORE ME
THIS 9th DAY OF DECEMBER, 2021

Stephen Cyford

A COMMISSIONER ETC.

ANDEAN E. MEDJEDOVIC

[redacted]

UNIVERSITY OF WATERLOO - Completed Graduate Courses

Model Theory and Set Theory *(PMATH433)*
Taught by: Rahim Moosa
Textbook: Instructor Notes
Topics Covered: Model theory: the semantics of first order logic including the compactness theorem and its consequences, elementary embeddings and equivalence, the theory of definable sets and types, quantifier elimination, and omega-stability. Set theory: well-orderings, ordinals, cardinals, Zermelo-Fraenkel axioms, axiom of choice, informal discussion of classes and independence results

Representation Theory of Finite Groups *(PMATH445)*
Taught by: Wentang Kuo
Textbook: Serre, Linear Reps. of Fin. Groups
Topics Covered: Irreducible representations, tensor products of representations. Character theory. Representations as modules over the group ring, Artin-Wedderburn structure theorem for semisimple rings. Induced representations, Frobenius reciprocity, Mackey's irreducibility criterion

The Geometry of Numbers *(PMATH940)*
Taught by: Cameron Stewart
Textbook: Conway-Sloane, Sphere packings, Lattices and Groups
Topics Covered: Minkowski's Theorem, L^3 Algorithms, Lattices, Leech and E_8 lattice, Modular forms, Sphere packing

Tensor Products *(PMATH950)*
Taught by: Vern Paulsen
Textbook: Instructors Notes, Recent Papers
Topics Covered: Tensor products of Banach spaces, Operator spaces and systems, contractive and unital maps, Pisier's theory of similarity, Grothendieck's theorems on the subject

Category Theory and Homological Algebra *(PMATH945)*
Taught by: Jason Bell
Textbook: Instructors Notes
Topics Covered: Categories, Yoneda's Lemma, Projective and Injective Modules, Mitchell's Embedding Theorem, Resolutions, Ext and Tor Functors

Algebraic Number Theory *(PMATH441)*
Taught by: David Mckinnon
Textbook: Lang, Algebraic Number Theory
Topics Covered: unique factorization, Dedekind domains, class numbers, Dirichlet's unit theorem, solutions of Diophantine equations

Algebraic Geometry *(PMATH764)*
Taught by: Matt Satriano
Textbook: Hartshorne
Topics Covered: Algebraic Curves, Hilbert's Nullstellensatz, Bezout's Theorem, Divisor Class Numbers

Diophantine Approximation *(PMATH940)*
Taught by: Cameron Stewart
Textbook: Instructors Notes
Topics Covered: Heights of Algebraic Numbers, Ostrowski's Theorem, Dirichlet's and Liouville's Theorem, Linear forms in Logarithms and Baker's Theorem on the subject with applications, Convergents, Minkowski's Convex Body Theorem, Linear forms in 2 Logarithms

Analytic Number Theory I *(PMATH440)*
Taught by: Mike Rubinstein
Textbook: Apostol, Intro. to Analytic NT
Topics Covered: Poisson Summation, Abel Summation, Prime Number Theorem, Dirichlet Characters and infinite primes in arithmetic progressions, properties of the Riemann zeta function

Analytic Number Theory II *(PMATH940)*
Taught by: Mike Rubinstein
Textbook: Apostol, Intro. to Analytic NT
Topics Covered: Gauss Sums, Hardy-Littlewood Circle Method, Moments of the Riemann zeta function, Waring's Problem, Partitions

Geometry of Manifolds *(PMATH465)*
Taught by: Stephen New
Textbook: Intro. to Smooth Manifolds, John Lee
Topics Covered: Point-Set Topology, Smooth Manifolds, Tangent Bundles, Vector Fields, de Rham Cohomology

Lebesgue Integration and Fourier Analysis *(PMATH450)*
Taught by: Stephen New
Textbook: Axler, Measure Integration and Real Analysis
Topics Covered: Lebesgue measure and Lebesgue integral, Dominated Convergence Theorem, Hilbert and L_p Spaces, Theorems on the convergence of Fourier series

Introduction to Lie Groups and Lie Algebras *(PMATH863)*
Taught by: Stephen New
Textbook: Daniel Bump, Lie Groups
Topics Covered: Matrix Lie Groups and their associated Lie algebras, Fundamental Groups, Representation of Lie Groups, Maximal Tori, Root Systems and Weights

Functional Analysis *(PMATH453)*
Taught by: Nico Spronk
Textbook: Conway, Functional Analysis
Topics Covered: Banach and Hilbert Spaces, Hahn-Banach Theorem, Banach-Steinhaus Theorem,

Banach-Alaoglu Theorem, Goldstine's Theorem, Compact Operators and Spectral Theorem

Semidefinite Optimization *(CO471)*
Taught by: Steve Vavasis
Textbook: Conforti et al., Integer Programming
Topics Covered: Optimization over convex sets described as the intersections of the set of symmetric, positive semidefinite matrices with affine spaces. Formulations of problems from combinatorial optimization, graph theory, number theory, probability and statistics, engineering design and control theory. Theoretical and practical consequences of these formulations. Duality theory and algorithms

UNIVERSITY OF WATERLOO - Future Graduate Courses (by the time I graduate)

Intro. to Commutative Algebra *(PMATH446)*

Algebraic Topology *(PMATH467)*

Rings and Their Applications *(PMATH945)*

Symplectic Geometry *(PMATH965)*

Geometric Invariance Theory, Moduli Spaces *(PMATH965)*

Harmonic Analysis *(PMATH833)*

Fractal Geometry *(PMATH950)*

Elements of Random Matrix Theory *(PMATH990)*

Court File No.

ONTARIO
SUPERIOR COURT OF JUSTICE

B E T W E E N:

DILLON KELLAR and LAURENCE DAY

Plaintiffs

and

ANDEAN MEDJEDOVIC

Defendant

AFFIDAVIT OF ADAM AVENIR

I, Adam Avenir, of the City of Richland, in the County of Benton, in the State of Washington, in the United States of America, MAKE OATH AND SAY:

1. I am one of the co-founders of Code Arena[1] and am currently involved in running Code Arena's day-to-day operations. As such, I have knowledge of the matters contained in this Affidavit. Where my knowledge is based on information and belief, I indicate the source of my information and I believe it to be true.

Personal Background

2. In 2001, I graduated from Washington State University with a Bachelor's degree in Communications.

[1] Code Arena also goes by the name Code 423n4 and Code4rena.

3. In 2008, I founded a company called "&yet", and served as its CEO until 2015. "&yet" began as a web design and development company, and expanded into web application and open-source tool creation and development. The company also expanded into the field of security auditing and consulting, by creating a security auditing and consulting division called "Lift Security". As part of my role as CEO of "&yet", I was charged with the oversight, management and strategy of the "Lift Security" division. This division provided security auditing and consulting services to GitHub, which is a well-known online collaboration platform for software developers, as well as other customers.

4. In late 2020, I became interested in Decentralized Finance (**"DeFi"**). In early 2021, I helped co-found Code Arena. Currently, I am primarily responsible for running Code Arena's day-to-day operations.

5. My pseudonym is "sockdrawermoney". That is the username I use for Code Arena and Discord.

Code Arena

6. Code Arena is an online organization aimed at creating a community-driven approach to competitive security audits. Specifically, Code Arena organizes online competitions where auditors (users) referred to as "wardens" are challenged to "hunt exploits" (search for weaknesses) in the smart contracts of decentralized protocols, and prepare "reports" containing their findings (vectors of attack and general causes for instability or concern). Wardens are attracted to these competitions by "bounty pools" (USDC[2] and ETH[3] token rewards), which are funded by the

[2] USDC or USD Coin is a "digital stablecoin", which is a type of digital asset that is designed to maintain a stable value relative to a national currency, that is pegged to the United States dollar and runs on the Ethereum blockchain.
[3] ETH is the native token of the Ethereum blockchain.

sponsors of the competitions. The sponsors are, for instance, decentralized autonomous organizations (**“DAO”**) looking to have their projects reviewed, audited and analyzed. The wardens’ reports are evaluated by judges, who then allocate a portion of the token rewards to those who had the best performances. The results of the competitions are posted on Code Arena’s website on a leaderboard and in the Code Arena Discord chat.

7. For users to become wardens and participate in Code Arena’s competitions, they must register on our website by creating a “handle” (username). They also have the option of linking an “avatar” (a digital image) and a Twitter account to their username.

8. The username that a user creates allows Code Arena to identify the winners of the competitions, allocate funds to them, tag them in the Discord chat, and list them on the leaderboard. I have attached the warden registration instructions as **Exhibit 1**.

9. Many members of the Code Arena community consider themselves to be “white-hat hackers” (ethical security hackers whose work involves identifying security vulnerabilities and exploits in software and computer systems for the benefit of DeFi organizations and platforms).

Learning About the Attack on Indexed Finance’s Index Pools

10. Prior to October 14, 2021, I had heard of Indexed Finance by general reputation and I had joined the Indexed Finance Discord chats because I admired the work they were doing. In the past, I have held Indexed Finance tokens, but I did not hold any Indexed Finance tokens at the time of the Attack.

11. Sometime in the evening on October 14, 2021, I became aware of an attack on Indexed Finance’s index pools by an unknown attacker (the **“Attack”**). I learned of the Attack by reading

tweets about it on Twitter. I saw the tweets about the Attack on Twitter because I am generally connected to the DeFi community on that social media platform.

12. The next morning, on October 15, 2021, I received a message on Discord from a user with the pseudonym “hickuphh3”. This user was known to me through Code Arena, as he actively participates in Code Arena’s auditing competitions as a warden.

13. The message from “hickuphh3” included a link to a tweet by a Twitter account named @litocoen, who had reposted an update from Indexed Finance about the Attack. This update contained information about a possible suspect, whose pseudonym was “BogHolder”. At first, I was not sure why “hickuphh3” was sending me this tweet. I then recalled that a Discord user with the names “BogHolder” and “UmbralUpsilon” was associated with a Code Arena warden who had participated in Code Arena competitions using the warden name “tensors” (I discuss this in the paragraphs below). I have attached a copy of the Discord messages exchanged between myself as “sockdrawermoney” and “hickuphh3” as **Exhibit 2**.

Pre-Attack interactions with “UmbralUpsilon”/“tensors”/“BogHolder”

14. Specifically, I was able to connect “UmbralUpsilon” and “BogHolder” to the Code Arena warden “tensors” because I recalled having had a conversation with the Discord user “UmbralUpsilon” about a month before the attack. I looked through my Discord chat history and found a record of this conversation, which was dated September 2, 2021. By the time I reviewed my Discord chat history, “UmbralUpsilon” had changed his Discord username to “BogHolder”, and so the Discord chat had updated itself to appear as though I had a conversation with “BogHolder”. While I do not know exactly when “UmbralUpsilon” changed his username to

"BogHolder", I recalled from looking at our Discord chat history that the user was previously named "UmbralUpsilon".

15. My Discord conversation with "UmbralUpsilon" was about how he had successfully competed in one of Code Arena's competitions called the "PoolTogether contest", which had run from July 28 to July 31, 2021. Code Arena had updated its leaderboard to identify the winners, but "UmbralUpsilon" had not yet received his token rewards payout and so he had reached out to me about the status of the payout. I had asked him what his Code Arena warden name was, and he responded that it was "tensors". I have attached a copy of the Discord conversation between myself as "sockdrawermoney" and "UmbralUpsilon"/"tensors"/"BogHolder" as **Exhibit 3**.

16. I also noticed that the Discord user "UmbralUpsilon" had successfully participated in another Code Arena competition called the "Notional Code contest" as the warden "tensors", which had run from August 25 to September 8, 2021. "UmbralUpsilon" aka "tensors" placed fourth at the competition. On September 24, 2021, the Code Arena coordinator "itsmetechjay" posted the results of this contest on Discord, listing the Discord users that had successfully participated in the contest and tagging the warden "tensors" as the fourth-place winner. I remember this because I follow the results of the contest and I have a draft copy of the results that were shared internally amongst Code Arena organizers prior to them being posted. I have attached a copy of the draft Notional contest results listing the warden "tensors" as the fourth-place winner as **Exhibit 4**. The reason I do not have a copy of the final results posted on Discord identifying the fourth-place winner of the Notional contest is because when a user deletes their username, the Discord platform automatically updates all references to that name to reflect the changes made by that user. As such, when I went back to check the Notional contest results on Discord, I noticed that the fourth-place winner was now listed as "Deleted User" because he had deleted his usernames by

that point. I have attached a copy of the Notional contest results posted by “itsmetechjay” with the tag to “Deleted User” as **Exhibit 5**.

17. Moreover, while the Discord results of the Notional contest showed “Deleted User” as the fourth-place winner, Code Arena had posted a list of the wardens that had contributed reports for the Notional contest on its website and the user “tensors” was fourth on that list. That list, which was posted on October 1, 2021, is not subject to change and so “tensors” is still listed as the fourth-place winner. I have attached a copy of the list from the Code Arena website as **Exhibit 6**.

Post Attack communications with “tensors8”

18. On the morning of October 15, 2021, one of the other Code Arena organizers, pseudonym “itsmetechjay”, sent a message to the group chat for Code Arena coordinators to notify us that someone had reached out to her on Discord to ask whether he could be added to the chat for Code Arena wardens and whether Code Arena could change the username we had for him on file. I have attached a copy of “itsmetechjay”’s messages to the Code Arena organizers as **Exhibit 7.** I had a hunch that this warden might be connected to “UmbralUpsilon”/“tensors”/“BogHolder” and so I asked “itsmetechjay” for a screenshot of her conversation with him. From this, I saw that this warden had named himself “tensors8”. I have attached a copy of a Discord chat between “itsmetechjay” and “tensors8” as **Exhibit 8**.

19. Shortly after my conversation with “itsmetechjay”, I decided to reach out to “tensors8” and ask him about the Attack. I sent him a message on Discord to ask whether he was involved in the Attack and if so, whether he was planning on returning the assets he took and claiming the white-hat bounty that Indexed Finance had offered (Indexed Finance had publicly offered the attacker a 10% bounty to the attacker, with the idea being to pretend that the Attack had been a friendly

"white-hat" security audit). "tensors8" replied that he was not involved in the Attack. I asked him if he was the same user as "tensors" and "BogHolder". He replied that he was not sure how those two users were related. I asked him if he had competed under the warden name "tensors" in the past. He replied "don't know" and asked me about Code Arena's policy on hackers being allowed to participate in its competitions.

20. At this point, I suspected that the usernames "tensors", "UmbralUpsilon", "BogHolder" and "tensors8" all belonged to the same person, and so I sent "tensors8" another message notifying him that I was aware of the evidence against "BogHolder" and explaining that Code Arena would likely not allow him to participate in competitions in the future. I have attached a copy of the Discord conversation between myself as "sockdrawermoney" and "tensors8" as **Exhibit 9**.

21. A few hours later, "tensors8" changed his name again, this time to "quasiCubism".

22. After seeing that "tensors8" had changed his name to "quasiCubism", I reached out again and asked if he was ok, because there was mounting evidence about his identity and I was concerned that he would do something drastic. He replied "dw ill be fine". I then asked if he had decided to keep the tokens that he took in the Attack. At this point, he dropped the pretence of ignorance and replied "indeed".

23. I thought I might be able to convince him to return the tokens and collect the white-hat bounty that Indexed Finance offered, by explaining that doing so would result in him becoming a notable white-hat hacker with talent to rival one of the most well-known white-hat hackers in the DeFi community, an individual known as "samczsun".

24. “quasiCubism” responded: “or how about notorious black hat skillz to rival samczun? this could be a real rivalry it makes more sense too black vs white instead of white vs white”. In contrast to white-hat hackers, “black-hat hackers” are malicious hackers that search for and exploit vulnerabilities in computer systems for their own gain.

25. I have attached a copy of the Discord conversation between myself as “sockdrawermoney” and “quasiCubism” as **Exhibit 10**.

Communications with Laurence Day and Dillon Kellar of Indexed Finance

26. Sometime in the evening on October 15, 2021, Laurence Day reached out to me on Discord to ask me if I had information on “BogHolder” aka “tensors”, who was the suspect in the Attack. This was the first time I had ever spoken to Laurence. I understand that he reached out to me because “hickuphh3” had separately contacted him and Dillon Kellar about “BogHolder”, and suggested that they contact someone at Code Arena.

27. Laurence added Dillon to our conversation. I gave them the information I had at the time, and sent them a screenshot of the conversation I had with “BogHolder”/“UmbralUpsilon” on September 2, 2021, where he confirmed he was the same user as “tensors”. I then kept Laurence and Dillon updated on my conversations with “BogHolder”, by sending them screenshots of my Discord chats with “tensors8” and “quasiCubism”. I have attached a copy of my Discord conversation with Laurence and Dillon as **Exhibit 11**.

28. I understand that Laurence and Dillon used this information in their investigation into the identity of the attacker.

29. I make this affidavit in support of a motion in this proceeding brought by Laurence and Dillon.

AFFIRMED by Adam Avenir at the City Richland, Washington, before me at the City of Toronto on December 6, 2021 in accordance with O. Reg. 431/20, Administering Oath or Declaration Remotely.

Commissioner for Taking Affidavits
(or as may be)

Stephen Aylward (LSO# 66556E)

ADAM AVENIR

THIS IS **EXHIBIT "1"** TO
THE AFFIDAVIT OF **ADAM AVENIR**
SWORN BEFORE ME
THIS 6th DAY OF DECEMBER, 2021

Stephen Aylward

A COMMISSIONER ETC.

Register as a warden

Registering as a warden allows you to be listed on our leaderboard. It's possible to do this step asynchronously from submitting a bug for a contest.

Fork this repo and create a PR:

1. Add a JSON file for yourself at _data/handles, and an avatar at _data/handles/avatars:

```
{
  "handle": "maurelian",
  "image": "./avatars/maurelian.jpg",
  "link": "https://twitter.com/maurelian_"
}
```

2. If you're registering a team, add the individual handles of the team members like so:

```
{
  "image": "",
  "handle": "pocotiempo",
  "members": ["maurelian", "0xRajeev", "mariano"]
}
```

The handle your issues are submitted under will determine where awards will go, so it's possible to be part of a team on some contests and *also* compete as an individual on other contests.

THIS IS **EXHIBIT "2"** TO
THE AFFIDAVIT OF **ADAM AVENIR**
SWORN BEFORE ME
THIS 6th DAY OF DECEMBER, 2021

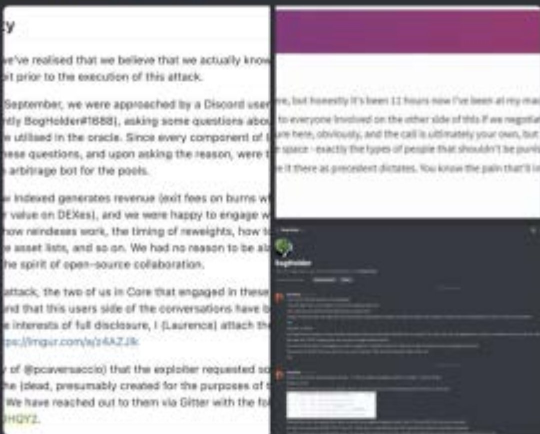
Stephen Aylward

A COMMISSIONER ETC.

hickuphh3 Today at 8:50 AM
https://twitter.com/litocoen/status/1449037095360770052?s=20

O.o not sure if u guys saw this

> **lito.eth (@litocoen)**
>
> update: turns out @laurence_e_day and @d1ll0nk engaged with an individual who is very likely the hacker
> https://t.co/1u6DJP1OuS



y

e've realised that we believe that we actually know
t prior to the execution of this attack.

September, we were approached by a Discord user
tly BogHolder#1888), asking some questions abou
e utilised in the oracle. Since every component of
ese questions, and upon asking the reason, were t
arbitrage bot for the pools.

Indexed generates revenue (exit fees on burns w
value on DEXes), and we were happy to engage w
ow reindexes work, the timing of reweights, how t
e asset lists, and so on. We had no reason to be al
he spirit of open-source collaboration.

attack, the two of us in Core that engaged in these
nd that this users side of the conversations have b
e interests of full disclosure, I (Laurence) attach th
ps://imgur.com/a/z4AZJlk

of @pcaversaccio) that the exploiter requested so
e (dead, presumably created for the purposes of t
We have reached out to them via Gitter with the fo
HQY2.

> Twitter • Today at 8:38 AM

sockdrawermoney Today at 8:55 AM
sorry, I'm multitasking at the moment and only aware of the ndx hack on a cursory level. what's the implication?

oh shit, I see. the warden `tensors` is now `bogholder`

hickuphh3 Today at 8:57 AM
Yeah... It's a serious allegation

THIS IS **EXHIBIT "3"** TO
THE AFFIDAVIT OF **ADAM AVENIR**
SWORN BEFORE ME
THIS 6th DAY OF DECEMBER, 2021

A COMMISSIONER ETC.

BogHolder 09/02/2021

hey

I see the leaderboard is updated, but I haven't gotten any payout

I guess think this is for the PoolTogether contest?

sockdrawermoney 09/02/2021

Hm! Ok. What is your handle?

BogHolder 09/02/2021

tensors

sockdrawermoney 09/02/2021

I'll check with ninek and get back to you. Could be queued at the multisig

BogHolder 09/02/2021

ok, thanks

THIS IS **EXHIBIT "4"** TO
THE AFFIDAVIT OF **ADAM AVENIR**
SWORN BEFORE ME
THIS 6th DAY OF DECEMBER, 2021

Stephen Gifford

A COMMISSIONER ETC.

$86,001.08 USDC » cmichel
$26,838.42 USDC » leastwood
$10,494.54 USDC » pauliax
$8,405.33 USDC » tensors
$5,709.62 USDC » gpersoon
$5,609.01 USDC » Omik
$4,249.68 USDC » JMukesh
$1,875.00 USDC » hrkrshnn
$408.66 USDC » a_delamo
$408.66 USDC » defsec
$0.00 USDC » ad3sh_

THIS IS **EXHIBIT "5"** TO
THE AFFIDAVIT OF **ADAM AVENIR**
SWORN BEFORE ME
THIS 6th DAY OF DECEMBER, 2021

A COMMISSIONER ETC.

👩🏽💻 Jay | C4 09/24/2021

🤑 🎉 Here are awards for **Notional**.... 🙌

$86,001.08 USDC » @cmichel
$26,838.42 USDC » @0xleastwood
$10,494.54 USDC » @Thunder
$8,405.33 USDC » @Deleted User
$5,709.62 USDC » @Gerard Persoon
$5,609.01 USDC » @Omik
$4,249.68 USDC » @JMukesh
$1,875.00 USDC » @hrkrshnn
$408.66 USDC » @a_delamo
$408.66 USDC » @DefSec

We will get those distributed on Polygon Monday. I'll be reaching out to you all shortly to verify you're good with us using your same address on Polygon.

🙏 10 🎉 12

THIS IS **EXHIBIT "6"** TO
THE AFFIDAVIT OF **ADAM AVENIR**
SWORN BEFORE ME
THIS 6th DAY OF DECEMBER, 2021

Stephen Aylward

A COMMISSIONER ETC.

WARDENS

11 Wardens contributed reports to the Notional code contest:

1. cmichel
2. leastwood
3. pauliax
4. tensors
5. gpersoon
6. Omik
7. Jmukesh
8. hrkrshnn
9. a_delamo
10. LSDan
11. ad3sh_

This contest was judged by ghoul.sol.

Final report assembled by moneylegobatman and ninek.

THIS IS **EXHIBIT "7"** TO
THE AFFIDAVIT OF **ADAM AVENIR**
SWORN BEFORE ME
THIS 6th DAY OF DECEMBER, 2021

Stephen Aylward

A COMMISSIONER ETC.

Jay | C4 10/15/2021

hey @eric (ninek) | C4:

> also, can I change the address you guys have on file for me?
> do you keep them all in a list or do you get it new from each contest submission?

do we have a process for changing warden payment addresses?

@Jay | C4 hey @eric (ninek) | C4: > also, can I change the address you

eric (ninek) | C4 10/15/2021

who's that from? cc @🧦 sockdrawer | C4

@eric (ninek) | C4 who's that from? cc @🧦 sockdrawer | C4

Jay | C4 10/15/2021

tensors aka umbraupsilon

THIS IS **EXHIBIT “8”** TO
THE AFFIDAVIT OF **ADAM AVENIR**
SWORN BEFORE ME
THIS 6th DAY OF DECEMBER, 2021

Stephen Ayford

A COMMISSIONER ETC.

tensors8

This is the beginning of your direct message history with **@tensors8**.

C4 1 Mutual Server • **Remove Friend** **Block**

October 15, 2021

tensors8 Today at 11:40 AM
hey, can I be added to the wardens chat? I'm logging on with my other discord? (edited)

itsmetechjay | C4 Today at 11:41 AM
hey there! gave you the wardens role so you should see it now - let me know if you don't.

tensors8 Today at 11:41 AM
thanks

are the badger funds released yet?

itsmetechjay | C4 Today at 11:43 AM
the usdc's were sent. I believe they are getting the tokens distributed soon.

tensors8 Today at 11:44 AM
ok sweet

also, can I change the address you guys have on file for me?
do you keep them all in a list or do you get it new from each contest submission?

THIS IS **EXHIBIT "9"** TO
THE AFFIDAVIT OF **ADAM AVENIR**
SWORN BEFORE ME
THIS 6th DAY OF DECEMBER, 2021

Stephen Aylward

A COMMISSIONER ETC.

sockdrawermoney Today at 10:11 AM
hey!
Were you involved in the ndx hack? if so, do you intend to return the funds and claim the white hat bounty they offered?

tensors8 Today at 10:12 AM
no, I was not involved, must be a confusion

sockdrawermoney Today at 10:12 AM
are you tensors / aka bogholder?

tensors8 Today at 10:13 AM
not sure how those two are related

sockdrawermoney Today at 10:14 AM
have you competed under the warden name 'tensors' in the past?
(I'm not making any accusation here btw. but there is an allegation against bogholder, who previously used the warden handle 'tensors' and if that's you, I'd like to talk about it)

tensors8 Today at 10:17 AM
dont know
whats the c4 policy on hackers competing on contests?

sockdrawermoney Today at 10:18 AM
this situation is requiring us to develop one—which is why I'd like to talk to you if that's you 🙂

tensors8 Today at 10:19 AM
well, its not me,
hough do let me know if c4 comes up with some policy ideas
*though

@tensors8 dont know
sockdrawermoney Today at 10:21 AM
what was the 'don't know' in response to?
there's too many coincidences in play... I can imagine that this is all pretty stressful for you.
certainly if it *was* you and you made yourself the 'antihero' as indexed finance calls it and returned the funds in exchange for their generous white hat bounty offer, you wouldn't be black hat here anymore.

white hat bounty offer, you wouldn't be black hat here anymore.

tensors8 Today at 10:32 AM

anyway, I would like to keep submitting stuff for c4, if you guys are cool with that

it wasn't me though, so it should be no problem

sockdrawermoney Today at 10:35 AM

I want to be clear that I'm not trying to get you to confess to something.

I think you've been a great contributor to C4

and I'd like to see C4 make you pretty dang rich and celebrated for your work

tensors8 Today at 10:38 AM

thank you, I like you guys at C4 too. I want to keep contributing and help it grow

sockdrawermoney Today at 10:51 AM

if there's a significant amount of mounting evidence that continues to point toward bogholder, I don't think we'll be able to allow tensors to continue to compete and be part of the community. another warden already reached out to me linking tensors and bogholder, and some of your actions today add to coincidental evidence supporting that.

I'm just going to speak very personally here. I've had my own share of questionable decisions in my life and I'm not gonna judge bogholder if the allegations are true. At the same time, if all the evidence points to bogholder and we continue to allow this person to compete, it jeopardizes the community's ability to trust C4. It puts us in a very hard position because this kind of approach runs counter to our purpose as an org.

If, however, the funds were returned today and the white hat bounty claimed, I expect we'd gladly continue to allow the whitehat bogholder / tensors to compete.

THIS IS **EXHIBIT "10"** TO
THE AFFIDAVIT OF **ADAM AVENIR**
SWORN BEFORE ME
THIS 6th DAY OF DECEMBER, 2021

A COMMISSIONER ETC.

sockdrawermoney Today at 5:45 PM
Hey just reaching out cos I am worried about you.

quasiCubism Today at 8:02 PM
dw ill be fine

sockdrawermoney Today at 8:07 PM
Did you decide to keep it?

quasiCubism Today at 8:08 PM
indeed

sockdrawermoney Today at 8:09 PM
What made you decide to do that?

quasiCubism Today at 8:09 PM
why would I give away 90% of my portfolio to a protocol?

doesn't make a lot of sense

sockdrawermoney Today at 8:16 PM

you know if you gave it back you could still make a lot of money as a real hero and build a pretty great reputation as a pretty notorious white hat with skills to rival samczsun

quasiCubism Today at 8:16 PM

or how about notorious black hat skillz to rival samczsun? this could be a real rivalry

it makes more sense too black vs white instead of white vs white

THIS IS **EXHIBIT "11"** TO
THE AFFIDAVIT OF **ADAM AVENIR**
SWORN BEFORE ME
THIS 6th DAY OF DECEMBER, 2021

Stephen Cyfrad

A COMMISSIONER ETC.

sockdrawermoney AKA sockdrawer | C4

sockdrawermoney

This is the beginning of your direct message history with @sockdrawermoney.

6 mutual servers • Remove friend Block

Saturday, 16 October 2021 02:39

16 October 2021

Norsefire 16/10/2021

Hey sockdrawer

Laurence Day here from Indexed Finance

Do you have a minute to have a word?

It's regarding the recent exploit we've suffered, and we've got reason to believe that one of the C4 wardens is responsible

sockdrawermoney 16/10/2021

Hi Laurence. Feel awful for y'all

Norsefire 16/10/2021

Heh thanks man

sockdrawermoney 16/10/2021

Yes, I did see this.

sockdrawermoney 16/10/2021
feel free to give it to hickup

Oh wait

I have one more screenshot

Norsefire 16/10/2021
Hm?

Saturday, 16 October 2021 03:50

sockdrawermoney 16/10/2021

BogHolder 09/02/2021
hey
I see the leaderboard is updated, but I haven't gotten any payout
I guess think this is for the PoolTogether contest?

sockdrawermoney 09/02/2021
Hm! Ok. What is your handle?

BogHolder 09/02/2021
tensors

sockdrawermoney 09/02/2021
I'll check with ninek and get back to you. Could be queued at the multisig

BogHolder 09/02/2021
ok, thanks

UmbraUpsilon » BogHolder = warden `tensors`

so this is a screenshot from a month ago connecting BogHolder to being tensors (in addition to us having his eth address)

not a huge deal but gives the lie pretty heavily to him saying the two handles aren't connected

Norsefire 16/10/2021
aye indeed

sockdrawermoney 16/10/2021
He did not / has not replied to me yet btw. I will let you know if he does

Court File No./N° du dossier du greffe: CV-21-00673984-00CP

Electronically issued
Délivré par voie électronique : 17-Dec-2021
Toronto

Court File No.

ONTARIO
SUPERIOR COURT OF JUSTICE

B E T W E E N:

(Court Seal)

DILLON KELLAR and LAURENCE DAY

Plaintiffs

and

ANDEAN MEDJEDOVIC

Defendant

Proceeding under the *Class Proceedings Act, 1992,* SO 1992, c 6

NOTICE OF ACTION

TO THE DEFENDANT

A LEGAL PROCEEDING HAS BEEN COMMENCED AGAINST YOU by the Plaintiffs. The claim made against you is set out in the following pages.

IF YOU WISH TO DEFEND THIS PROCEEDING, you or an Ontario lawyer acting for you must prepare a Statement of Defence in Form 18A prescribed by the *Rules of Civil Procedure*, serve it on the Plaintiff's lawyer or, where the Plaintiff does not have a lawyer, serve it on the Plaintiff, and file it, with proof of service in this court office, WITHIN TWENTY DAYS after this Statement of Claim is served on you, if you are served in Ontario.

If you are served in another province or territory of Canada or in the United States of America, the period for serving and filing your Statement of Defence is forty days. If you are served outside Canada and the United States of America, the period is sixty days.

Instead of serving and filing a Statement of Defence, you may serve and file a Notice of Intent to Defend in Form 18B prescribed by the *Rules of Civil Procedure*. This will entitle you to ten more days within which to serve and file your Statement of Defence.

IF YOU FAIL TO DEFEND THIS PROCEEDING, JUDGMENT MAY BE GIVEN AGAINST YOU IN YOUR ABSENCE AND WITHOUT FURTHER NOTICE TO YOU. IF YOU WISH TO DEFEND THIS PROCEEDING BUT ARE UNABLE TO PAY LEGAL FEES, LEGAL AID MAY BE AVAILABLE TO YOU BY CONTACTING A LOCAL LEGAL AID OFFICE.

IF YOU PAY THE PLAINTIFF'S CLAIM, and $100,000 for costs, within the time for serving and filing your Statement of Defence you may move to have this proceeding dismissed by the Court. If you believe the amount claimed for costs is excessive, you may pay the Plaintiff's claim and $400 for costs and have the costs assessed by the Court.

TAKE NOTICE: THIS ACTION WILL AUTOMATICALLY BE DISMISSED if it has not been set down for trial or terminated by any means within five years after the action was commenced unless otherwise ordered by the court.

Date ____________________ Issued by ______________________________

Local Registrar

Address of court office: Superior Court of Justice
330 University Avenue, 9th Floor
Toronto ON M5G 1R7

TO: [redacted]

CLAIM

1. The plaintiffs claim:

(a) An order certifying this action as a class proceeding under s. 5(1) of the *Class Proceedings Act* and appointing the plaintiffs as representative plaintiffs for the Class (capitalized terms defined below);

(b) Damages in the amount of at least $16.5 million[1] as compensation for losses suffered by the direct holders of DEFI5 and CC10 tokens;

(c) Damages in an amount to be determined at trial, but at least in the amount of $10 million as compensation for losses suffered by the indirect holders of DEFI5 and CC10 tokens;

(d) An order rescinding and setting aside any contract(s) between the defendant and any Class members relating to the Attack;

(e) An order recognizing or imposing a constructive trust over the digital assets held in the Wallet controlled by the defendant;

(f) Punitive and exemplary damages;

(g) An interim and interlocutory *Mareva* order freezing the defendant's assets, including the digital assets held in the Wallet;

[1] All dollar values are in USD.

(h) An interim and interlocutory order for the preservation of the digital assets held in the Wallet;

(i) A representation order under r. 10.01 of the *Rules of Civil Procedure* appointing the plaintiffs as representatives of the Indexed Finance DAO (an unincorporated association);

(j) Prejudgment and postjudgment interest;

(k) The costs of this proceeding; and

(l) Such further and other relief as this Honourable Court may deem just.

Overview

2. On October 14, 2021, the defendant, Andean Medjedovic (**"Andean"**), launched a sophisticated cyber-attack (the **"Attack"**) against Indexed Finance, a decentralized financial platform for cryptocurrencies and other digital assets. As a result of the Attack, Andean routed approximately $15.8 million from Indexed Finance's index pools to his "wallet" (account) on the Ethereum blockchain with public address: 0xba5ed1488be60ba2facc6b66c6d6f0befba22ebe (the **"Wallet"**).

3. To achieve this, Andean used computer hacking techniques to bypass Indexed Finance's trading controls. He executed a series of trades, using approximately $159 million in borrowed assets, that he knew would distort the algorithm used by Indexed Finance to set trading prices. This allowed Andean to purchase those assets at artificially deflated prices, thus acquiring assets

representing over 90% of the value of the DEFI5 and CC10 pools at a tiny fraction of their true value.

The Parties

4. The defendant, Andean, is a 19-year-old mathematics prodigy who has completed a master's degree in mathematics at the University of Waterloo. He is a resident of Ontario.

5. The plaintiff, Dillon Kellar is a co-founder of Indexed Finance and a resident of the City of Leander, Texas.

6. The plaintiff, Laurence Day is a full-time contributor to Indexed Finance, where his responsibilities include communications, technical writing, and research. He is a resident of the City of Leeds in the United Kingdom.

7. Indexed Finance is a project focused on the development of passive portfolio management strategies for digital assets on the Ethereum blockchain. Indexed Finance is an unincorporated association of its users, or “tokenholders.” It is a “decentralized autonomous organization” (or “**DAO**”), a common governance model in the crypto world. Indexed Finance has no physical offices and no centralized location.

Background

8. Index pools are the crypto world’s equivalent of index funds. They allow users to purchase a digital “token” that represents a pool of digital assets, allowing users to gain diversification through exposure to a broader index of digital assets at a low cost. Index pools are “non-custodial”, meaning that the underlying assets are owned by its users (and not by Indexed Finance).

9. The Attack targeted two index pools:

- **DEFI5:** the "DeFi Top 5 Tokens Index" (or **"DEFI5"**) focuses on large cap decentralized finance protocols across the Ethereum network;

- **CC10:** the "Cryptocurrency Top 10 Tokens Index" (or **"CC10"**) covers the most popular medium to large-cap cryptocurrencies on the Ethereum network.

10. Index pools are like exchange-traded index funds (**"ETFs"**) in traditional finance. Like a share of an ETF, each token of an index pool represents a fractional stake in a set of underlying assets. Like the shares of an ETF, index pool tokens are traded on an exchange. Like an ETF, the trading price for an index pool token is regulated so that it tracks the net asset value (**"NAV"**) of its underlying assets. Like an ETF, the actual trading price of an index pool token may diverge from its NAV. When this occurs, arbitrage traders can exploit the divergence and earn a profit, at the expense of the pool's tokenholders. Index pools use a complex mechanism to ensure that the pool token's trading price matches its NAV. Unlike an ETF, however, an index pool allows users to issue and redeem their own pool tokens directly from the index pool in exchange for the index token's trading price.

11. Adding a new token to the pool is akin to adding a new stock to the bundle of stocks included in an ETF. When a new token is added to one of Indexed Finance pools, the index pool recalculates the trading price for pool tokens using a benchmark called "Total Pool Value" which is used to approximate the index pool's NAV (the **"Benchmark"**). The index pool sets a trade volume limit that restricts the number of new pool tokens that can be issued at the new trading price to a maximum of 1.5% of the Benchmark's value.

The Attack

12. The Attack used market manipulation and computer hacking techniques to trigger a glitch in the pricing mechanism for the DEFI5 and CC10 index pools. The glitch caused the index pools to set a trading price for the DEFI5 and CC10 pool tokens at a tiny fraction of their NAV. The Attack then purchased assets at the depressed trading prices, i.e. to exploit the pricing glitch that the attacker himself had created.

13. The Attack involved the deployment of customized computer code developed by Andean, involving dozens of trades and hundreds of commands. It occurred over a period of just a few minutes, first targeting the DEFI5 index pool and then the CC10 index pool. While the mechanics of the Attack were highly complex, the plan of the Attack involved three basic components. For the DEFI5 Attack:

(a) **Benchmark Manipulation:** Andean used over $150 million in borrowed assets (more than 10 times DEFI5's NAV) to execute a series of trades designed to manipulate the Benchmark by temporarily distorting the price of its reference asset (the asset price by which the Benchmark is set).

(b) **Hacking the Trade Volume Limits:** by manipulating the Benchmark, Andean caused the DEFI5 index pool to set an artificially low price for the DEFI5 pool token relative to its NAV. Due to the index pool's trade volume limit, Andean should only have been able buy a limited number of pool tokens at prices influenced by the Benchmark manipulation (to a maximum of 1.5% of the Benchmark's value). However, Andean devised a hack by which he disabled the trade volume limit, permitting him to issue an enormous number of pool tokens at manipulated prices.

(c) **"Arbitrage" Trades:** the combined effect of manipulating the Benchmark manipulation and circumventing the volume limit was that the DEFI5 index pool set a price for issuing new pool tokens that was vastly below their NAV. Andean executed trades by issuing new pool tokens at the price that his actions had deflated, then immediately redeeming the pool token into its underlying assets. Andean repeated this pattern until he had drained over 90% of DEFI5's NAV.

14. The Attack repeated the above process on the CC10 index pool, with similar results.

15. Andean funded and coordinated the Attack through the Wallet.

16. Andean sought to conceal his identity by running the cryptocurrency used to pay the transaction costs for the Attack through a sophisticated "privacy mixer" called Tornado Cash.

Liability

17. Andean's conduct constitutes civil fraud on the holders of DEFI5 and CC10 tokens. In the course of the Attack, he knowingly made a false representation by manipulating the value of the Benchmark. This constituted a misrepresentation by conduct and/or active concealment of a material fact. By manipulating the Benchmark, Andean induced the DEFI5 and CC10 index pools — the contents of which were owned by the tokenholders – to sell him the pools' underlying assets at dramatically deflated prices, causing them to suffer significant losses.

18. To the extent that the trades involved in the Attack involved the formation of any contract(s) between or among Andean and any Class members, any such contracts would be void *ab initio*, or voidable, and should be rescinded and set aside on grounds of misrepresentation, mistake, unconscionability, and/or fraud/illegality.

19. Further, Andean violated the duty of honest performance in respect of any such contracts.

20. Andean has been unjustly enriched as a result of the Attack at the expense of the DEFI5 and CC10 tokenholders. There is no juristic reason for Andean's enrichment. The Attack involved conduct that is prohibited by provisions of the *Criminal Code* relating to computer hacking (s. 342.1) and fraud (s. 380(2)).

21. In taking the digital assets and storing them in his own Wallet, Andean interfered with the tokenholders' immediate right of possession over the digital assets and is liable in conversion.

Remedy

22. The digital assets stored in the Wallet are the rightful property of the tokenholders and a constructive trust should be recognized or imposed over the Wallet.

23. The holders of DEFI5 and CC10 tokens suffered direct losses of approximately \$12.5 million and \$4.0 million, respectively. Furthermore, additional losses were suffered by token holders who held their tokens indirectly, i.e. who owned tokens through other "pools" (the equivalent of a "fund of funds"). The effect of the Attack on the NAV of the DEFI5 and CC10 tokens caused severe disruptions in the prices of any pool token on the blockchain that held DEFI5 and CC10 tokens. In the immediate aftermath of the Attack, these disruptions caused massive and

predictable losses to arbitrage traders. The Plaintiffs continue to investigate the quantum of these losses but estimate that they exceed $10 million.

24. Andean was, at all times, aware that his conduct would harm the tokenholders. His conduct was high-handed, oppressive, harsh, vindicative, reprehensible, malicious, and in disregard of the rights of the DEFI5 and CC10 tokenholders.

The Class

25. The plaintiffs seek to represent the following proposed class (the **"Class"**):

> *All persons or entities anywhere in the world who owned tokens of DEFI5 or CC10, whether directly or indirectly, immediately prior to the time of the Attack, being October 14, 2021 at 6:37:43 pm (UTC) for DEFI5 and 6:39:49 pm (UTC) for CC10.*

26. At the time of the Attack, the plaintiff Dillon Kellar directly held DEFI5 and CC10 tokens. The plaintiff Laurence Day directly held DEFI5 tokens, and he indirectly held both DEFI5 and CC10 tokens. The Indexed Finance DAO itself directly held tokens of CC10 and DEFI5 and indirectly held tokens of each.

December 17, 2021

STOCKWOODS LLP
Barristers
Toronto-Dominion Centre
TD North Tower, Box 140
77 King Street West, Suite 4130
Toronto ON M5K 1H1

Gerald Chan (54548T)
Tel: 416-593-1617
GeraldC@stockwoods.ca

Fredrick Schumann (59377L)
Tel: 416-593-2490
FredrickS@stockwoods.ca

Stephen Aylward (66556E)
Tel: 416-593-2496
stephena@stockwoods.ca

Alexandra Heine (83514R)
Tel: 416-593-1669
AlexandraH@stockwoods.ca

Tel: 416-593-7200
Fax: 416-593-9345

Lawyers for the Plaintiffs/Moving Parties

Electronically issued / Délivré par voie électronique : 17-Dec-2021

Court File No./N° du dossier du greffe: CV-21-00673984-00CP

DILLON KELLAR et al. and ANDEAN MEDJEDOVIC Court File No.

Plaintiffs Defendant

ONTARIO
SUPERIOR COURT OF JUSTICE

Proceeding commenced at TORONTO

NOTICE OF ACTION

STOCKWOODS LLP
Barristers
Toronto-Dominion Centre
TD North Tower, Box 140
77 King Street West, Suite 4130
Toronto ON M5K 1H1

Gerald Chan (54548T)
Tel: 416-593-1617 / GeraldC@stockwoods.ca

Fredrick Schumann (59377L)
Tel: 416-593-2490 / FredrickS@stockwoods.ca

Stephen Aylward (66556E)
Tel: 416-593-2496 / stephena@stockwoods.ca

Alexandra Heine (83514R)
Tel: 416-593-1669 / AlexandraH@stockwoods.ca

Tel: 416-593-2496
Fax: 416-593-9345

Lawyers for the Plaintiffs

Court File No. CV-21-00673984-00CP

ONTARIO
SUPERIOR COURT OF JUSTICE

B E T W E E N:

DILLON KELLAR and LAURENCE DAY

Plaintiffs

and

ANDEAN MEDJEDOVIC

Defendant

Proceedings under the *Class Proceedings Act*, 1992, SO 1992, c 6

MAREVA ORDER

NOTICE

If you, the Defendant, disobey this order you may be held to be in contempt of court and may be imprisoned, fined or have your assets seized. You are entitled to apply on at least twenty-four (24) hours notice to the Plaintiff, for an order granting you sufficient funds for ordinary living expenses and legal advice and representation.

Any other person who knows of this order and does anything which helps or permits the Defendant to breach the terms of this Order may also be held to be in contempt of court and may be imprisoned, fined or have their assets seized.

THIS MOTION, made by the plaintiffs, Dillon Kellar and Laurence Day, for an interim Order restraining the defendant, Andean Medjedovic, from dissipating certain assets, and for other relief, was heard this day at the court house at 361 University Avenue, Toronto.

ON READING the motion record and factum of the plaintiffs/moving parties, and on noting the undertaking of the plaintiffs to abide by any order this court may make concerning damages arising from the granting and enforcement of this order, and on hearing submissions from counsel for the parties,

1. THIS COURT ORDERS that time for service and filing of this motion is abridged.

MAREVA INJUNCTION

2. THIS COURT ORDERS that the defendant, and his servants, employees, agents, assigns, officers, directors, and anyone else acting on their behalf or in conjunction with any of them, and any and all persons with notice of this injunction, are restrained from directly or indirectly, by any means whatsoever:

(a) selling, removing, dissipating, alienating, transferring, assigning, encumbering, or similarly dealing with any of the cryptocurrencies and other digital assets held in the account (or "wallet") with the Ethereum blockchain address 0xba5ed1488be60ba2facc6b66c6d6f0befba22ebe (the **"Wallet"**) or any assets into which the assets held in the Wallet may subsequently be (or have been since October 14, 2021) liquidated, exchanged, or otherwise transferred (the **"Assets"**);

(b) disposing of or dealing with or diminishing the value of any of the Assets in any way;

(c) engaging in or proceeding with any transaction, the effect of which is to transfer or receive funds outside Ontario from the sale, transfer, assignment, or encumbering of any of the Assets;

(d) instructing, requesting, counselling, demanding, or encouraging any other person to do so; and

(e) facilitating, assisting in, aiding, abetting, or participating in any acts the effect of which is to do so.

Nothing in this order shall prevent the defendant from cooperating with a court-appointed receiver to transfer the Assets in a manner directed by the receiver.

3. THIS COURT ORDERS that paragraph 2 applies to the Assets whether or not they are in the defendant's own name and whether they are solely or jointly owned.

ORDINARY LIVING EXPENSES

4. THIS COURT ORDERS that the defendant may apply for an order, on at least twenty-four (24) hours notice to the plaintiffs, specifying the amount of funds which the defendant is entitled to spend on ordinary living expenses and legal advice and representation.

VARIATION, DISCHARGE OR EXTENSION OF ORDER

6. THIS COURT ORDERS that anyone served with or notified of this order may apply to the court at any time to vary or discharge this order, on four days notice to the plaintiffs.

7. THIS COURT ORDERS that this order shall remain in effect pending a further order of this court.

DILLON KELLAR et al. and ANDEAN MEDJEDOVIC Court File No. CV-21-00673984-00CP
Plaintiffs Defendant

SUPERIOR COURT OF JUSTICE

Proceeding commenced at TORONTO

MAREVA ORDER

STOCKWOODS LLP
Barristers
Toronto-Dominion Centre
TD North Tower, Box 140
77 King Street West, Suite 4130
Toronto ON M5K 1H1

Gerald Chan (54548T)
Tel: 416-593-1617 / GeraldC@stockwoods.ca

Fredrick Schumann (59377L)
Tel: 416-593-2490 / FredrickS@stockwoods.ca

Stephen Aylward (66556E)
Tel: 416-593-2496 / stephena@stockwoods.ca

Alexandra Heine (83514R)
Tel: 416-593-1669 / AlexandraH@stockwoods.ca

Tel: 416-593-7200
Fax: 416-593-9345

Lawyers for the Plaintiffs

Court File No. CV-21-00673984-00CP

ONTARIO
SUPERIOR COURT OF JUSTICE

B E T W E E N:

DILLON KELLAR and LAURENCE DAY

Plaintiffs

and

ANDEAN MEDJEDOVIC

Defendant

RECEIVERSHIP ORDER

THIS MOTION, made by the plaintiffs, Dillon Kellar and Laurence Day, for an interim receivership order and for other relief, was heard this day at the court house at 361 University Avenue, Toronto.

ON READING the motion record and factum of the plaintiffs/moving parties, and on noting the undertaking of the plaintiffs to abide by any order this court may make concerning damages arising from the granting and enforcement of this order, and on hearing submissions from counsel for the parties,

Appointment

1. THIS COURT ORDERS that Raymond Chabot Administrateur Provisoire Inc. is hereby appointed receiver of property (**"Receiver"**) over the digital assets (the **"Assets"**) held in the

account (or ‘wallet”) with the Ethereum blockchain address 0xba5ed1488be60ba2facc6b66c6d6f0befba22ebe (the **“Wallet”**).

Receiver's Powers

2. THIS COURT ORDERS that the Receiver is hereby empowered and authorized to do the following in respect of the Assets:

(a) to receive and take possession of and exercise control over the Assets;

(b) to preserve and protect the Assets by arranging for a secure method for storing the Assets; and

(c) to take any steps reasonably incidental to the exercise of these powers.

And where the Receiver takes any such actions or steps, it shall be exclusively authorized and empowered to do so, to the exclusion of all other persons and without interference from any person, including the defendant.

3. THIS COURT ORDERS that the Receiver shall have no power, duty, or responsibility whatsoever in respect of liquidation or management of the Assets, including investment advice or portfolio management, but shall simply preserve the Assets pending further order of this Court.

Duty To Cooperate With the Receiver

4. THIS COURT ORDERS that the defendant shall cooperate with the Receiver and shall follow all reasonable instructions provided by the Receiver for the secure transfer of the Assets from the defendant to Receiver and shall effect such transfer under the direct supervision of the

Receiver’s representatives at such reasonable time and place and in such reasonable manner as the Receiver may require.

5. THIS COURT ORDERS that the defendant shall provide whatever information or documentation to the Receiver as may be necessary for the Receiver to carry out its powers under this order.

No Proceedings Against the Receiver

6. THIS COURT ORDERS that no proceeding or enforcement process in any court or tribunal shall be commenced or continued against the Receiver except with the written consent of the Receiver or with leave of this Court.

Limitation on the Receiver's Liability

7. THIS COURT ORDERS that the Receiver shall incur no liability or obligation as a result of its appointment or the carrying out of the provisions of this order, save and except for any gross negligence or wilful misconduct on its part. Nothing in this order shall derogate from the protections afforded the Receiver by any applicable legislation.

Receiver's Accounts

8. THIS COURT ORDERS that costs of the Receiver shall be borne by the plaintiffs, provided that nothing in this order shall prevent the plaintiffs from later claiming such costs in the action in which this order is made.

Request for Directions

9. THIS COURT ORDERS that the Receiver may from time to time apply to this Court for advice and directions in the discharge of its powers and duties hereunder.

Variation, Discharge, or Extension of Order

10. THIS COURT ORDERS that anyone served with or notified of this order may apply to the court at any time to vary or discharge this order, on four days' notice to the plaintiffs.

11. THIS COURT ORDERS this order shall remain in effect pending a further order of this court.

DILLON KELLAR et al. Plaintiffs	and	ANDEAN MEDJEDOVIC Defendant	Court File No. CV-21-00673984-00CP

SUPERIOR COURT OF JUSTICE

Proceeding commenced at TORONTO

RECEIVERSHIP ORDER

STOCKWOODS LLP
Barristers
Toronto-Dominion Centre
TD North Tower, Box 140
77 King Street West, Suite 4130
Toronto ON M5K 1H1

Gerald Chan (54548T)
Tel: 416-593-1617 / GeraldC@stockwoods.ca

Fredrick Schumann (59377L)
Tel: 416-593-2490 / FredrickS@stockwoods.ca

Stephen Aylward (66556E)
Tel: 416-593-2496 / stephena@stockwoods.ca

Alexandra Heine (83514R)
Tel: 416-593-1669 / AlexandraH@stockwoods.ca

Tel: 416-593-2496
Fax: 416-593-9345

Lawyers for the Plaintiffs

~~Commercial List No.:~~ Court File No. CV-21-00673984-00CP

ONTARIO
SUPERIOR COURT OF JUSTICE
~~COMMERCIAL LIST~~[1]

B E T W E E N:

~~**PLAINTIFF**~~

DILLON KELLAR and LAURENCE DAY

Plaintiffs

and

ANDEAN MEDJEDOVIC

Defendant~~**DEFENDANT**~~

Proceedings under the *Class Proceedings Act*, 1992, SO 1992, c 6

MAREVA ORDER[2]

NOTICE

If you, the Defendant, disobey this order you may be held to be in contempt of court and may be imprisoned, fined or have your assets seized. You are entitled to apply on at least twenty-four (24) hours notice to the Plaintiff, for an order granting you sufficient funds for ordinary living expenses and legal advice and representation.

Any other person who knows of this order and does anything which helps or permits the Defendant to breach the terms of this Order may

---

~~[1] Prepared by the Commercial List Users' Committee of the Ontario Superior Court of Justice. The theory and approach behind this model order is to give the Courts and practitioners a guide for the use of such orders, while recognizing that the model order must be tailored to suit the particular circumstances of each case before the Court.~~

~~[2] See generally UK Practice Direction form for "Freezing Injunctions" http://www.dca.gov.uk/civil/procedure/procrules_fin/contents/practice_directions/pd_part25.htm.~~

also be held to be in contempt of court and may be imprisoned, fined or have their assets seized.

THIS MOTION, made ~~without notice~~ by the ~~Plaintiff, [ ],~~plaintiffs, Dillon Kellar and Laurence Day, for an interim Order ~~in the form of a *Mareva* injunction~~ restraining the defendant, ~~[ ],~~Andean Medjedovic, from dissipating ~~its~~certain assets, and for other relief, was heard this day at ~~[ ].~~the court house at 361 University Avenue, Toronto.

ON READING the ~~Affidavit of [ ] sworn [ ], on hearing~~ motion record and factum of the ~~submissions of counsel for the Plaintiff~~plaintiffs/moving parties, and on noting the undertaking of the ~~Plaintiff~~plaintiffs to abide by any order this court may make concerning damages arising from the granting and enforcement of this order, and on hearing submissions from counsel for the parties,

~~**Mareva Injunction**~~

1. THIS COURT ORDERS that time for service and filing of this motion is abridged.

MAREVA INJUNCTION

~~1.~~2. THIS COURT ORDERS that the defendant, and ~~its~~his servants, employees, agents, assigns, officers, directors, and anyone else acting on their behalf or in conjunction with any of them, and any and all persons with notice of this injunction, are restrained from directly or indirectly, by any means whatsoever:

(a) selling, removing, dissipating, alienating, transferring, assigning, encumbering, or similarly dealing with any ~~assets of the~~ of the cryptocurrencies and other digital assets held in the account (or "wallet") with the Ethereum blockchain address 0xba5ed1488be60ba2facc6b66c6d6f0befba22ebe (the **"Wallet"**) or any assets into which the assets held in the Wallet may subsequently be (or have been since October 14, 2021) liquidated, exchanged, or otherwise transferred (the **"Assets"**);~~Defendant, wherever situate [*that are located in Ontario*],~~[3] ~~including but not limited to the assets and accounts listed in Schedule "A" hereto;~~[4]

(b) disposing of or dealing with or diminishing the value of any of the Assets in any way;

(c) engaging in or proceeding with any transaction, the effect of which is to transfer or receive funds outside Ontario from the sale, transfer, assignment, or encumbering of any of the Assets;

~~(b)~~(d) instructing, requesting, counselling, demanding, or encouraging any other person to do so; and

~~(c)~~(e) facilitating, assisting in, aiding, abetting, or participating in any acts the effect of which is to do so.

Nothing in this order shall prevent the defendant from cooperating with a court-appointed receiver to transfer the Assets in a manner directed by the receiver.

~~2.~~3. THIS COURT ORDERS that paragraph ~~1~~2 applies to ~~all of~~ the ~~Defendant's~~ Assets whether or not they are in ~~his~~the defendant's own name and whether they are solely or jointly owned. ~~For~~

~~[3] See *Mooney v. Orr*, [1994] B.C.J. No. 2652 (B.C.S.C.) and *Pharma Investment Ltd. v. Clark*, [1997] O.J. No. 1334 (Gen. Div.) for a discussion of the scope of a Mareva Injunction.~~

~~[4] Ordinarily, the plaintiff must show grounds for the belief that the defendant has some assets within the jurisdiction to obtain the injunction in the first place, but in its standard form, the Mareva injunction is not limited to those named assets: *Cretanor Marine Co. Ltd. v. Irish Marine Management Ltd.* [1978] 1 W.L.R. 966 at 973 (C.A.).~~

~~the purpose of this order, the Defendant's assets include any asset which he has the power, directly or indirectly, to dispose of or deal with as if it were his own. The Defendant is to be regarded as having such power if a third party holds or controls the assets in accordance with his direct or indirect instructions.[5]~~

~~3. **[THIS COURT ORDERS** that if the total value free of charges or other securities of the Defendant' assets [*in Ontario*] exceeds $**[ ]**, the Defendant may sell, remove, dissipate, alienate, transfer, assign, encumber, or similarly deal with them so long as the total unencumbered value of the Defendant's assets [*in Ontario*] remains above $**[ ]]**.~~[6]

ORDINARY LIVING EXPENSES

4. THIS COURT ORDERS that the defendant may apply for an order, on at least twenty-four (24) hours notice to the ~~Plaintiff~~plaintiffs, specifying the amount of funds which the defendant is entitled to spend on ordinary living expenses and legal advice and representation.~~[7]~~

~~**Disclosure of Information**~~

~~5. **THIS COURT ORDERS** that the Defendant prepare and provide to the Plaintiff within [ ] days of the date of service of this Order, a sworn statement describing the nature, value, and~~

~~[5] *Federal Bank of the Middle East Ltd. v. Hadkinson*, [2000] 1 W.L.R. 1695 (Eng. C.A.)~~

~~[6] *Z Ltd. v. A.,* [1982] 1 All ER 556 (C.A.). As a practical point, specifying the maximum amount to be frozen will be simple where the claim relates to a specific amount of money, however this task will be more challenging where the claim is for general damages to be particularized and quantified at a later stage of the litigation. It will also be difficult for the affected financial institutions to determine which assets may be released under this provision. It may therefore be more appropriate to deal with the quantification of the maximum amount to be frozen at the return of the motion.~~

~~[7] *Z Ltd. v. A., supra*; *Pharma Investments Ltd. v. Clark, supra* at para. 13. This provision may not be appropriate in the case of a specific fraud claim where the misappropriated amount is frozen, since the Defendant cannot be allowed to use funds that are identifiable as obtained wrongfully for living expenses. Further it will be difficult to specify an amount, without evidence from the Defendant regarding his or her needs and assets. See also the practical concerns raised above in footnote 5. Lord Denning has suggested that a separate account be opened so that the financial institutions affected by the order need not determine which sums are required for ordinary living expenses. Depending on the Plaintiff's knowledge of the specific accounts of the Defendant, it might be possible to specify from which account the funds for living expenses may be withdrawn. Given these practical difficulties, it is more appropriate to address the issue of living expenses on the expeditious return of the motion.~~

~~location of his assets worldwide [*in Ontario*], whether in his own name or not and whether solely or jointly owned.~~[8]

~~6. **THIS COURT ORDERS** that the Defendant submit to examinations under oath within [ ] days of the delivery by the Defendant of the aforementioned sworn statements.~~

~~7. **THIS COURT ORDERS** that if the provision of any of this information is likely to incriminate the Defendant, he may be entitled to refuse to provide it, but is recommended to take legal advice before refusing to provide the information. Wrongful refusal to provide the information referred to in paragraph 5 herein is contempt of court and may render the Defendant liable to be imprisoned, fined, or have his assets seized.~~[9]

~~**Third Parties**~~

~~8. **THIS COURT ORDERS [ ]** (the "Banks") to forthwith freeze and prevent any removal or transfer of monies or assets of the Defendant held in any account or on credit on behalf of the Defendant, with the Banks, until further Order of the Court, including but not limited to the accounts listed in Schedule "A" hereto.~~[10]

~~9. **THIS COURT ORDERS** that the Banks forthwith disclose and deliver up to the Plaintiff any and all records held by the Banks concerning the Defendant's assets and accounts, including the existence, nature, value and location of any monies or assets or credit, wherever situate [*in Ontario*], held on behalf of the Defendant by the Banks.~~[11]

~~**Alternative Payment of Security into Court**~~

~~10. **THIS COURT ORDERS** that this Order will cease to have effect if the Defendant provides security by paying the sum of $**[ ]** into Court, and the Accountant of the Superior Court of Justice is hereby directed to accept such payment.~~[12]

~~[8] The Court has the inherent power to make ancillary orders as appear to be just and convenient to ensure that the exercise of the Mareva jurisdiction is effective to achieve its purpose and may make an order of "discovery in aid", an injunction where the plaintiff has "grounds for believing that the defendant does have assets within the jurisdiction, but has insufficient particulars of the whereabouts of such assets to make the injunction effective": Sharpe, at 2.1070, 2.1080.~~

~~[9] *Pharma Investment Ltd. v. Clark, supra* at para. 16, but see *CBS United Kingdom Ltd. v. Lambert* [1983] Ch. 37, [1982] 3 All E.R. 237 (C.A.).~~

~~[10] *Z Ltd. v. A, supra* at 563.~~

~~[11] The Plaintiff ordinarily must bear any costs associated with a search of bank records to determine the whereabouts and amounts of the defendant's assets on deposit: *Searose Ltd. v. Seatrain U.K. Ltd.* [1981] 1 W.L.R. (Q.B.).~~

~~[12] Specifying the amount of security attracts the same practical problems identified in footnote 5.~~

COSTS

5. THIS COURT ORDERS that costs of this motion is in the cause.

VARIATION, DISCHARGE OR EXTENSION OF ORDER

~~11.~~6. THIS COURT ORDERS that anyone served with or notified of this order may apply to the court at any time to vary or discharge this order, on four ~~(4)~~ days notice to the ~~Plaintiff~~plaintiffs.

~~12.~~7. THIS COURT ORDERS that ~~the Plaintiff~~ this order shall ~~apply for an extension~~remain in effect pending a further order of this ~~Order within ten (10) days hereof, failing which this Order will terminate.~~[13] court.

~~[13] *Rules of Civil Procedure*, R.R.O. 1990, Reg. 194, rule 40.02.~~

~~**SCHEDULE "A"**~~

~~**Commercial List No.:**~~

~~***ONTARIO***~~
~~**SUPERIOR COURT OF JUSTICE (COMMERCIAL LIST)**~~

~~PROCEEDING COMMENCED AT TORONTO~~

DILLON KELLAR et al. and ANDEAN MEDJEDOVIC Court File No. CV-21-00673984-00CP
Plaintiffs Defendant

SUPERIOR COURT OF JUSTICE

Proceeding commenced at TORONTO

MAREVA ORDER

STOCKWOODS LLP
Barristers
Toronto-Dominion Centre
TD North Tower, Box 140
77 King Street West, Suite 4130
Toronto ON M5K 1H1

Gerald Chan (54548T)
Tel: 416-593-1617 / GeraldC@stockwoods.ca

Fredrick Schumann (59377L)
Tel: 416-593-2490 / FredrickS@stockwoods.ca

Stephen Aylward (66556E)
Tel: 416-593-2496 / stephena@stockwoods.ca

Alexandra Heine (83514R)
Tel: 416-593-1669 / AlexandraH@stockwoods.ca

Tel: 416-593-7200
Fax: 416-593-9345

Lawyers for the Plaintiffs

~~Revised: January 21, 2014~~
~~s.243(1) BIA (National Receiver) and s. 101 CJA (Ontario) Receiver~~

~~Court File No.~~ Court File No. CV-21-00673984-00CP

ONTARIO
SUPERIOR COURT OF JUSTICE
~~**COMMERCIAL LIST**~~

~~**PLAINTIFF**~~[1]

~~Plaintiff~~

B E T W E E N:

DILLON KELLAR and LAURENCE DAY
~~**DEFENDANT**~~

Plaintiffs

and

ANDEAN MEDJEDOVIC

Defendant

RECEIVERSHIP ORDER
~~**(APPOINTING RECEIVER)**~~

[1] ~~The Model Order Subcommittee notes that a receivership proceeding may be commenced by action or by application. This model order is drafted on the basis that the receivership proceeding is commenced by way of an action.~~

THIS MOTION, made by the ~~Plaintiff[2]~~plaintiffs, Dillon Kellar and Laurence Day, for an ~~Order pursuant to section 243(1) of the *Bankruptcy and Insolvency Act*, R.S.C. 1985, c. B-3, as amended (the "BIA")~~ interim receivership order and ~~section 101 of the *Courts of Justice Act*, R.S.O. 1990, c. C.43, as amended (the "CJA") appointing [RECEIVER'S NAME] as receiver [and manager] (in such capacities, the "Receiver") without security, of all of the assets, undertakings and properties of [DEBTOR'S NAME] (the "Debtor") acquired~~ for~~, or used in relation to a business carried on by the Debtor~~ other relief, was heard this day at ~~330~~the court house at 361 University Avenue, Toronto~~, Ontario~~.

ON READING the ~~affidavit of [NAME] sworn [DATE]~~motion record and factum of the ~~Exhibits thereto~~plaintiffs/moving parties, and on noting the undertaking of the plaintiffs to abide by any order this court may make concerning damages arising from the granting and enforcement of this order, and on hearing ~~the~~ submissions ~~of~~from counsel for ~~[NAMES], no one appearing for [NAME] although duly served as appears from the affidavit of service of [NAME] sworn [DATE] and on reading the consent of [RECEIVER'S NAME] to act as~~ the ~~Receiver~~parties,

~~SERVICE~~

Appointment

~~1.~~ THIS COURT ORDERS that ~~the time for service of the Notice of Motion and the Motion is hereby abridged and validated[3] so that this motion is properly returnable today and hereby dispenses with further service thereof.~~

~~[2] Section 243(1) of the BIA provides that the Court may appoint a receiver "on application by a secured creditor".~~

~~[3] If service is effected in a manner other than as authorized by the Ontario *Rules of Civil Procedure*, an order validating irregular service is required pursuant to Rule 16.08 of the *Rules of Civil Procedure* and may be granted in appropriate circumstances.~~

~~**APPOINTMENT**~~

~~2.~~1. ~~THIS COURT ORDERS that pursuant to section 243(1) of the BIA and section 101 of the CJA, [RECEIVER'S NAME]~~Raymond Chabot Administrateur Provisoire Inc. is hereby appointed receiver~~, without security,~~ of ~~all of~~property (**"Receiver"**) over the digital assets~~, undertakings and properties of~~ (the ~~Debtor acquired for, or used~~**"Assets"**) held in ~~relation to a business carried on by~~ the ~~Debtor, including all proceeds thereof (~~account (or 'wallet") with the ~~"Property").~~Ethereum blockchain address 0xba5ed1488be60ba2facc6b66c6d6f0befba22ebe (the **"Wallet"**).

~~**RECEIVER'S POWERS**~~

Receiver's Powers

~~3.~~2. THIS COURT ORDERS that the Receiver is hereby empowered and authorized~~, but not obligated,~~ to ~~act at once~~do the following in respect of the ~~Property and, without in any way limiting the generality of the foregoing, the Receiver is hereby expressly empowered and authorized to do any of the following where the Receiver considers it necessary or desirable:~~ Assets:

(a) to receive and take possession of and exercise control over the ~~Property and any and all proceeds, receipts and disbursements arising out of or from the Property~~Assets;

~~(b) to receive, preserve, and protect the Property, or any part or parts thereof, including, but not limited to, the changing of locks and security codes, the relocating of Property to safeguard it, the engaging of independent security personnel, the taking of physical inventories and the placement of such insurance coverage as may be necessary or desirable;~~

~~(c) to manage, operate, and carry on the business of the Debtor, including the powers to enter into any agreements, incur any obligations in the ordinary~~

~~course of business, cease to carry on all or any part of the business, or cease to perform any contracts of the Debtor;~~

(b) ~~to engage consultants, appraisers, agents, experts, auditors, accountants, managers, counsel and such other persons from time to time and on whatever basis, including on a temporary basis, to assist with the exercise of the~~ to preserve and protect the Assets by arranging for a secure method for storing the Assets; and

~~(d) **Receiver's Powers** and duties, including without limitation those conferred by this Order;~~

~~(e) to purchase or lease such machinery, equipment, inventories, supplies, premises or other assets to continue the business of the Debtor or any part or parts thereof;~~

~~(f) to receive and collect all monies and accounts now owed or hereafter owing to the Debtor and to exercise all remedies of the Debtor in collecting such monies, including, without limitation, to enforce any security held by the Debtor;~~

~~(g) to settle, extend or compromise any indebtedness owing to the Debtor;~~

~~(h) to execute, assign, issue and endorse documents of whatever nature in respect of any of the Property, whether in the Receiver's name or in the name and on behalf of the Debtor, for any purpose pursuant to this Order;~~

~~(i) to initiate, prosecute and continue the prosecution of any and all proceedings and to defend all proceedings now pending or hereafter instituted with respect to the Debtor, the Property or the Receiver, and to settle or compromise any such proceedings.~~[4] ~~The authority hereby~~

[4] ~~This model order does not include specific authority permitting the Receiver to either file an assignment in bankruptcy on behalf of the Debtor, or to consent to the making of a bankruptcy order against the Debtor. A~~

~~conveyed shall extend to such appeals or applications for judicial review in respect of any order or judgment pronounced in any such proceeding;~~

~~(j) to market any or all of the Property, including advertising and soliciting offers in respect of the Property or any part or parts thereof and negotiating such terms and conditions of sale as the Receiver in its discretion may deem appropriate;~~

~~(k) to sell, convey, transfer, lease or assign the Property or any part or parts thereof out of the ordinary course of business,~~

~~(i) without the approval of this Court in respect of any transaction not exceeding $________, provided that the aggregate consideration for all such transactions does not exceed $__________; and~~

~~(ii) with the approval of this Court in respect of any transaction in which the purchase price or the aggregate purchase price exceeds the applicable amount set out in the preceding clause;~~

~~and in each such case notice under subsection 63(4) of the Ontario *Personal Property Security Act*, [or section 31 of the Ontario *Mortgages Act*, as the case may be,][5] shall not be required, and in each case the Ontario *Bulk Sales Act* shall not apply.~~

~~(l) to apply for any vesting order or other orders necessary to convey the Property or any part or parts thereof to a purchaser or purchasers thereof, free and clear of any liens or encumbrances affecting such Property;~~

~~bankruptcy may have the effect of altering the priorities among creditors, and therefore the specific authority of the Court should be sought if the Receiver wishes to take one of these steps.~~

~~[5] If the Receiver will be dealing with assets in other provinces, consider adding references to applicable statutes in other provinces. If this is done, those statutes must be reviewed to ensure that the Receiver is exempt from or can be exempted from such notice periods, and further that the Ontario Court has the jurisdiction to grant such an exemption.~~

~~(m) to report to, meet with and discuss with such affected Persons (as defined below) as the Receiver deems appropriate on all matters relating to the Property and the receivership, and to share information, subject to such terms as to confidentiality as the Receiver deems advisable;~~

~~(n) to register a copy of this Order and any other Orders in respect of the Property against title to any of the Property;~~

~~(o) to apply for any permits, licences, approvals or permissions as may be required by any governmental authority and any renewals thereof for and on behalf of and, if thought desirable by the Receiver, in the name of the Debtor;~~

~~(p) to enter into agreements with any trustee in bankruptcy appointed in respect of the Debtor, including, without limiting the generality of the foregoing, the ability to enter into occupation agreements for any property owned or leased by the Debtor;~~

~~(q) to exercise any shareholder, partnership, joint venture or other rights which the Debtor may have; and~~

~~(r)~~(c) to take any steps reasonably incidental to the exercise of these powers~~ or the performance of any statutory obligations~~.

And~~ in each case~~ where the Receiver takes any such actions or steps, it shall be exclusively authorized and empowered to do so, to the exclusion of all other persons ~~(as defined below), including the Debtor, ~~and without interference from any ~~other Person~~person, including the defendant.

~~**DUTY TO PROVIDE ACCESS AND CO-OPERATION TO THE RECEIVER**~~

~~4. THIS COURT ORDERS that (i) the Debtor, (ii) all of its current and former directors, officers, employees, agents, accountants, legal counsel and shareholders, and all other persons~~

~~acting on its instructions or behalf, and (iii) all other individuals, firms, corporations, governmental bodies or agencies, or other entities having notice of this Order (all of the foregoing, collectively, being "Persons" and each being a "Person") shall forthwith advise the Receiver of the existence of any Property in such Person's possession or control, shall grant immediate and continued access to the Property to the Receiver, and shall deliver all such Property to the Receiver upon the Receiver's request.~~

~~5. THIS COURT ORDERS that all Persons shall forthwith advise the Receiver of the existence of any books, documents, securities, contracts, orders, corporate and accounting records, and any other papers, records and information of any kind related to the business or affairs of the Debtor, and any computer programs, computer tapes, computer disks, or other data storage media containing any such information (the foregoing, collectively, the "Records") in that Person's possession or control, and shall provide to the Receiver or permit the Receiver to make, retain and take away copies thereof and grant to the Receiver unfettered access to and use of accounting, computer, software and physical facilities relating thereto, provided however that nothing in this paragraph 5 or in paragraph 6 of this Order shall require the delivery of Records, or the granting of access to Records, which may not be disclosed or provided to the Receiver due to the privilege attaching to solicitor client communication or due to statutory provisions prohibiting such disclosure.~~

~~6. THIS COURT ORDERS that if any Records are stored or otherwise contained on a computer or other electronic system of information storage, whether by independent service provider or otherwise, all Persons in possession or control of such Records shall forthwith give unfettered access to the Receiver for the purpose of allowing the Receiver to recover and fully copy all of the information contained therein whether by way of printing the information onto paper or making copies of computer disks or such other manner of retrieving and copying the information as the Receiver in its discretion deems expedient, and shall not alter, erase or destroy any Records without the prior written consent of the Receiver. Further, for the purposes of this paragraph, all Persons shall provide the Receiver with all such assistance in gaining immediate access to the information in the Records as the Receiver may in its discretion require including providing the Receiver with instructions on the use of any computer or other system and providing~~

~~the Receiver with any and all access codes, account names and account numbers that may be required to gain access to the information.~~

~~7. THIS COURT ORDERS that the Receiver shall provide each of the relevant landlords with notice of the Receiver's intention to remove any fixtures from any leased premises at least seven (7) days prior to the date of the intended removal. The relevant landlord shall be entitled to have a representative present in the leased premises to observe such removal and, if the landlord disputes the Receiver's entitlement to remove any such fixture under the provisions of the lease, such fixture shall remain on the premises and shall be dealt with as agreed between any applicable secured creditors, such landlord and the Receiver, or by further Order of this Court upon application by the Receiver on at least two (2) days notice to such landlord and any such secured creditors.~~

3. THIS COURT ORDERS that the Receiver shall have no power, duty, or responsibility whatsoever in respect of liquidation or management of the Assets, including investment advice or portfolio management, but shall simply preserve the Assets pending further order of this Court.

Duty To Cooperate With the Receiver

4. THIS COURT ORDERS that the defendant shall cooperate with the Receiver and shall follow all reasonable instructions provided by the Receiver for the secure transfer of the Assets from the defendant to Receiver and shall effect such transfer under the direct supervision of the Receiver's representatives at such reasonable time and place and in such reasonable manner as the Receiver may require.

5. THIS COURT ORDERS that the defendant shall provide whatever information or documentation to the Receiver as may be necessary for the Receiver to carry out its powers under this order.

No Proceedings Against the Receiver

~~8.~~6. THIS COURT ORDERS that no proceeding or enforcement process in any court or tribunal ~~(each, a "Proceeding"),~~ shall be commenced or continued against the Receiver except with the written consent of the Receiver or with leave of this Court.

~~**NO PROCEEDINGS AGAINST THE DEBTOR OR THE PROPERTY**~~

~~9. THIS COURT ORDERS that no Proceeding against or in respect of the Debtor or the Property shall be commenced or continued except with the written consent of the Receiver or with leave of this Court and any and all Proceedings currently under way against or in respect of the Debtor or the Property are hereby stayed and suspended pending further Order of this Court.~~

~~**NO EXERCISE OF RIGHTS OR REMEDIES**~~

~~10. THIS COURT ORDERS that all rights and remedies against the Debtor, the Receiver, or affecting the Property, are hereby stayed and suspended except with the written consent of the Receiver or leave of this Court, provided however that this stay and suspension does not apply in respect of any "eligible financial contract" as defined in the BIA, and further provided that nothing in this paragraph shall (i) empower the Receiver or the Debtor to carry on any business which the Debtor is not lawfully entitled to carry on, (ii) exempt the Receiver or the Debtor from compliance with statutory or regulatory provisions relating to health, safety or the environment, (iii) prevent the filing of any registration to preserve or perfect a security interest, or (iv) prevent the registration of a claim for lien.~~

~~**NO INTERFERENCE WITH THE RECEIVER**~~

~~11. THIS COURT ORDERS that no Person shall discontinue, fail to honour, alter, interfere with, repudiate, terminate or cease to perform any right, renewal right, contract, agreement, licence or permit in favour of or held by the Debtor, without written consent of the Receiver or leave of this Court.~~

~~CONTINUATION OF SERVICES~~

~~12. THIS COURT ORDERS that all Persons having oral or written agreements with the Debtor or statutory or regulatory mandates for the supply of goods and/or services, including without limitation, all computer software, communication and other data services, centralized banking services, payroll services, insurance, transportation services, utility or other services to the Debtor are hereby restrained until further Order of this Court from discontinuing, altering, interfering with or terminating the supply of such goods or services as may be required by the Receiver, and that the Receiver shall be entitled to the continued use of the Debtor's current telephone numbers, facsimile numbers, internet addresses and domain names, provided in each case that the normal prices or charges for all such goods or services received after the date of this Order are paid by the Receiver in accordance with normal payment practices of the Debtor or such other practices as may be agreed upon by the supplier or service provider and the Receiver, or as may be ordered by this Court.~~

~~RECEIVER TO HOLD FUNDS~~

~~13. THIS COURT ORDERS that all funds, monies, cheques, instruments, and other forms of payments received or collected by the Receiver from and after the making of this Order from any source whatsoever, including without limitation the sale of all or any of the Property and the collection of any accounts receivable in whole or in part, whether in existence on the date of this Order or hereafter coming into existence, shall be deposited into one or more new accounts to be opened by the Receiver (the "Post Receivership Accounts") and the monies standing to the credit of such Post Receivership Accounts from time to time, net of any disbursements provided for herein, shall be held by the Receiver to be paid in accordance with the terms of this Order or any further Order of this Court.~~

~~EMPLOYEES~~

~~14. THIS COURT ORDERS that all employees of the Debtor shall remain the employees of the Debtor until such time as the Receiver, on the Debtor's behalf, may terminate the employment of such employees. The Receiver shall not be liable for any employee-related liabilities, including any successor employer liabilities as provided for in section 14.06(1.2) of the BIA, other than such~~

~~amounts as the Receiver may specifically agree in writing to pay, or in respect of its obligations under sections 81.4(5) or 81.6(3) of the BIA or under the *Wage Earner Protection Program Act*.~~

~~PIPEDA~~

~~15. THIS COURT ORDERS that, pursuant to clause 7(3)(c) of the Canada *Personal Information Protection and Electronic Documents Act*, the Receiver shall disclose personal information of identifiable individuals to prospective purchasers or bidders for the Property and to their advisors, but only to the extent desirable or required to negotiate and attempt to complete one or more sales of the Property (each, a "Sale"). Each prospective purchaser or bidder to whom such personal information is disclosed shall maintain and protect the privacy of such information and limit the use of such information to its evaluation of the Sale, and if it does not complete a Sale, shall return all such information to the Receiver, or in the alternative destroy all such information. The purchaser of any Property shall be entitled to continue to use the personal information provided to it, and related to the Property purchased, in a manner which is in all material respects identical to the prior use of such information by the Debtor, and shall return all other personal information to the Receiver, or ensure that all other personal information is destroyed.~~

~~LIMITATION ON ENVIRONMENTAL LIABILITIES~~

~~16. THIS COURT ORDERS that nothing herein contained shall require the Receiver to occupy or to take control, care, charge, possession or management (separately and/or collectively, "Possession") of any of the Property that might be environmentally contaminated, might be a pollutant or a contaminant, or might cause or contribute to a spill, discharge, release or deposit of a substance contrary to any federal, provincial or other law respecting the protection, conservation, enhancement, remediation or rehabilitation of the environment or relating to the disposal of waste or other contamination including, without limitation, the *Canadian Environmental Protection Act*, the Ontario *Environmental Protection Act*, the *Ontario Water Resources Act*, or the Ontario *Occupational Health and Safety Act* and regulations thereunder (the "Environmental Legislation"), provided however that nothing herein shall exempt the Receiver from any duty to report or make disclosure imposed by applicable Environmental Legislation. The Receiver shall not, as a result of this Order or anything done in pursuance of the Receiver's duties and powers under this Order,~~

~~be deemed to be in Possession of any of the Property within the meaning of any Environmental Legislation, unless it is actually in possession.~~

~~**LIMITATION ON THE RECEIVER'S LIABILITY**~~

Limitation on the Receiver's Liability

~~17.~~7. THIS COURT ORDERS that the Receiver shall incur no liability or obligation as a result of its appointment or the carrying out of the provisions of this order, save and except for any gross negligence or wilful misconduct on its part~~, or in respect of its obligations under sections 81.4(5) or 81.6(3) of the BIA or under the *Wage Earner Protection Program Act*. ~~. Nothing in this order shall derogate from the protections afforded the Receiver by ~~section 14.06 of the BIA or by any other~~any applicable legislation.

Receiver's Accounts

~~18. THIS COURT ORDERS that the Receiver and counsel to the Receiver shall be paid their reasonable fees and disbursements, in each case at their standard rates and charges unless otherwise ordered by the Court on the passing of accounts, and that the Receiver and counsel to the Receiver shall be entitled to and are hereby granted a charge (the "Receiver's Charge") on the Property, as security for such fees and disbursements, both before and after the making of this Order in respect of these proceedings, and that the Receiver's Charge shall form a first charge on the Property in priority to all security interests, trusts, liens, charges and encumbrances, statutory or otherwise, in favour of any Person, but subject to sections 14.06(7), 81.4(4), and 81.6(2) of the BIA.~~[6]

~~19. THIS COURT ORDERS that the Receiver and its legal counsel shall pass its accounts from time to time, and for this purpose the accounts of the Receiver and its legal counsel are hereby referred to a judge of the Commercial List of the Ontario Superior Court of Justice.~~

[6] ~~Note that subsection 243(6) of the BIA provides that the Court may not make such an order "unless it is satisfied that the secured creditors who would be materially affected by the order were given reasonable notice and an opportunity to make representations".~~

~~20. THIS COURT ORDERS that prior to the passing of its accounts, the Receiver shall be at liberty from time to time to apply reasonable amounts, out of the monies in its hands, against its fees and disbursements, including legal fees and disbursements, incurred at the standard rates and charges of the Receiver or its counsel, and such amounts shall constitute advances against its remuneration and disbursements when and as approved by this Court.~~

~~FUNDING OF THE RECEIVERSHIP~~

~~21. THIS COURT ORDERS that the Receiver be at liberty and it is hereby empowered to borrow by way of a revolving credit or otherwise, such monies from time to time as it may consider necessary or desirable, provided that the outstanding principal amount does not exceed \$_________ (or such greater amount as this Court may by further Order authorize) at any time, at such rate or rates of interest as it deems advisable for such period or periods of time as it may arrange, for the purpose of funding the exercise of the powers and duties conferred upon the Receiver by this Order, including interim expenditures. The whole of the Property shall be and is hereby charged by way of a fixed and specific charge (the "Receiver's Borrowings Charge") as security for the payment of the monies borrowed, together with interest and charges thereon, in priority to all security interests, trusts, liens, charges and encumbrances, statutory or otherwise, in favour of any Person, but subordinate in priority to the Receiver's Charge and the charges as set out in sections 14.06(7), 81.4(4), and 81.6(2) of the BIA.~~

~~22. THIS COURT ORDERS that neither the Receiver's Borrowings Charge nor any other security granted by the Receiver in connection with its borrowings under this Order shall be enforced without leave of this Court.~~

~~23. THIS COURT ORDERS that the Receiver is at liberty and authorized to issue certificates substantially in the form annexed as Schedule "A" hereto (the "Receiver's Certificates") for any amount borrowed by it pursuant to this Order.~~

~~24. THIS COURT ORDERS that the monies from time to time borrowed by the Receiver pursuant to this Order or any further order of this Court and any and all Receiver's Certificates evidencing the same or any part thereof shall rank on a *pari passu* basis, unless otherwise agreed to by the holders of any prior issued Receiver's Certificates.~~

~~**SERVICE AND NOTICE**~~

~~25. THIS COURT ORDERS that the E-Service Protocol of the Commercial List (the "**Protocol**") is approved and adopted by reference herein and, in this proceeding, the service of documents made in accordance with the Protocol (which can be found on the Commercial List website at) shall be valid and effective service. Subject to Rule 17.05 this Order shall constitute an order for substituted service pursuant to Rule 16.04 of the Rules of Civil Procedure. Subject to Rule 3.01(d) of the Rules of Civil Procedure and paragraph 21 of the Protocol, service of documents in accordance with the Protocol will be effective on transmission. This Court further orders that a Case Website shall be established in accordance with the Protocol with the following URL '<@>'.~~

~~26. THIS COURT ORDERS that if the service or distribution of documents in accordance with the Protocol is not practicable, the Receiver is at liberty to serve or distribute this Order, any other materials and orders in these proceedings, any notices or other correspondence, by forwarding true copies thereof by prepaid ordinary mail, courier, personal delivery or facsimile transmission to the Debtor's creditors or other interested parties at their respective addresses as last shown on the records of the Debtor and that any such service or distribution by courier, personal delivery or facsimile transmission shall be deemed to be received on the next business day following the date of forwarding thereof, or if sent by ordinary mail, on the third business day after mailing.~~

~~**GENERAL**~~

8. THIS COURT ORDERS that costs of the Receiver shall be borne by the plaintiffs, provided that nothing in this order shall prevent the plaintiffs from later claiming such costs in the action in which this order is made.

Request for Directions

~~27.~~9. THIS COURT ORDERS that the Receiver may from time to time apply to this Court for advice and directions in the discharge of its powers and duties hereunder.

Variation, Discharge, or Extension of Order

~~28.~~ THIS COURT ORDERS that ~~nothing in~~ anyone served with or notified of this order ~~shall prevent the Receiver from acting as a trustee in bankruptcy of the Debtor.~~

~~29. THIS COURT HEREBY REQUESTS the aid and recognition of any court, tribunal, regulatory or administrative body having jurisdiction in Canada or in the United States to give effect to this Order and to assist the Receiver and its agents in carrying out the terms of this Order. All courts, tribunals, regulatory and administrative bodies are hereby respectfully requested to make such orders and to provide such assistance to the Receiver, as an officer of this Court, as~~ may ~~be necessary or desirable to give effect to this Order or to assist the Receiver and its agents in carrying out the terms of this Order.~~

~~30. THIS COURT ORDERS that the Receiver be at liberty and is hereby authorized and empowered to~~ apply to ~~any court, tribunal, regulatory or administrative body, wherever located, for the recognition of this Order and for assistance in carrying out the terms of this Order, and that the Receiver is authorized and empowered to act as a representative in respect of the within proceedings for the purpose of having these proceedings recognized in a jurisdiction outside Canada.~~

~~31. THIS COURT ORDERS that the Plaintiff shall have its costs of this motion, up to and including entry and service of this Order, provided for by the terms of the Plaintiff's security or, if not so provided by the Plaintiff's security, then on a substantial indemnity basis to be paid by the Receiver from the Debtor's estate with such priority and at such~~ the court at any time ~~as this Court may determine.~~

~~32.~~10. ~~THIS COURT ORDERS that any interested party may apply to this Court~~ to vary or ~~amend~~discharge this order, on ~~not less than seven (7) days'~~four days' notice to the ~~Receiver and to~~

~~any other party likely to be affected by the order sought or upon such other notice, if any, as this Court may order~~plaintiffs.

~~SCHEDULE "A"~~

~~RECEIVER CERTIFICATE~~

~~CERTIFICATE NO. ______________~~

~~AMOUNT $_____________________~~

~~1. THIS IS TO CERTIFY that [RECEIVER'S NAME], the receiver (the "Receiver") of the assets, undertakings and properties [DEBTOR'S NAME] acquired for, or used in relation to a business carried on by the Debtor, including all proceeds thereof (collectively, the "Property") appointed by Order of the Ontario Superior Court of Justice (Commercial List) (the "Court") dated the ___ day of ______, 20__ (the "Order") made in an action having Court file number __-CL-_______, has received as such Receiver from the holder of this certificate (the "Lender") the principal sum of $___________, being part of the total principal sum of $___________ which the Receiver is authorized to borrow under and pursuant to the Order.~~

~~2. The principal sum evidenced by this certificate is payable on demand by the Lender with interest thereon calculated and compounded [daily][monthly not in advance on the _______ day of each month] after the date hereof at a notional rate per annum equal to the rate of ______ per cent above the prime commercial lending rate of Bank of _________ from time to time.~~

~~3. Such principal sum with interest thereon is, by the terms of the Order, together with the principal sums and interest thereon of all other certificates issued by the Receiver pursuant to the Order or to any further order of the Court, a charge upon the whole of the Property, in priority to the security interests of any other person, but subject to the priority of the charges set out in the Order and in the *Bankruptcy and Insolvency Act*, and the right of the Receiver to indemnify itself out of such Property in respect of its remuneration and expenses.~~

~~4. All sums payable in respect of principal and interest under this certificate are payable at the main office of the Lender at Toronto, Ontario.~~

~~5. Until all liability in respect of this certificate has been terminated, no certificates creating charges ranking or purporting to rank in priority to this certificate shall be issued by the Receiver to any person other than the holder of this certificate without the prior written consent of the holder of this certificate.~~

~~6. The charge securing this certificate shall operate so as to permit the Receiver to deal with the Property as authorized by the Order and as authorized by any further or other order of the Court.~~

~~7. The Receiver does not undertake, and it is not under any personal liability, to pay any sum in respect of which it may issue certificates under the terms of the Order.~~

~~DATED the ______ day of _______________, 20__.~~

11. THIS COURT ORDERS this order shall remain in effect pending a further order of this court.

____

DILLON KELLAR et al. and ANDEAN MEDJEDOVIC Court File No. CV-21-00673984-00CP
Plaintiffs Defendant

SUPERIOR COURT OF JUSTICE

Proceeding commenced at TORONTO

RECEIVERSHIP ORDER

STOCKWOODS LLP
Barristers
Toronto-Dominion Centre
TD North Tower, Box 140
77 King Street West, Suite 4130
Toronto ON M5K 1H1

Gerald Chan (54548T)
Tel: 416-593-1617 / GeraldC@stockwoods.ca

Fredrick Schumann (59377L)
Tel: 416-593-2490 / FredrickS@stockwoods.ca

Stephen Aylward (66556E)
Tel: 416-593-2496 / stephena@stockwoods.ca

Alexandra Heine (83514R)
Tel: 416-593-1669 / AlexandraH@stockwoods.ca

Tel: 416-593-2496
Fax: 416-593-9345

Lawyers for the Plaintiffs

DILLON KELLAR et al. and ANDEAN MEDJEDOVIC Court File No. CV-21-00673984-00CP
Plaintiffs Defendant

ONTARIO
SUPERIOR COURT OF JUSTICE

Proceeding commenced at TORONTO

MOTION RECORD OF THE MOVING PLAINTIFFS, VOLUME 2

STOCKWOODS LLP
Barristers
Toronto-Dominion Centre
TD North Tower, Box 140
77 King Street West, Suite 4130
Toronto ON M5K 1H1

Gerald Chan (54548T)
Tel: 416-593-1617 / GeraldC@stockwoods.ca

Fredrick Schumann (59377L)
Tel: 416-593-2490 / FredrickS@stockwoods.ca

Stephen Aylward (66556E)
Tel: 416-593-2496 / stephena@stockwoods.ca

Alexandra Heine (83514R)
Tel: 416-593-1669 / AlexandraH@stockwoods.ca

Tel: 416-593-2496
Fax: 416-593-9345

Lawyers for the Plaintiffs