EigenPhi
WISDOM OF DEFI

Report on Code at Risk

An In-depth Analysis of How AAVE's $1.6 Million Bad Debt Was Created

December 2022

Content

Abstract 1

Takeaways 1

The storyline of the whole event 2

- Dumping process
- Short squeeze
- Liquidation
- Aftermath

Dumping CRV across the market 3

- A complete description of the dumping steps
- Token flow between Ethereum and OKX
- CRV shorter's position on AAVE before liquidation

How did bad debt occur? 6

- The liquidation process
- Correlation between liquidation and short-squeeze activities
- Aftermath: PnL of different participants

The root cause of the risk 8

Liquidators' behavior and preferences 10

- Liquidators' revenue and loss
- Source of capital

Interesting transactions 13

- CRV shorter's on-chain limit order during dumping
- CRV shorter attacked by sandwich during dumping
- Liquidators attacked by sandwich

Appendix 14

- Appendix 1: CRV shorter's addresses
- Appendix 2: Tx records of CRV from 0x57e0's related address 0xba52 to OKX
- Appendix 3: Tx records of USDC transferred back to 0x57e0 through Circle
- Appendix 4: A calculation of CRV shorter's PnL before and after liquidation

Disclaimer 15

Abstract

The MEV world is aptly described as a dark forest where the transparency of on-chain activities brings unprecedented opportunities and risks for users: everything becomes calculable. A living example of this has recently emerged: a crypto whale failed miserably against a short squeeze and left an uncovered debt on the lending platform AAVE.

This report will show how the whale created this bad debt using a thorough analysis of token flows. We will also share EigenPhi's idea of a control system based on liquidity sensors and a feedback loop to address the risk issues arising from DeFi's new features compared to traditional finance.

Takeaways

- A crypto whale dumped the CRV market with 92 million CRV borrowed from AAVE. This action resulted in a precise short squeeze attack costing the crypto whale an estimated $20 million and creating a bad debt on AAVE worth about $1.6 million.
- The two pull-ups in CRV prices successively caused the shorter's AAVE position to trigger the liquidation and insolvency threshold. 385 liquidations by 21 unique addresses emptied 63.596 million USDC collateral, leaving 2.456 million CRV unpaid.
- AAVE utilizes quotes fed by on-chain oracles to calculate whether the liquidation threshold is triggered, which has a lag of about 10 minutes compared to Binance's price information.
- In between the two price pulls, there were more than 3 hours when the liquidation condition was not triggered due to a temporary price drop. At this stage, AAVE may have missed the best time to adopt a contingency strategy.
- We believe the root cause of this event is the transparent nature of a blockchain makes financial information easily accessible, giving attackers more advantages.
- However, the current lending protocols are not designed with a risk control mechanism based on timely adjustment according to both price and liquidity information.
- We propose creating a feedback control system for DeFi based on safety cushions and liquidity sensors to better address risk in the long term.

The storyline of the whole event

Dumping process

On Nov 13, the CRV shorter transferred almost 39 million USDC from its ponzishorter.eth to 0x57E04786E231Af3343562C062E0d058F25daCE9E, which he used to operate the whole dumping process.

- The CRV shorter deposited a total of 63.596 million USDC to AAVE V2 and progressively borrowed 92 million CRV (about 14% of circulating supply) from the platform through revolving collateral.
- 71.55 million CRV was transferred to this related address and then immediately sent to an address tagged as OKX by Etherscan. The remaining CRV was all used to swap out USDC through DEX aggregators like 1inch and 0x protocol.
- During the dumping period, the price of CRV decreased from 0.59 to 0.43 until Nov 22.

Short squeeze

Around 11:00 on Nov 22, the price of CRV suddenly began to increase. The CRV shorter likely faced a short squeeze.

Liquidation

Starting from 13:31 on Nov 22, the CRV shorter's position on AAVE triggered the liquidation threshold, and the debt was cleared by a total of 385 liquidations in two successive batches. 21 unique liquidators participated in this process.

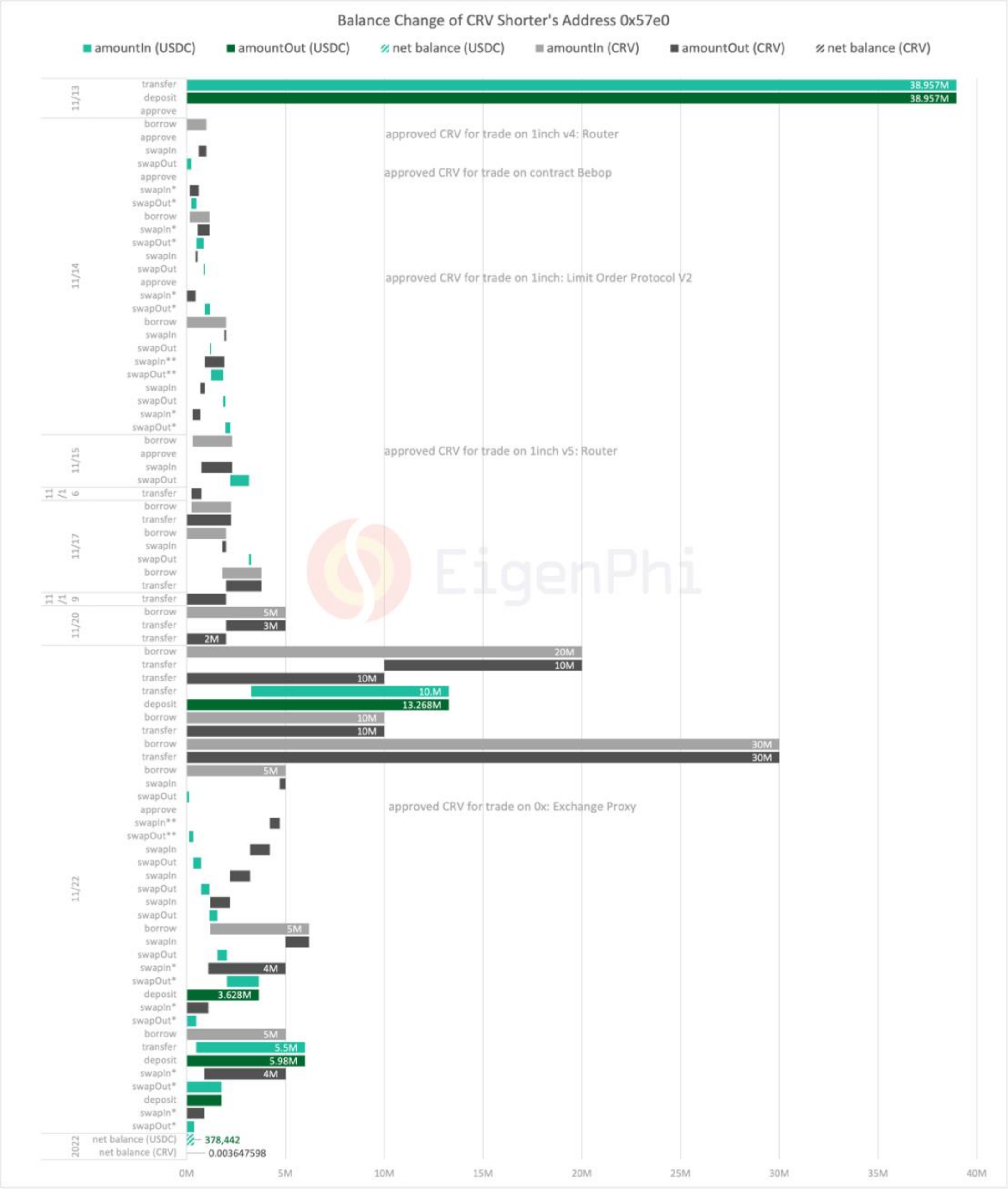
Aftermath

- AAVE: 2.456 million CRV unpaid, the value of which will change according to CRV's price. At $0.636, it equals about $1.6 million.
- Liquidators: the total revenue is about $3.55 million, but most of their proceeds flowed to validators through gas fees and miner tips.
- CRV shorter: loses an estimated $20 million (Appendix 4).
- Based on the PnL of the above participants, we guess most value eventually flows to the short squeezers and other unknown participants.

The following part is a detailed analysis of token flow during the dumping process, the remaining balance of the shorter's address, and his position on AAVE before and after the liquidation process. We also tried finding the exact turning point when the position crossed the liquidation threshold and the root cause of the result.

Dumping CRV across the market

A complete description of the dumping steps

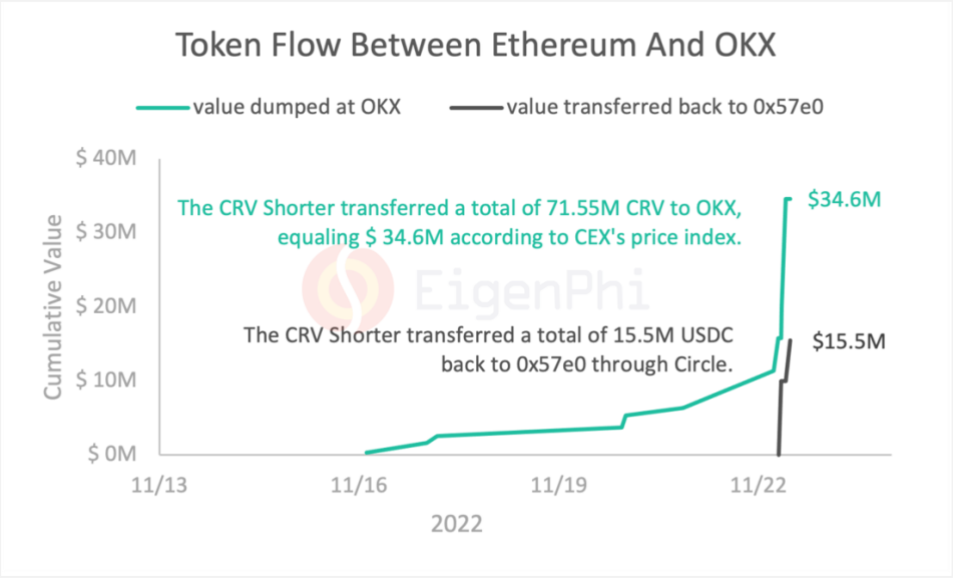


The above figure shows a detailed illustration of the actions taken by the shorter during the dumping process.

- The shorter transferred a principal of 38.957M USDC from ponzishorter.eth to its related address 0x57e0.
- Then he deposited USDC to AAVE V2 and borrowed a lot of CRV in subsequent transactions.
- The shorter used part of the CRV to swap out USDC through the following protocols:
    - 1inch V4, V5, Limit Order
    - Bebop
    - 0x Exchange
- He transferred another part of the CRV to OKX through an intermediate address 0xBA529566855d9d0Bf3De1cc988E5f529F92Bd80C, dumping the CEX's market. 15.5M USDC was then transferred back to 0x57e0 through Circle.
- The shorter's token balance at 0x57e0 at the end (checked by Etherscan's data):
    - USDC: 378,442
    - CRV: ~0

In a word, the dumping operations were relatively moderate before Nov 22. But on Nov 22, the shorter poured a large amount of CRV onto the market. He used up his CRV, leaving only a tiny amount of USDC in his address compared to his principal.

Token flow between Ethereum and OKX



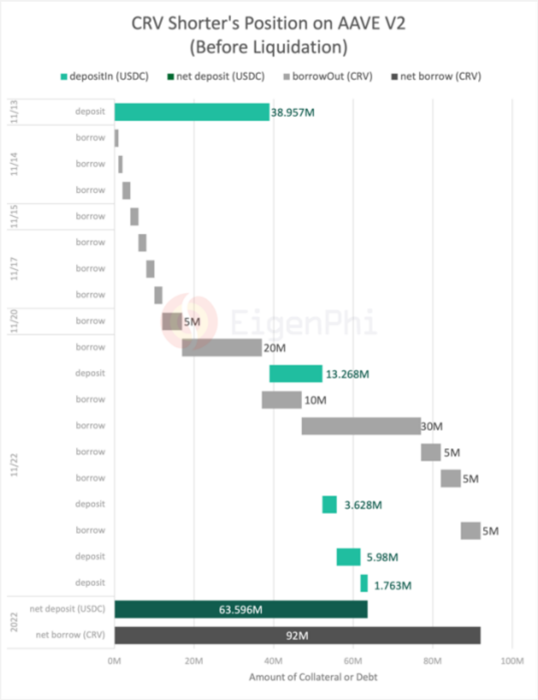
We also tracked the token flow between his EOA address and the address related to the centralized exchange, OKX (Appendix 2). The CRV shorter transferred 34.6 million dollars of CRV to OKX and 15.5 million dollars of USDC back to its EOA address (Appendix 3), which was then used as collateral and borrowed more CRV.

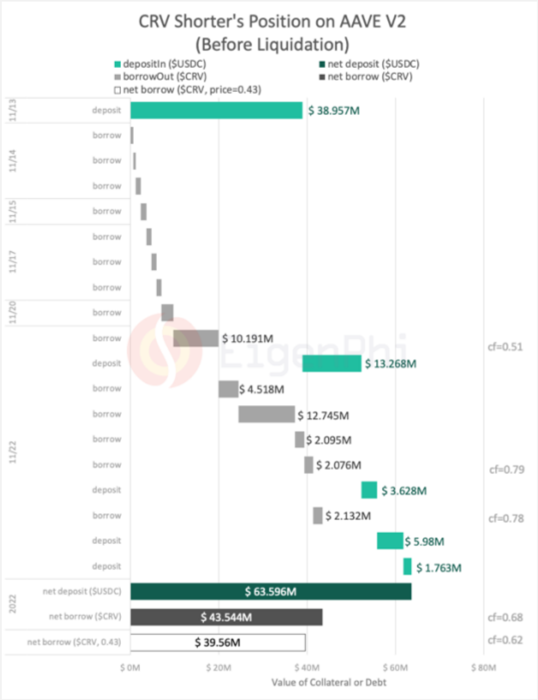
CRV shorter's position on AAVE before liquidation

By extracting only borrow and deposit token flows, we get the following figure showing the shorter's position change from the perspective of the lending platform. The shorter deposited 63.596 million USDC and borrowed 92 million CRV ($39.56 million at price CRV=$0.43) from the platform at the end of the dumping process.

$$cf = \frac{\$Debt}{\$Collateral}$$

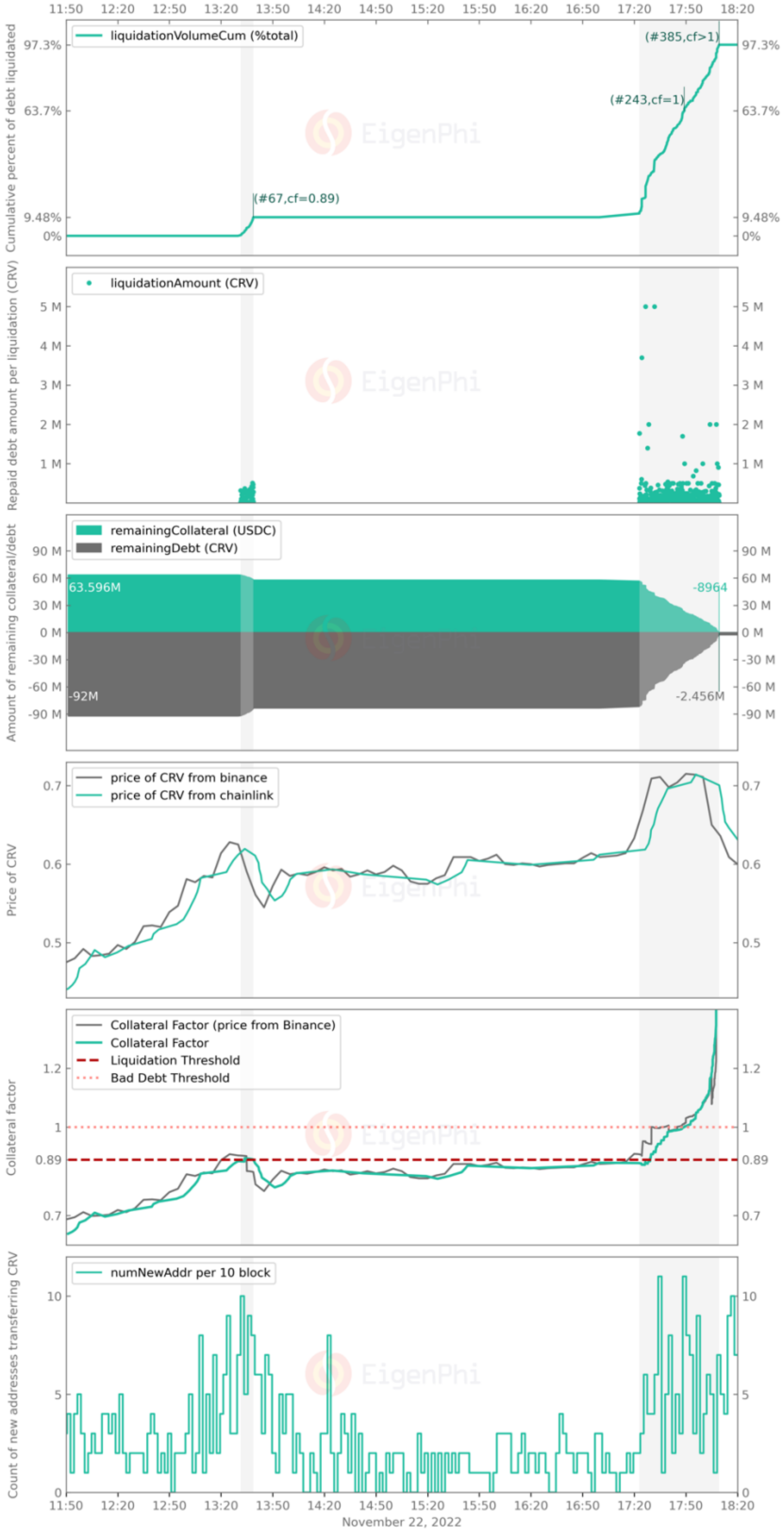
More importantly, one can easily calculate the *collateral factor* (*cf*) of its position after dollarizing the amounts. We can also see that the shorter was careful to replenish collateral during the dumping process to prevent the collateral factor from increasing over the liquidation threshold, which is 0.89 for USDC as collateral.





How did bad debt occur?

The following figures merge the facts we consider significant in analyzing the cause of bad debt during the liquidation process.



The liquidation process

- After the shorter finished his last operation at 11:53, Nov 22, he had sold all his CRV, and the market price of CRV was around $0.43. At this point, the price of CRV began to increase rapidly. Starting from 13:31 on the same day, the first batch of liquidation transactions liquidated less than 10% of total debt, corresponding to the first price peak after a short squeeze.
- After a short period, the shorter's position temporarily deviated from the dangerous liquidation threshold, as the price dropped after the first peak. However, this stage lasted about three and a half hours before the price pulled up rapidly again, causing the position to trigger a series of liquidations again, meaning the remaining collateral balance became less than the remaining outstanding loan. At about 17:50, the bad debts began to appear, with 36.3% of the debt still remaining. The liquidation process ended at 18:09. **Eventually, there was 2.456 million CRV in unpaid loans.**
- The reason the liquidators took 8,964 more USDC than the total amount pledged by the shorter may be related to the interest accrued on the collateral during this period.
- A total of 385 liquidations occurred in 356 transactions. Sometimes, there may be more than one liquidation in a single transaction. Liquidators sourced the initial capital for 125 (32.5%) liquidations from flash loans.
- The average liquidation amount is relatively small, less than 1% of the total debt. The highest amount liquidated was about 5 million.
- 21 unique liquidators participated in the liquidation process. The amount of each liquidation as a percentage of the remaining debt has a 75% probability of less than 1%, and the maximum was 24%, far less than the AAVE's upper limit (50%) set for each liquidation.

In addition, to calculate the collateral factor of the position at a given moment, we compared the quotes from Chainlink and Binance. It is clear that the former has a lag effect compared to the latter, but the overall fluctuation pattern is consistent. Looking at the precise time when the collateral factor triggered both the liquidation and bad debt thresholds, AAVE determines whether to activate liquidations based on the quotes from on-chain oracles like Chainlink.

Correlation between liquidation and short-squeeze activities

Lastly, the liquidation pace correlates highly with price fluctuation, and both price peaks correspond to exactly two liquidation periods.

This appears to be a planned and precise short-squeeze strategy. To further test this idea, we counted the activity of addresses on the chain that transferred CRV tokens during this period.

One interesting finding is that the two phases of price rise to the peak coincide with the emergence of many new addresses that transfer CRV for the first time during the whole history of Ethereum. This data indicates that many traders who followed the trend of short squeezes showed collective impetuous behavior.

For example, after removing the relevant addresses from the liquidators, 21.5 million CRV were transferred in and out of this new CRV-transferring address with a large turnover rate, 0xee8e0fcc8bff03ec5f100d02cb7b3196d78863a7.

Aftermath: PnL of different participants

We can estimate the PnL of different participants after the liquidation:

- AAVE: 2.456 million CRV unpaid, the value of which will change according to CRV's price. At $0.636, it equals about $1.6 million.
- Liquidators: the total revenue is about $3.55 million, but most of their proceeds flowed to validators through gas fees and miner tips.
- CRV shorter: loses an estimated $20 million (Appendix 4).
- Based on the above participants' PnL, we guess most value eventually flows to the short squeezers and other unknown participants.

The root cause of the risk

By gathering additional background information, we know that the CRV shorter, Avi (@avi_eisen), successfully executed the Mango Squeeze on Solana. However, the CRV bad debt event is different. Our data infers Avi employed a new strategy in this event and incurred losses in a short squeeze attack unless he conducted some sort of collateralized CRV lending operation in an unknown centralized market. But we believe the probability of this is relatively low.

Note that the short squeezers here, the participants who pulled up the price, are not the same person, and the timely release of the crvUSD white paper on Curve's part also facilitated the price pull. These chain reactions built an irrational collective behavior that caused the price to rise more than expected in the short term. The crucial question is: why AAVE failed to liquidate Avi's entire position before the collateral factor approached 1?

This incident has generated numerous discussions, with many suggesting the creation of bad debt is due to a lack of liquidity in CRV and a lack of proactive risk control measures. Admittedly, illiquid assets with a high liquidation threshold are prone to manipulation. The liquidity shortage of a lending asset directly affects the cost of funds available for the liquidator to use, which impacts the speed of liquidation. Also, the increasing price of CRV makes a short position unhealthier. All these facts provide the conditions for short squeezers to attack, but we should not consider it a root cause of risk.

In other words, the best solution is not, at least in the long run, to pin DeFi's risk control on introducing censorship on illiquid assets or adjusting risk parameters after the fact.

On the one hand, this is unrealistic. Let's not forget that AAVE relied partially on introducing long-tail assets to open up the market, given the already successful premise of Compound.

On the other hand, an asset's level of liquidity and safety margin can change over its life cycle and is also susceptible to contagion risk by associated assets. Recently, in the BSC ecosystem, the Ankr platform was hacked to issue a large number of aBNBc out of thin air due to a vulnerability, resulting in more than a dozen protocols' associated pools, including Pancake and Helio, suffering heavy damage.

The killer thing is that these attack vectors are unpredictable and give the protocols a rather short response time. Even with the Ethereum chain assuming more than 80% of ETH's liquidity is staked for PoS mining on a given day, as is the case with many other PoS blockchains, there is no guarantee this blue chip asset and its associated asset, stETH, will not have similar problems.

From our point of view, we should “blame” the root cause of the problem on a defect that accompanies the decentralized implementation of blockchains - transparency. The dark forest in the blockchain world offers scientists unprecedented access to information about the DeFi market. This transparency allows them to calculate any information bias regarding asset price and liquidity, while the current lending protocols' design hasn't introduced liquidity-based parameters to protect against risk. Like in this case, once exposed, the shorter's position would easily attract short squeeze attacks, as everything becomes calculable. Attackers have a much broader information set at their disposal than current lending protocols' response mechanisms.

Currently, the lending protocols designed a few presupposed scalar parameters to control the risk. The remediation strategies mostly prepare risk reserves for advancing funds in the event of insolvency. Although this preserves the LPs' money, the protocols' reputation is more or less damaged. We believe that a risk control solution based on a single hypothetical safety cushion would not be enough to protect this new financial system, where everything is transparent and calculable. The composability between DeFi Legos also increases the uncertainty of this complex system.

More specifically, we believe the liquidation triggers cannot be determined solely by a threshold calculated from a quote that reflects historical market information. Not to mention, the oracle feeds prices with a lag of about 10 minutes. Even in traditional financial markets, risk managers attempt to gather various market information and take temporary deleveraging measures where appropriate. We want to point out that risk managers in DeFi should consider both price and liquidity factors and establish risk control parameters that can adjust proactively based on market liquidity information. Otherwise, the protocol will probably be at a disadvantage against unknown attackers.

To improve the status quo, **we propose a feedback system that combines a safety cushion and various sensors based on real-time liquidity vectors to detect defects and respond in time to changes in the market.**

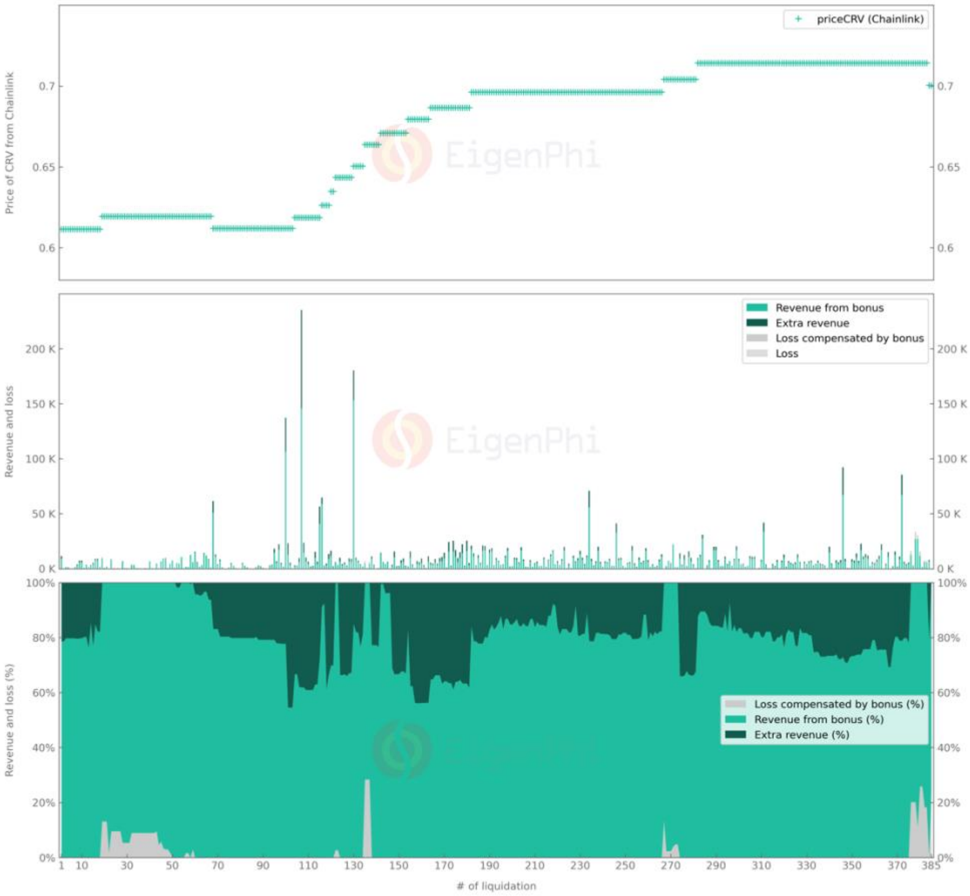
For example, in this case, there were more than 3 hours of response time between the two clearing batches. But the opportunity to recover losses is missed for no reason apart from the protocol relying on only a simple threshold design with the price referenced by that threshold being scalar and requiring a governance process to be updated. But if we consider price as a vector characterizing liquidity and introduce a contingency mechanism to deal with unexpected situations, the risk system will be more responsive and effective. We are committed to studying such events and building a generic risk control model. Feel free to discuss this with us.

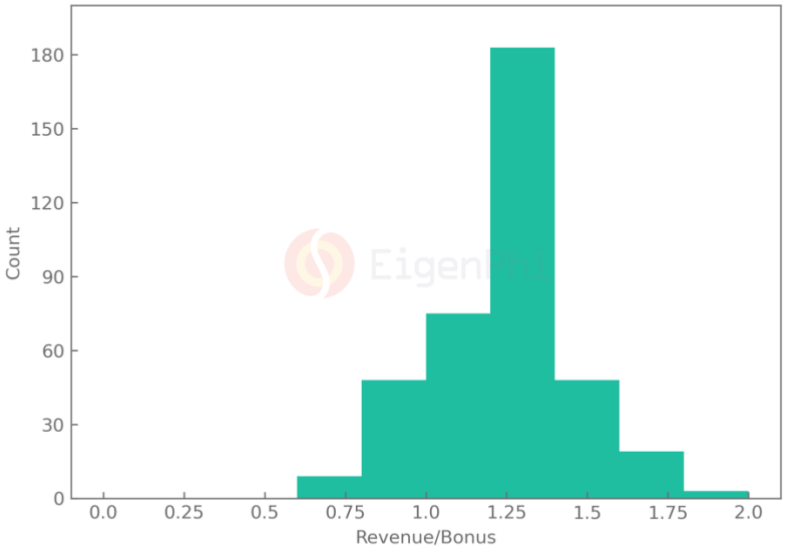
Liquidators' behavior and preferences

Finally, we have also provided some interested readers with information on the revenue and capital sources of the liquidators. But are not prepared to expand on the description. If you are interested, you can contact EigenPhi to discuss it with us.

Liquidators' revenue and loss

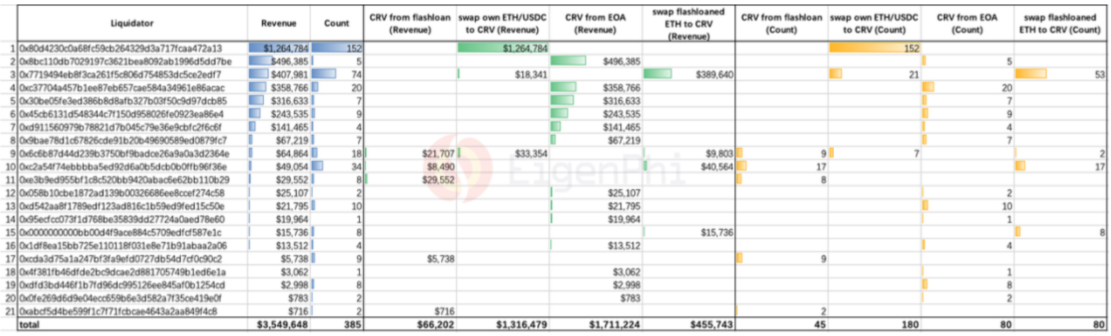
The following figure shows the revenue distribution over time and a breakdown of revenue contributed by the AAVE protocol's bonus or loss compensation bonus. Each liquidation received positive revenue before paying gas fees or miner tips to the validators.





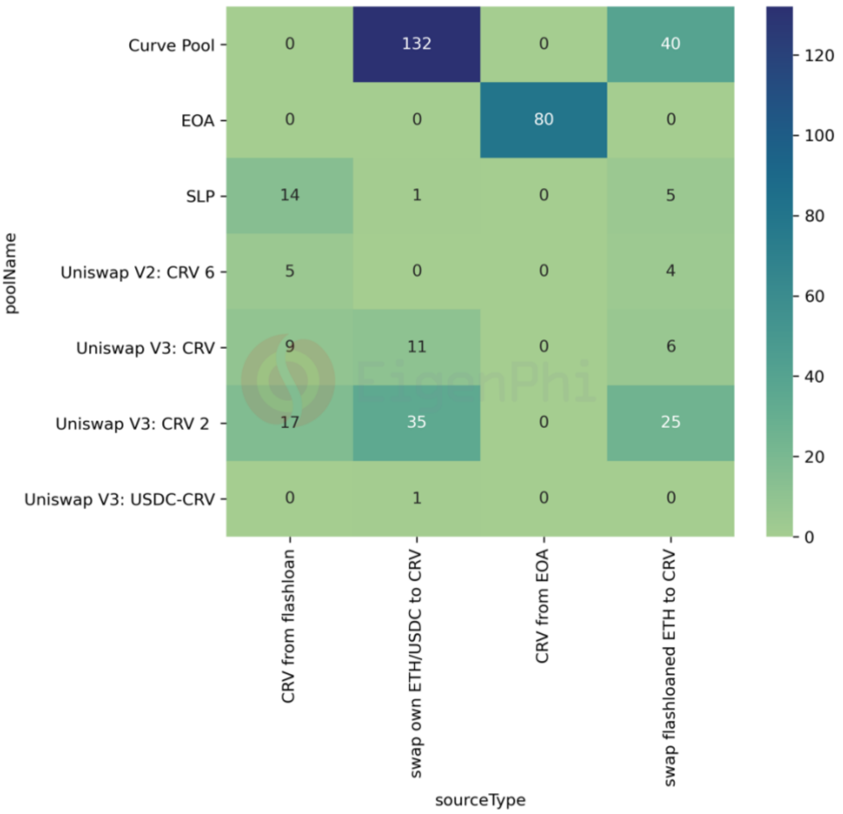
Source of capital

We also find the capital sources of each liquidation manually with the help of our visualization tool EigenTx. The results are shown in the following tables.



	Liquidator	Revenue	Count	CRV from flashloan (Revenue)	swap own ETH/USDC to CRV (Revenue)	CRV from EOA (Revenue)	swap flashloaned ETH to CRV (Revenue)	CRV from flashloan (Count)	swap own ETH/USDC to CRV (Count)	CRV from EOA (Count)	swap flashloaned ETH to CRV (Count)
1	0x80d4230c0a68fc59cb264329d3a717fcaa472a13	$1,264,784	152		$1,264,784				152		
2	0x8bc110db7029197c3621bea8092ab1996d5dd7be	$496,385	5			$496,385				5	
3	0x7719494eb8f3ca261f5c806d754853dc5ce2edf7	$407,981	74		$18,341		$389,640		21		53
4	0xc37704a457b1ee87eb657cae584a34961e86acac	$358,766	20			$358,766				20	
5	0x30be05fe3ed386b8d8afb327b03f50c9d97dcb85	$316,633	7			$316,633				7	
6	0x45cb6131d548344c7f150d958026fe0923ea86e4	$243,535	9			$243,535				9	
7	0xd911560979b78821d7b045c79e36e9cbfc2f6c6f	$141,465	4			$141,465				4	
8	0x9bae78d1c67826cde91b20b49690589ed0879fc7	$67,219	7			$67,219				7	
9	0x6c6b87d44d239b3750bf9badce26a9a0a3d2364e	$64,864	18	$21,707	$33,354		$9,803	9	7		2
10	0xc2a54f74ebbbba5ed92d6a0b5dcb0b0ffb96f36e	$49,054	34	$8,490			$40,564	17			17
11	0xe3b9ed955bf1c8c520bb9420abac6e62bb110b29	$29,552	8	$29,552				8			
12	0x058b10cbe1872ad139b00326686ee8ccef274c58	$25,107	2			$25,107				2	
13	0xd542aa8f1789edf123ad816c1b59ed9fed15c50e	$21,795	10			$21,795				10	
14	0x95ecfcc073f1d768be35839dd27724a0aed78e60	$19,964	1			$19,964				1	
15	0x000000000bb00d4f9ace884c5709edfcf587e1c	$15,736	8				$15,736				8
16	0x1df8ea15bb725e110118f031e8e71b91abaa2a06	$13,512	4			$13,512				4	
17	0xcda3d75a1a247bf3fa9efd0727db54d7cf0c90c2	$5,738	9	$5,738				9			
18	0x4f381fb46dfde2bc9dcae2d881705749b1ed6e1a	$3,062	1			$3,062				1	
19	0xdfd3bd446f1b7fd96dc995126ee845af0b1254cd	$2,998	8			$2,998				8	
20	0x0fe269d6d9e04ecc659b6e3d582a7f35ce419e0f	$783	2			$783				2	
21	0xabcf5d4be599f1c7f71fcbcae4643a2aa849f4c8	$716	2	$716				2			
	total	$3,549,648	385	$66,202	$1,316,479	$1,711,224	$455,743	45	180	80	80

The following figure shows the count of liquidations grouped by source types and source addresses.



Interesting transactions

CRV shorter's on-chain limit order during dumping

- https://etherscan.io/tx/0xf1324421f4444ee1a2d54301cc7e5405cd36fb79253287fa7f79ed8654f1cb31
- https://etherscan.io/tx/0x008b745ea488d78061c5533932c218940dd7707dc63949bb1b29602cd4554a94

CRV shorter attacked by sandwich during dumping

- https://eigenphi.io/mev/ethereum/eigentx/0x54c705bf70d55c96233e153d11ab33a1d7f0fa5e0800e42a1f04f9e858a662c7,0x3a5ebb5b76fcb6e0fbafa53ab1b8e6d62ee73dff90dba7b8d0a7b7caac57ecb3,0xae63aeb4dd7148aa446ab94b0a6f232d74eca71a07736922df09f251000db4ab

Liquidators attacked by sandwich

- https://eigenphi.io/mev/ethereum/eigentx/0x97ccb751af893a954fb95cbc2e03ab132b6320fa239fd2b7c093c74b02c9c86f,0xcebcdfc496d7adfeda347cbbcd6a6b11c0ba5ba4c472056d504b23735e033346,0x6588d2a264f4bacab9d805c40043d1f6cac338d033dbab1650defdbf7dacde3c
- https://eigenphi.io/mev/eigentx/0x2b6ba3ccab8e1919d1fc76ab8908a0b4bc6e480e6a6191b9d12506a094954237,0xca0de303ded3e9f91705799cef3fee0238ad2671fb24d24d8b61bf6cc205cb1c,0x6b076a76a00ef5151afcc2796e1d9896f4131c39c2d1c57a438b447d618026e9

Appendix

Appendix 1: CRV shorter's addresses

- Shorter's initial capital was from ponzishorter.eth: 0xADBaB4F38Ff9DCD71886f43B148bcad4A3081fB9
- The address used to dump the CRV market: 0x57E04786E231Af3343562C062E0d058F25daCE9E
- The intermediate address used to transfer CRV to OKX: 0xBA529566855d9d0Bf3De1cc988E5f529F92Bd80C

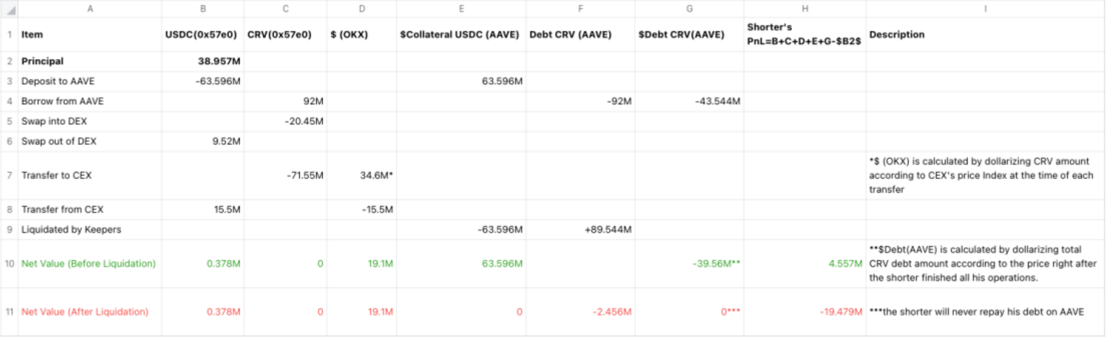
Appendix 2: Tx records of CRV from 0x57e0's related address 0xba52 to OKX

- https://etherscan.io/address/0xBA529566855d9d0Bf3De1cc988E5f529F92Bd80C#tokentxns

Appendix 3: Tx records of USDC transferred back to 0x57e0 through Circle

- Circle's contract: 0x55fe002aeff02f77364de339a1292923a15844b8
- 10M: 0x5dca0eb6cf8cea08abe48e64c0fee6ba0888874849d8728781c78b197c756908
- 5.5M: 0x3bad26dac3c13f7f8bcbae4f45a61bd25f1ea589aa333032a5095558cf1571fc

Appendix 4: A calculation of CRV shorter's PnL before and after liquidation



	A	B	C	D	E	F	G	H	I
1	**Item**	**USDC(0x57e0)**	**CRV(0x57e0)**	**$ (OKX)**	**$Collateral USDC (AAVE)**	**Debt CRV (AAVE)**	**$Debt CRV(AAVE)**	**Shorter's PnL=B+C+D+E+G-$B2$**	**Description**
2	**Principal**	**38.957M**							
3	Deposit to AAVE	-63.596M			63.596M				
4	Borrow from AAVE		92M			-92M	-43.544M		
5	Swap into DEX		-20.45M						
6	Swap out of DEX	9.52M							
7	Transfer to CEX		-71.55M	34.6M*					*$ (OKX) is calculated by dollarizing CRV amount according to CEX's price Index at the time of each transfer
8	Transfer from CEX	15.5M		-15.5M					
9	Liquidated by Keepers				-63.596M	+89.544M			
10	Net Value (Before Liquidation)	0.378M	0	19.1M	63.596M		-39.56M**	4.557M	**$Debt(AAVE) is calculated by dollarizing total CRV debt amount according to the price right after the shorter finished all his operations.
11	Net Value (After Liquidation)	0.378M	0	19.1M	0	-2.456M	0***	-19.479M	***the shorter will never repay his debt on AAVE

Disclaimer

The "Information" contained in this post has been prepared solely for informational purposes, is in summary form, and does not purport to be complete. The Information is not, and is not intended to be, an offer to sell, or a solicitation of an offer to purchase, any securities. The Information does not provide and should not be treated as giving investment advice. The Information does not take into account specific investment objectives, financial situation or the particular needs of any prospective investor. No representation or warranty is made, expressed or implied, with respect to the fairness, correctness, accuracy, reasonableness or completeness of the Information.

We do not undertake to update the Information. It should not be regarded by prospective investors as a substitute for the exercise of their own judgment or research. Prospective investors should consult with their own legal, regulatory, tax, business, investment, financial and accounting advisers to the extent that they deem it necessary, and make any investment decisions based upon their own judgment and advice from such advisers as they deem necessary and not upon any view expressed herein.

*We are open to discussion. Please feel free to contact us via contact@eigenphi.com.

EigenPhi

WISDOM OF DEFI

https://www.eigenphi.io/

@eigenphi

contact@eigenphi.com