

# Blockchain Security Incident Analysis Report

Arthur Xia  
arthurxia.career@gmail.com  
2023/06

- Neoteric Finance – [Page 2](#)

TL; DR:

The Neoteric platform combines the token mechanics of RFI and LIQ to provide a frictionless yield generation and perpetual liquidity meta-market-making mechanism, which takes a 10% tax from every transaction to distribute holders. There were multiple rug pulls on token \$NTRC, and the rug puller made nearly 660 \$BNB profit on one rug pull on July 27, 2022. The project is currently inactive.

- Nirvana Finance – [Page 20](#)

TL; DR:

Nirvana is a Defi 3.0 investment protocol for a sustainable store of wealth. Its primary token is \$ANA. On July 28th, 2022, Nirvana Finance was exploited via a flash loan attack with the attacker profiting about \$3,574,635. The stolen funds have been bridged from the Solana network to the Ethereum wallet.

# Neoteric Finance

## 1/ Project Info:

### 1. Project Introduction:

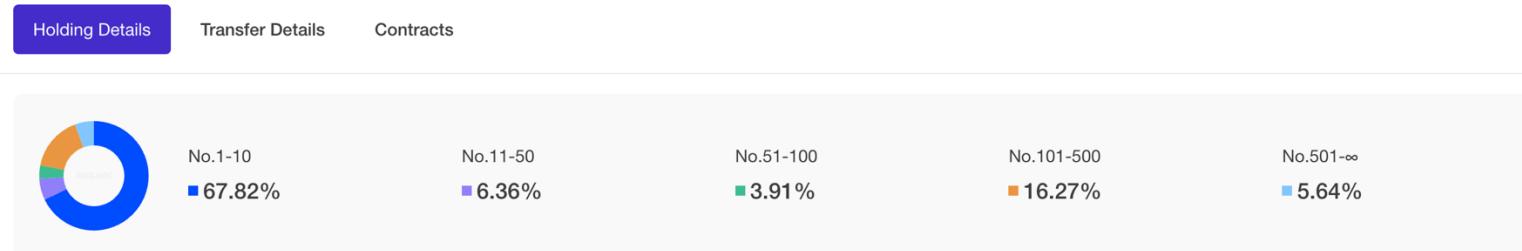
Neoteric is a soft fork of the RFI and Liquid on ERC-20. It has essentially the combination of token mechanics of RFI and LIQ, which includes a frictionless Yield Generation(Hold and Earn) and perpetual liquidity meta-market-making mechanism that grows liquidity as more trades are executed. These mechanisms take a 10% tax from every transaction and use these taxed tokens to distribute among holders and at the same time generate liquidity pool tokens.[\[1\]](#)

Neoteric is one such crypto with no one to identify as being in charge, it could be anyone responsible for it. There is very little information about the token at all. There is also no whitepaper for Neoteric. [\[2\]](#)

### 2. Token Info: \$NTRC

- Coinmarketcap: <https://coinmarketcap.com/currencies/neoteric/>
- Contract: `0x733A90389db7d9c246D064A257E5652f7Be36B8A`[\[3\]](#)
- Contract Source Code:  
<https://bscscan.com/token/0x733A90389db7d9c246D064A257E5652f7Be36B8A#code#L1> (No Contract Security Audit Submitted)

Holding details: Current Supply is 500.0M with 3,726 addresses holding \$NTRC[\[4\]](#).

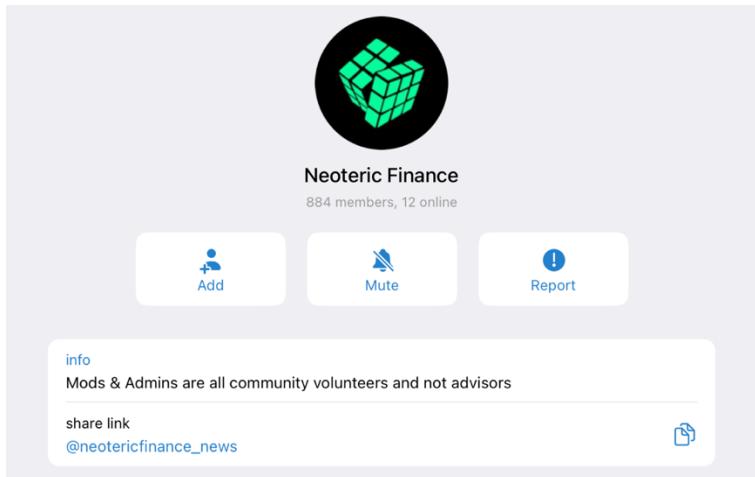


### 3. Community:

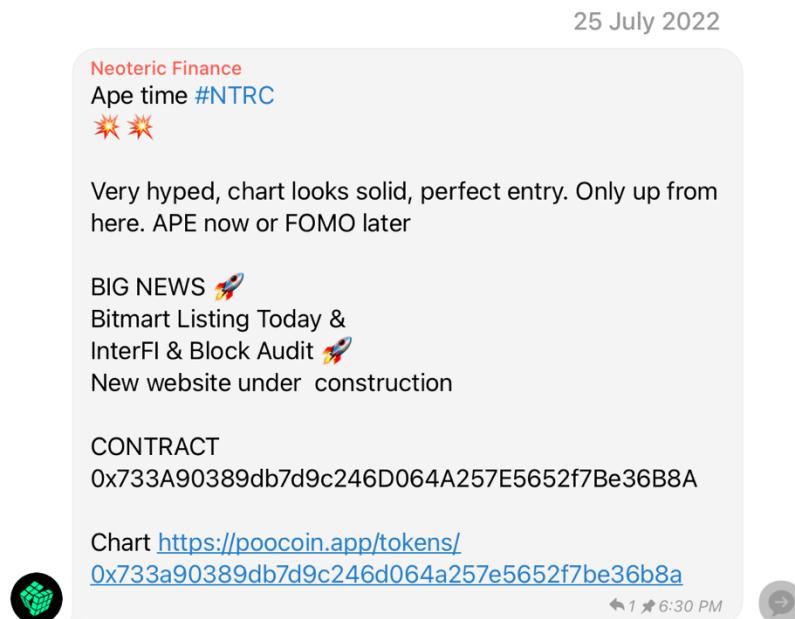
- Official Website: <https://www.neoteric.finance/> (unavailable now)
- Twitter: <https://twitter.com/neotericfinance>
  - They last posted on Jul 15, 2022, and there are 809 Followers, 0 Following. There are only 3 posts now and looks like they deleted the rest of them. The first two tweets had very little interaction, mostly under 10. While the third tweet which is also the latest one had a lot of interaction, with 40

replies, four times as many as the previous two posts, and most of the comments were negative complaints about the project.<sup>[6]</sup>

- c. Telegram: [https://t.me/neotericfinance\\_news](https://t.me/neotericfinance_news)
  - 1. Official channels no longer show any other social media, and a telegram search turned up what appeared to be the former official community. There are 884 members in it.



- 2. From 5 pinned messages in the Telegram group, we can find that \$NTRC was going to be listed on BitMart Exchange<sup>[7]</sup> on 25 July 2022.
  - \* Information about the listing could not be found on BitMart's official media.



#### 4. Project Team Info:

No information about the project team can be found.

## 2/ Related Incident or Scam

### 1. Incident 1 on July 19, 2022

#### a. General info:

According to Certik Alert<sup>[8]</sup>, there was a rug pull on July 19, 2022. And the price of \$NTRC dropped over 91.6%, and at that time reports showed losses at approximately \$100k and still increasing<sup>[9]</sup>.



CertiK Alert ✅ 🚨  
@CertiKAlert

...

#CommunityAlert 🚨

We are seeing a #rugpull on project @neotericfinance - symbol \$NTRC that led to a slippage of >91.6%.

Current reports show losses at approximately \$100k but are increasing.

[bscscan.com/token/0x733a90...](https://bscscan.com/token/0x733a90...)

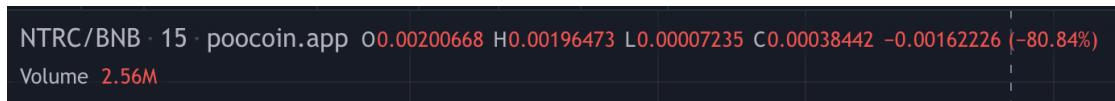
Stay safe out there!



6:56 PM · Jul 19, 2022

### b. Details:

According to PopCoin Charts<sup>[10]</sup>, on 19 July 2022, at around 21:15 UTC, the trading volume suddenly jumped, and the total trading volume reached 2.56M in 15 minutes, 100k times the average level. The price also lost 80% of its value in 15 minutes.



But according to the chart, this is not the first time such a rapid decline has happened, that also happened on July 15<sup>th</sup> and July 16<sup>th</sup>.

There are three main types of rug pulls in crypto: liquidity stealing, limiting sell orders, and dumping. This should be a dumping.

Due to insufficient liquidity and excessive concentration of token holdings when the whales leave the field or the project side to ship the moment such phenomenon. It is worth noting that on the following day, the price recovered its original level and broke through the record high.

## 2. Incident 2 on July 27, 2022

### a. General info:

According to the official Twitter of PeckShieldAlert<sup>[11]</sup>, they found that there was a rug pull on July 27, 2022<sup>[12]</sup>.

'The price of \$NTRC dropped about 80%, and about 660 \$BNB was stolen to the address of 0x6E9afD530416FC332d47939463C292d9062209b1' <sup>[13]</sup>



12:13 AM · Jul 27, 2022

### Alert Detail

Alert ID :	896d68e3-5ce6-7274-f5c4-cfa4889bea95
Network :	BSC
Alert Name :	Slippage
Description :	NTRC Price : \$0.00424045, Drop: -83.48%
Severity :	Medium
Type :	Vigilant
Contract :	0x733a90389db7d9c246d064a257e5652f7be36b8a ( NTRC )
Timestamp :	07/27/2022 01:10:26 AM +UTC
Transaction Hash :	0x1149ca44542d302f48898e1335dd637b3042391b6839763f78e6c3abb168b117
Address :	0x733a90389db7d9c246d064a257e5652f7be36b8a

Alert Detail from PeckShieldAlert<sup>[14]</sup>

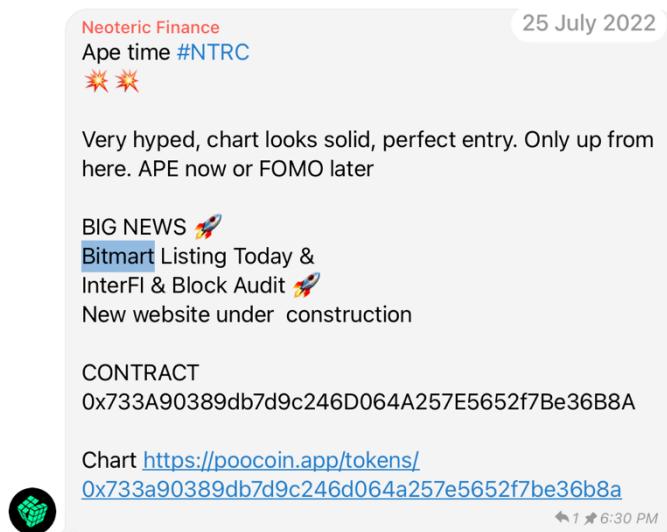
## b. Details:



Since July 25, the price of the currency has continued to rise. The increase reached about 6,000%.

The pull-up coincided with the official announcement that \$NTRC would be listed on BitMart.

Details of \$NTRC cannot be obtained from other official sources. It is worth mentioning that a BitMart account @Jim\_er in the group is officially certified as Senior BD Manager (Telegram).



Neoteric Finance  
882 members, 17 online

bitmart

Jim Bitmart  
@Jim\_er

Neoteric.finance @neotericfinance · Jul 15, 2022 · #LFG #NTRC

Just in 1 day we got to 800k mcap! #bsc #bscgem #BSCGemAlert

Next target 10 mil mcap and Dashboard live.

40 6 22

Jim\_Bitmart ✅  
@Jim\_Bitmart

Hi, this is Jim, I am the Senior Listing Manager from BitMart.  
We would like to communicate with you about cooperation and listing on BitMart Exchange.  
Looking forward to receiving your feedbacks. Thank you!

jim@bitmart.com

10:37 AM · Jul 16, 2022

Senior BD manager(Telegram)

The @Jim\_er you inquired is Senior BD manager(Telegram)

To prevent fraud in the name of BitMart, you can confirm whether the channel is an official channel or not. Including but not limited to Twitter, Facebook, Telegram, Medium, YouTube, Instagram, LinkedIn, Reddit, Phone number and WeChat account.

Please note that BitMart works with Listing Partners to identify quality tokens and assets. However, Listing Partners are not employees or representatives of BitMart, and are not authorized to enter any contracts or accept any payments on behalf of BitMart.

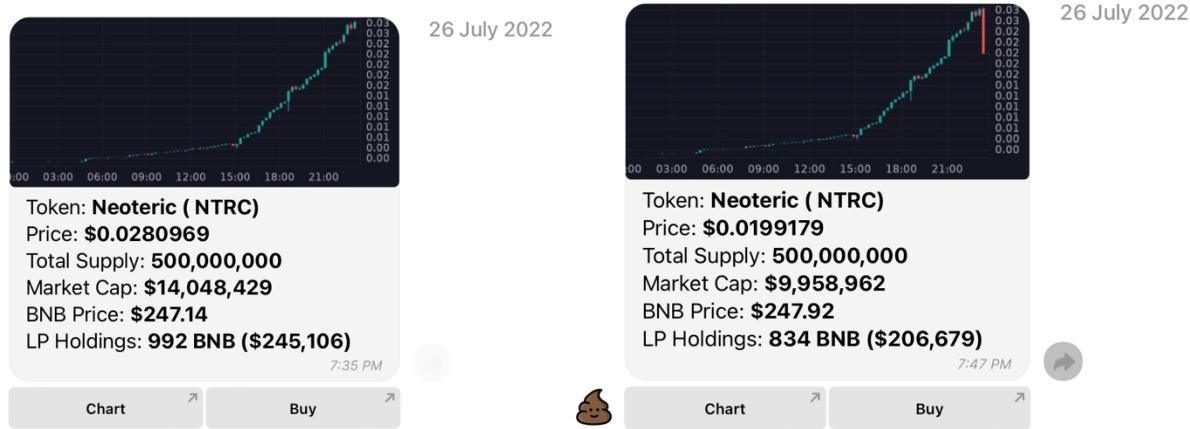
This account may be owned and operated by an external party not affiliated with BitMart. You should only trust our official account ending in bitmart.com to transmit legally binding agreement, information about your assets and wallet addresses, or other confidential information.

Confirm

BitMart Official Verification [\[15\]](#)

And Jim did leave a message on his official Twitter account asking for cooperators. [\[16\]](#)

BitMart [\[17\]](#) is a third-tier exchange that officially has more than 9 million users. It cannot be ruled out that the price pull is due to positive information and exchange liquidity.



Around 11:30 PM UTC on July 26, the LP flow pool reached 990+ \$BNB. Then the LP flow pool began to descend.



According to PopCoin Charts<sup>[18]</sup>, on 26 July 2022, at around 23:50 UTC, the price began a sustained flash crash, over 85% in one hour.

	0xd88daeb7dd8986ed57...	Transfer	19902660	309 days 21 hrs ago	0xe70f2c9cd6b585f44f8...		0x6e9af530416fc332d4...	0.055568245472683 BNB	0.0001155
	0x08800515c3757844cc...	Transfer	19902660	309 days 21 hrs ago	0x7465f2c76541c14679...		0x6e9af530416fc332d4...	0.067695805553546 BNB	0.0001155
	0xe38f22123bc7bf7a4a2...	Transfer	19902660	309 days 21 hrs ago	0x8696ce7ecbb67734c4806f6148e8c1133e98...		0x6e9af530416fc332d4...	0.087100943166381 BNB	0.0001155
	0x9cf51033f8bcabd83a0...	Transfer	19902660	309 days 21 hrs ago	0x7ebcb419f25bd3ffba7...		0x6e9af530416fc332d4...	0.088389648527616 BNB	0.0001155
	0x3a8413658cc72ce7b7...	Transfer	19902660	309 days 21 hrs ago	0x5b47f59a9a57024f87b...		0x6e9af530416fc332d4...	0.022298763868673 BNB	0.0001155
	0x912cc9f8693fd233d2b...	Transfer	19902660	309 days 21 hrs ago	0x082b9ca7578f588269...		0x6e9af530416fc332d4...	0.008480210726489 BNB	0.0001155
	0x994d34700acf2db361...	Transfer	19902660	309 days 21 hrs ago	0xc11bc381d875369a0c...		0x6e9af530416fc332d4...	0.030861704193367 BNB	0.0001155
	0xe51d338c21314880c2...	Transfer	19902659	309 days 21 hrs ago	0x978aeddaad25c4973c...		0x6e9af530416fc332d4...	0.055601877745801 BNB	0.0001155
	0x1f3a2f10267e2c6e277...	Transfer	19902659	309 days 21 hrs ago	0x6ef69a0468ea2b5d2e...		0x6e9af530416fc332d4...	0.079841778627827 BNB	0.0001155
	0x74875205bcaa2d8c1c7...	Transfer	19902659	309 days 21 hrs ago	0xb08caa88f6b738adfd8...		0x6e9af530416fc332d4...	0.100508372674348 BNB	0.0001155
	0xf84506bb3edc9e3a6e...	Transfer	19902659	309 days 21 hrs ago	0xae8253d475091e5168...		0x6e9af530416fc332d4...	0.00927302157454 BNB	0.0001155
	0xa8761b2408db965746...	Transfer	19902659	309 days 21 hrs ago	0xc0183531f26779c5dd...		0x6e9af530416fc332d4...	0.007500187696769 BNB	0.0001155
	0xe61cd2ad76d53f1219f4...	Transfer	19902659	309 days 21 hrs ago	0x40468dee214c7016d5...		0x6e9af530416fc332d4...	0.020320506279505 BNB	0.0001155
	0xfeaa8329de1a2b6f5df...	Transfer	19902659	309 days 21 hrs ago	0xa9f10ceca60704b969...		0x6e9af530416fc332d4...	0.01249991152798 BNB	0.0001155
	0x3c56be1bb6567aacb6f...	Transfer	19902659	309 days 21 hrs ago	0xd07c777a8cf538157d...		0x6e9af530416fc332d4...	0.012447069618472 BNB	0.0001155
	0x70ccb9d7897b0e023c...	Transfer	19902659	309 days 21 hrs ago	0xe1f17273d2302524ab...		0x6e9af530416fc332d4...	0.152417293581722 BNB	0.0001155
	0xe5b5d1e3be172b2b52...	Transfer	19902659	309 days 21 hrs ago	0x597351095ca5050a80...		0x6e9af530416fc332d4...	0.060549273092919 BNB	0.0001155
	0x67d57af9d98dec(ccd7a...	Transfer	19902658	309 days 21 hrs ago	0x0018b1ab95cfbc2b2e...		0x6e9af530416fc332d4...	0.177472670054003 BNB	0.0001155
	0xfe28292eeb9dd94593f...	Transfer	19902658	309 days 21 hrs ago	0x0046db013de12d144d...		0x6e9af530416fc332d4...	0.024241642063733 BNB	0.0001155
	0x8cec40193e7bd8bf...	Transfer	19902658	309 days 21 hrs ago	0x9a34e53e10f85a1319...		0x6e9af530416fc332d4...	0.09883440088711 BNB	0.0001155
	0x71a3b8e9718d8ee5fd...	Transfer	19902658	309 days 21 hrs ago	0xcf2237c884ca348780...		0x6e9af530416fc332d4...	0.023863867428306 BNB	0.0001155

On-chain data shows that account theft

**0x6E9afD530416FC332d47939463C292d9062209b1**[\[19\]](#) started gathering \$BNB on July 27, 12:50:23 AM UTC.

According to BscScan data, the account received a total of 658.90 \$BNB in 510 transactions at a price of \$271.71/BNB that day.

The total value is approximately \$179,029.7.

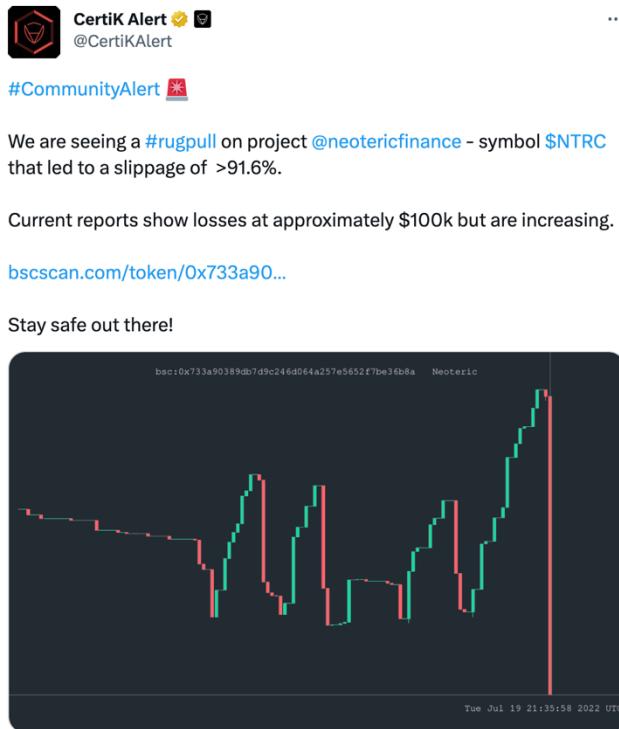
Then the LP pool was quickly drained.

There are three main types of rug pulls in crypto: liquidity stealing, limiting sell orders, and dumping. This should be liquidity stealing.

## 2/ Alerts

### 1. Incident 1 on July 19, 2022

The incident was first reported by Certik Alert [\[20\]](#).



6:56 PM · Jul 19, 2022

Some media reported the incident later:

#### 1) Binance [\[21\]](#)

A screenshot of a news article from Binance's website. The header includes the Binance logo, navigation links like "Buy Crypto", "Markets", "Trade", "Derivatives", "Earn", "Finance", "NFT", "Institutional", and "Feed", and a yellow banner encouraging users to "Register now and get verified - Enjoy Welcome Rewards up to \$100!". The main headline is "Security Team: Rug Pull at Neoteric.finace, loss of at least \$100,000". Below the headline is the timestamp "Binance 2022-07-19 21:56". A disclaimer states: "Full disclaimer: This platform includes third party opinions. We do not endorse their accuracy. Digital asset prices can be volatile. Do your own research. See full terms [here](#)." The article summary reads: "According to the monitoring released by CertiK on Twitter, a Rug Pull occurred in Neoteric.finace, and the price of its NTRC token fell by more than 91.6%. Current reports put the damage at around \$100,000, but still mounting. Please be vigilant."

## 2) PANews<sup>[22]</sup>

The screenshot shows the PANews website interface. At the top, there is a navigation bar with links for 'front page', 'depth', 'Newsletter' (which has a 'NEW' badge), 'Topic', 'column', and 'calendar'. Below the navigation is a search bar labeled 'Discover'. The main content area features a bold headline: 'Security Team: Rug Pull occurred in both Neoteric.finance project and ORCHID project'. Below the headline is a timestamp 'PA Frontline | 2022-07-19 22:25'. To the left of the timestamp are four circular icons with symbols: a heart, a star, a document, and a refresh. The main text of the article discusses two projects experiencing Rug Pulls, with token price drops of over 90% and losses of around \$100,000. A blue link 'Original link' is at the bottom.

front page depth Newsletter Topic column calendar

navigation Discover NEW

### Security Team: Rug Pull occurred in both Neoteric.finance project and ORCHID project

PA Frontline | 2022-07-19 22:25

According to news from PANews on July 20, according to CertiK monitoring, both the Neoteric.finance project and the ORCHID project had Rug Pulls. Among them, the NTRC token price of Neoteric.finance fell by more than 91.6%, and the current report shows that the loss is about 100,000 US dollars. The ORCHID token price of the ORCHID project fell by more than 96.4%, and the current report shows a loss of about \$50,000.

[Original link](#)

## 3) CNYES From Golden Finance<sup>[23]</sup>

The screenshot shows the CNYES From Golden Finance website. At the top, there is a 'Newsletter' button. The main headline is 'Security Team: Rug Pull at Neoteric.finance, loss of at least \$100,000'. Below the headline is a timestamp 'Golden Finance 2022/07/19 21:30'. To the right are social media sharing icons for Facebook, Twitter, and LinkedIn. The main text of the article discusses a Rug Pull at Neoteric.finance, with the NTRC token price falling by over 90% and losses reaching around \$100,000. On the right side of the article, there is a 'Editor's Choice' section with a thumbnail for 'U.S. Stocks Morning' and a small image of a person. Below the article, there is a link to 'Lululemon shares soar as'.

Newsletter

### Security Team: Rug Pull at Neoteric.finance, loss of at least \$100,000

Golden Finance 2022/07/19 21:30

f Aa

On July 20th, according to CertiK monitoring, Neoteric.finance had a Rug Pull, and its NTRC token price fell by more than 91.6%. Current reports put the damage at around \$100,000, but still mounting. Please be vigilant.

Editor's Choice see more ►

<U.S. Stocks Morning> U.S. stocks strengthened thank... 09:41

Lululemon shares soar as

## 4) Bihai123<sup>[24]</sup>

The screenshot shows the Bihai123 website. At the top, there is a logo for '币海财经 Bihai23.com' and a navigation bar with links for 'front page', 'global information', '24H Newsletter' (which is highlighted in red), 'economic calendar', 'Binhai Audiovisual', 'circle', and 'quotes'. Below the navigation is a breadcrumb trail: 'Home > News > Blockchain > Security Team: Neoteric.finance has a Rug Pull and lost at least \$100,000'. The main content area shows a timestamp 'Tuesday, July 19' and a time '09:22'. A blue circle indicates a new item. The headline is 'Security Team: Rug Pull at Neoteric.finance, loss of at least \$100,000'. The text of the article discusses the same event as the other sources, mentioning a Rug Pull at Neoteric.finance and significant token price drops. There is also a 'share' button at the bottom.

front page global information 24H Newsletter economic calendar Binhai Audiovisual circle quotes

Home > News > Blockchain > Security Team: Neoteric.finance has a Rug Pull and lost at least \$100,000

Tuesday, July 19

09:22 • Security Team: Rug Pull at Neoteric.finance, loss of at least \$100,000

[Security Team: Rug Pull at Neoteric.finance, loss of at least \$100,000] According to news on July 20, according to CertiK monitoring, a Rug Pull occurred at Neoteric.finance, and the price of its NTRC token fell by more than 91.6%. Current reports put the damage at around \$100,000, but still mounting. Please be vigilant.

share

## 5) Zcuc [25]

The screenshot shows a news article titled "Security Team: Rug Pull occurred in both Neoteric.finance project and ORCHID project". The article discusses a price drop for both projects, with the NTRC token falling by over 91.6% and the ORCHID token by over 96.4%. Below the article, there is a timestamp of July 20, 2022, at 11:07 am, and sharing options for social media.

\*Many other media reported on this incident. Not all of them are listed here.

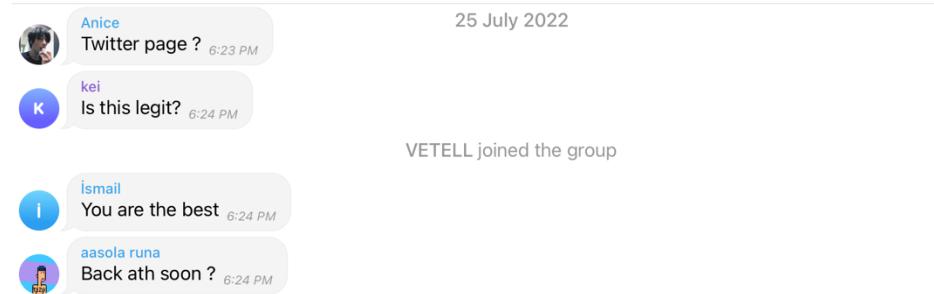
- 6) For Telegram Group, officials shut down the group chat function on July 19. In addition, an official telegram message on July 20 appeared to reply to the flash crash on July 19. But it's worth noting that on July 20, the price had returned to normal.

Officials explained that the plunge was probably due to the departure of the whales. They also encouraged holders and community participants to continue to build and maintain confidence in the project.

The group chat function was not officially opened until July 25.

The screenshot shows a Telegram group chat. On July 17, Neoteric Finance pinned a message stating "Chat is closed for next few hours until new mod starts thanks everyone". On July 19, Neoteric Finance pinned a message saying "Chat is closed for next few ho...". On July 20, Neoteric Finance pinned a message about big whales leaving and continuing growth, followed by Marketing has started LFG, a new website under construction, and 16% slippage. A user named শাফিউল joined the group, and a Deleted Account joined the group. The last message is from Charts /price.

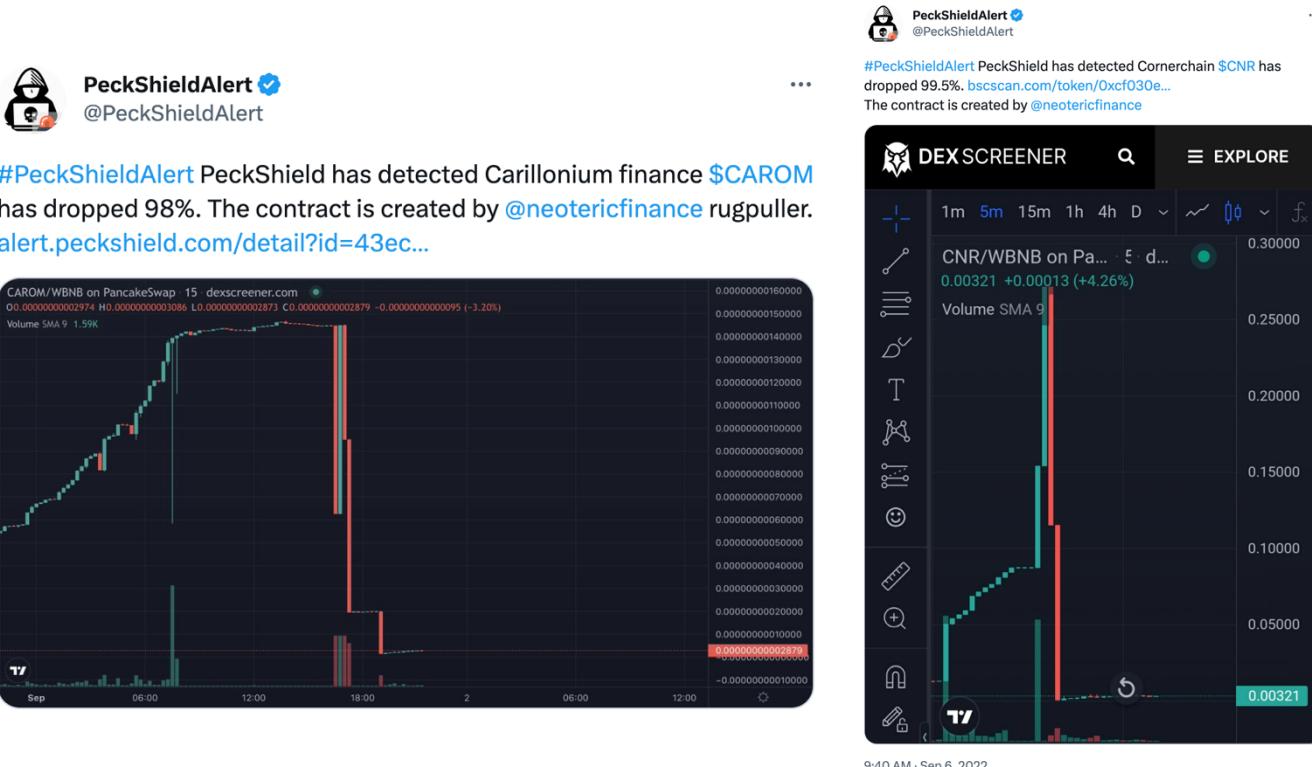
The level of activity and daily interaction in the group remained positive after the chat reopened, and it seemed that the flash collapse on July 19 did not negatively impact the community.



Just a day later, another even bigger rug pull occurred.

\*In a very interesting point, the rug puller made some other rug pulls on September 2022.

- [1] <https://twitter.com/PeckShieldAlert/status/1567145660000108544>
- [2] <https://twitter.com/PeckShieldAlert/status/1565336312218955776>



## 2. Incident 2 on July 27, 2022

The incident was first reported by PeckShieldAlert[\[26\]](#).



Some media reported the incident later:

### 1) Dragonfly Finance[\[27\]](#)

⌚ 7x24h newsletter

⌚ Today, Wednesday, June 2, 2023

07-27 15:47

#### Security Team: Rug Pull occurred in Neoteric.finance and lost about 660 BNB

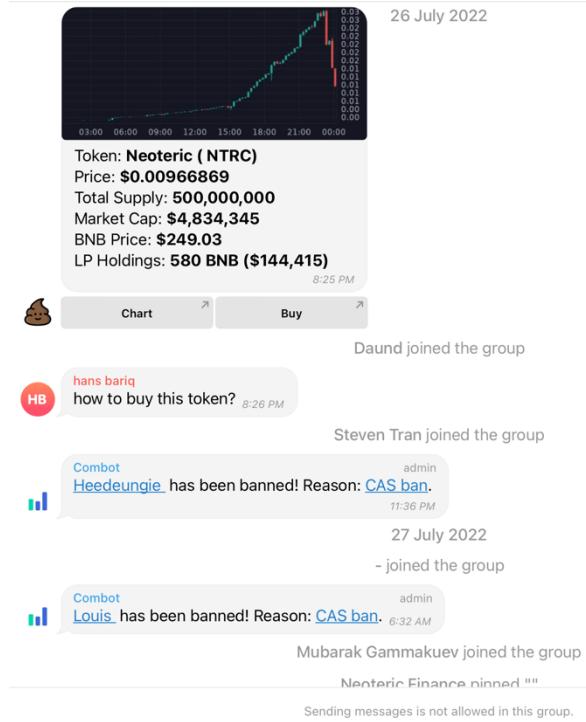
According to online media reports, according to monitoring by PieDun, a Rug Pull occurred in Neoteric.finance, and its token NTRC fell by more than 80%. The stolen funds are approximately 660 BNB and are currently located at this address: 0x6E9afD530416FC332d47939463C292d9062209b1.

generate image

## 2) BitChecker[28]



- 3) The official telegram group chat appears to have banned its members from speaking after the incident. There were no alerts or comments on the event in the Telegram.



## 4/ The Funds

### 1. Incident 1 on July 19, 2022

According to the Certik Alert [\[29\]](#), although the reports indicated losses of around \$100k, they were not entirely accurate.

The whereabouts of the money are also unclear.

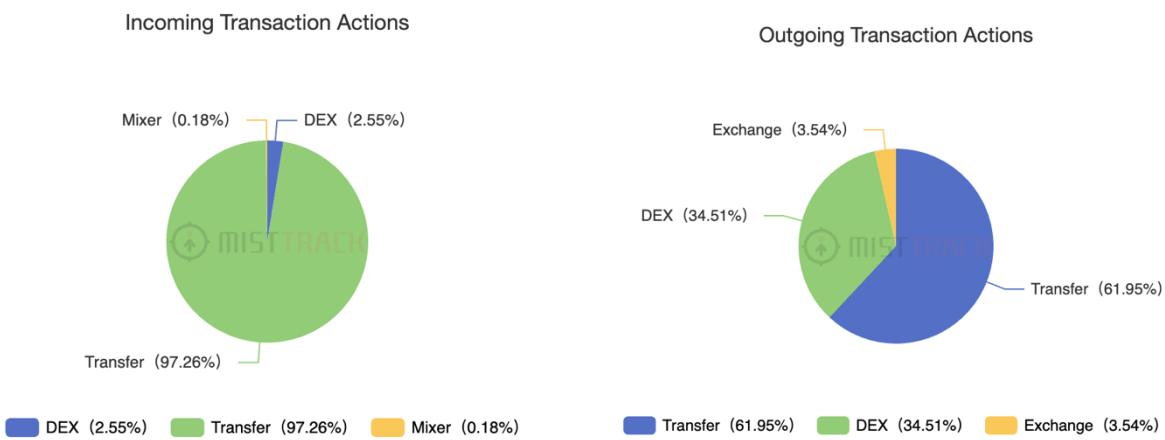
### 2. Incident 2 on July 27, 2022

According to the PeckShieldAlert [\[30\]](#):

*'Stolen funds (~660 \$BNB) currently sit in 0x6E9afD530416FC332d47939463C292d9062209b1'. [\[31\]](#)*

The account received a total of 658.90 \$BNB (\$179,029.7) by BscScan, and the current balance at this address is \$126.

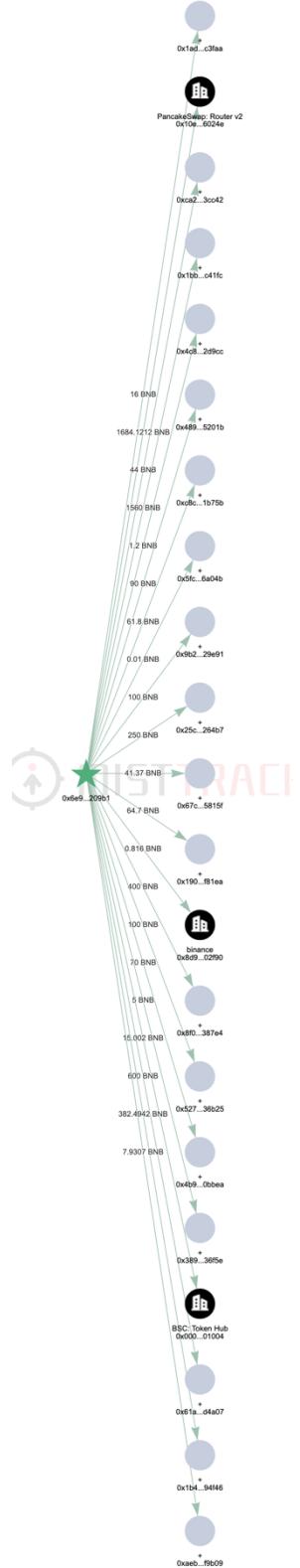
From the transaction records, the address did not put the obtained illegal tokens into the mixer like Tornado Cash but continued to use the address normally until October 2022. Although there have been three transactions since 2023, all of them have accepted worthless tokens and do not appear to be active transactions.



From the point of view of the outgoing transaction address, there are three types: exchange, DEX, and private address. [\[32\]](#)

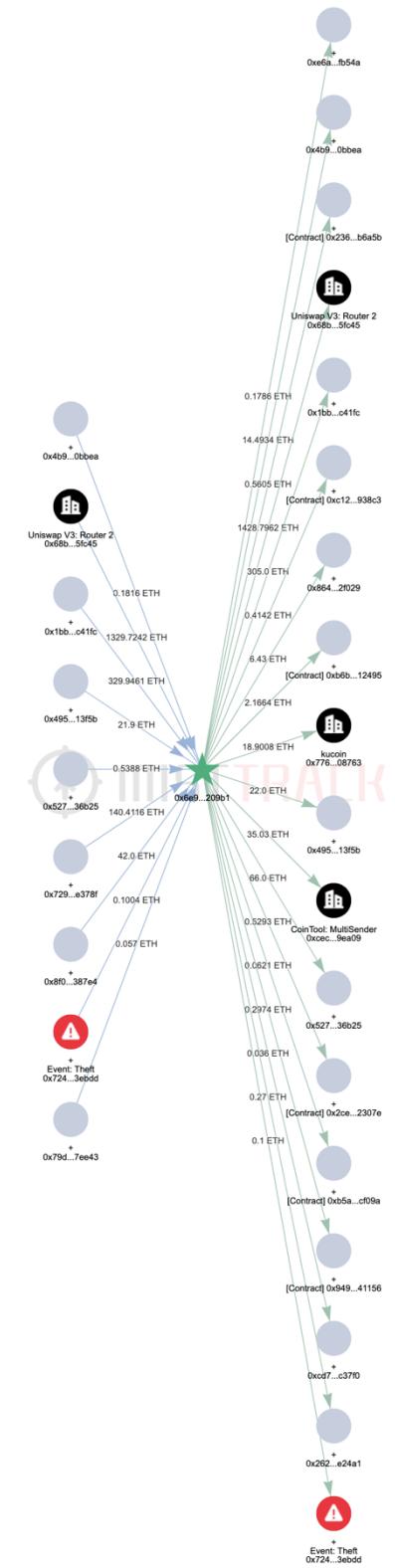
Here are all the associated BSC addresses [33]:

0x1addee6afa1523e961f84e9d0a8e2990072fc3faa  
0x10ed43c718714eb63d5aa57b78b54704e256024e (*PancakeSwap*)  
0xca2352383477b20228e075f12068181c2593cc42  
0x1bb2d2b396edc607ce8149820ad7c121aa6c41fc  
0x4c8608dfa3fa8617599b38983b57f0210192d9cc  
0x489d2b8c7fa7f58a1ebe7b7b1d5be24b0f05201b  
0xc8c55fee1ff3f1ec2d25b9c9abe43ccc67b1b75b  
0x5fc9ec39b601238ef32a31075dfb8a772366a04b  
0x9b28e5a35eb7f121792f56a26c04415f09f29e91  
0x25c47b48ef1f64dce9db7b5da9791e3a69a264b7  
0x67cd006ba2d66e564a551240a02e1c8be9c5815f  
0x190364cd29f19b7f295effea1e57180845ef81ea  
0x8d9a21da7c6e16b06e3c3bda918a344afba02f90 (*Binance*)  
0x8f0d9acb433ca1c0f214990c4c908f2aa12387e4  
0x527f0772eb635cd7ef8a6d8fc3aec781fa36b25  
0x4b9818718090dc53837485726c7ac094bb30bbea  
0x389fce409fa4e86f5b7afe54ea1c54e553336f5e  
0x0001004 (*BSC Token Hub*)  
0x61ac622c4a311c3d22f613933713de167e3d4a07  
0x1b44dd67cdd0d725129cdddca2ae5db239594f46  
0xaeb17c2f7b833c0ad117c476edf30059f50f9b09



Here are all the associated BSC addresses<sup>[34]</sup>:

0x4b9818718090dc53837485726c7ac094bb30bbea  
 0x68b3465833fb72a70ecdf485e0e4c7bd8665fc45 (Uniswap V3)  
 0x1bb2d2b396edc607ce8149820ad7c121aa6c41fc  
 0x49537cf4fb5318f4a18b74cd7fb28ccf6213f5b  
 0x527f0772eb635cd7ef8a6d8fc3aeec781fa36b25  
 0x7292494a3399550add20359e922f0da574e378f  
 0x8f0d9acb433ca1c0f214990c4c908f2aa12387e4  
 0x724b43a61c0a8c2f9b5e776680537db4d723ebdd (Theft Address)  
 0x79d396e4281079ca5622563875547085f4d7ee43  
 0xe6a883eea2701e1c725c15bf22de20dc306fb54a  
 0x4b9818718090dc53837485726c7ac094bb30bbea  
 0x236db07167ec97c93fb6c6318f2d6c9dd2ab6a5b (Contract)  
 0x1bb2d2b396edc607ce8149820ad7c121aa6c41fc  
 0xc1200eded3929dca039c5bb05439499a50e938c3  
 0x8649a3231ed806b66d55f0b42d0a4d2abc52f029  
 0xb6b05562ae4181aff8edef6547412a47bdf12495 (Contract)  
 0x776d6125735b5b02d5cee565d8ffe02d71608763 (Kucoin)  
 0x49537cf4fb5318f4a18b74cd7fb28ccf6213f5b  
 0xec8f07014d889442d7cf3b477b8f72f8179ea09 (CoinTool)  
 0x527f0772eb635cd7ef8a6d8fc3aeec781fa36b25  
 0x2cea46d3caf451387e852d7c1b8159268d82307e (Contract)  
 0xb5ad91f6573eb328549fe84c820626c078dcf09a (Contract)  
 0x9494b8319e16fe204f46f8791d3497d25c041156 (Contract)  
 0xcd762242768ed31b0fa0d9671f43b449629c37f0  
 0x262fd74bfcc98baebac5b0e2f87b0a6200be24a1  
 0x724b43a61c0a8c2f9b5e776680537db4d723ebdd (Theft Address)



# Nirvana Finance

## 1/ Project Info:

### 1. Project Introduction[\[35\]](#):

Nirvana is an investment protocol for a sustainable store of wealth with Defi 3.0. Its primary token \$ANA is a new asset class that features:

- Bounded risk through partial collateralization. The \$ANA token cannot go to zero, and its minimum price rises monotonically with demand.
- Ultra-low-risk backing value via diversified stablecoin reserves. \$ANA protects its holders against catastrophic stablecoin debugging through robust diversification.
- Renewable yield through a unique call-option incentive system. The Nirvana APY is market-driven and proportional to investment risk, creating a sustainable engine for high yield.
- True protocol-owned liquidity. 100% of \$ANA's liquidity is owned by the Nirvana protocol, providing a clean path to entering or exiting positions. The protocol is the counterparty to every trade and is not reliant on external market makers.

Using \$ANA as collateral, Nirvana enables zero liquidation-risk loans of NIRV that have a negative interest rate. You earn a yield on your debt. The loans have zero liquidation risk because the total amount of NIRV debt never values more than the floor value (guaranteed minimum value) of \$ANA. The loans have a negative interest because the NIRV borrower does not need to pay continuous fees to a liquidity provider.

- **Concentrated liquidity.** The NIRV token bundles the diverse reserve of stablecoins, concentrating their fragmented liquidity into one token. This bundling includes Solana-native tokens, as well as bridged assets, increasing the overall stablecoin liquidity on Solana.
- **Intrinsic value.** Nirvana maintains a diverse basket of reserve assets that backs the value of \$ANA. At any point in time, \$ANA has an intrinsic value guaranteed by the reserves. The protocol will always buy \$ANA back at its intrinsic value, and so this value becomes a hard floor price under which the token cannot trade.
- **Rising floor.** As the surplus reserves grow in value, the protocol algorithmically increases the intrinsic value of the token. This increase is tantamount to raising the floor

price. In other words, \$ANA holders enjoy permanent gains. Once the floor price ratchets up, those gains are locked forever.

- **Sustainable APY.** Users are incentivized to stake their \$ANA to gain periodic rewards. The protocol mints pre-ANA (prANA) tokens at a regular interval, based on the total supply of \$ANA. These prANA tokens are shared with stakers in proportion to how much they have staked. The result of repeated rewards creates a compounding APY for stakers.
- **Higher-order stablecoin.** \$ANA can be used as collateral for taking NIRV loans. The NIRV token is a superstable currency that is fully collateralized 1:1 with the intrinsic (floor) value of \$ANA. Since NIRV loans are priced at the floor value of \$ANA (which can never be breached), there is zero liquidation risk for these loans.
- **Risk-adjusted discount.** The protocol's reserve profits when the protocol sells \$ANA at the spot price and also when it sells time-released \$ANA (trANA) contracts. When a user purchases \$ANA tokens from Nirvana, the protocol mints several new tokens that are either available instantaneously, or that vest linearly for the user. The price of both time-released \$ANA and instant spot \$ANA is algorithmically set by the protocol's optimized AMM. Time-released \$ANA prices go up with demand for buying them, and lower over time as \$ANA tokens vest.

## 2. Token Info: \$ANA (Nirvana)

- Coingecko: <https://www.coingecko.com/en/coins/nirvana-ana>
- Coinmarketcap: <https://coinmarketcap.com/currencies/nirvana-ana/>
- Contract: ANAxByE6G2WjFp7A4NqtWYXb3mgruyzZYg3spfxe6Lbo
- Solana Explorer:  
<https://explorer.solana.com/address/ANAxByE6G2WjFp7A4NqtWYXb3mgruyzZYg3spfxe6Lbo>
- SolanaFM (A Data Tooling on Solana):  
<https://solana.fm/address/ANAxByE6G2WjFp7A4NqtWYXb3mgruyzZYg3spfxe6Lbo/largest?cluster=mainnet-solanafmbeta>

Token details: Current Supply: 2,048,269.884639<sup>[36]</sup>

Here are the addresses and percentages of the top ten holders<sup>[37]</sup>:

RANK	ADDRESS	OWNER	BALANCE (ANA)	% OF TOTAL SUPPLY
1	AS5yy4yhAL9pZZau4Mdf...VPdJ4Avsx3X2VofyLGJ3	Nirvana Finance Treasury	1,792,636.324909	87.520%
2	EFDAN5xp5kzoEmz8q1H1...NS156oz9Gwkn5stUmGMu	MEXC Exchange	57,334.436009	2.799%
3	FevU9JzLWWgdsMHCCu5...3kgZL5ukczeF2At42zRP	Raydium AMM Authority	44,558.922223	2.175%
4	CbvcYA2LYLVdNxYNrGXU...Nniqy3X6gCEqsAk3dKXg	HRVV2MaLdXqDdCoLa37z...Z7H1NYgj(tYzxNChYEEDa	25,234.290000	1.232%
5	2v9ft9VYGGD5FKS8Ushg...4t5W72CuuuXun7NRj7Lc	6ho6VQmTqrLr7bAff7Kx...bJLywAiUEUNtDtyXgZ9g	9,834.537361	0.480%
6	5fkfXkDDMMjKYKgPBZiZ...DwzMAExrzDfRK34kgZe3	5MobfQDxEMQJ5q7SL5x6...58Q2uL1hAsnuhHBtsn5j	8,885.133031	0.434%
7	HGcZYxJzGSJeW5cFt9UX...TQb9MdK3tNs1hoRdGGo3	7WVYPnkyq28ocRsff2Aw...Wg7YLKV7d5Ee8jVJKp9L	8,802.000000	0.430%
8	FALwX8RZbrDDTVu3ZdEX...LnpEDg8W5KtudSGH46pd	Nirvana Finance Treasury	7,835.212789	0.383%
9	6WvKIgmF36x1fFe8Zggx...dNe5fQnK4f9djLUrxJHC	J5ECjVnkKEbm4Ztxkmp...LunS8Lf2sKGujBxofLZ	7,694.723225	0.376%
10	4uszE4TZc9RhaNT6Piww...FSf8gGeFcTeeBqpYskJn	YzVGKYRTnZAvpNTs7yNh...XtzD2eeFNkz2xBELpmct	6,129.568452	0.299%

The addresses of the top 2 holders held more than 90% of the tokens, with ‘*Nirvana Finance Treasury*’<sup>[38]</sup> holding 87.5%.

### 3. Community:

- a. Official Website: <https://www.nirvana.finance>
- b. Twitter: [https://twitter.com/nirvana\\_fi](https://twitter.com/nirvana_fi)  
Their official Twitter has 320 following and 9,911 followers, Joined in November 2021. In total, this Twitter posted 532 tweets over a period of nearly nine months. Their last tweet, about asking hackers to return the money, was on July 28, 2022, and has not been updated since.
- c. DAO Twitter: <https://twitter.com/TheDAOofNirvana> (Unavailable Now)
- d. Discord: <http://discord.gg/nirvanafi> (Unavailable Now)
- e. Telegram: <https://t.me/nirvanafi> (172 followers)
- f. Medium: <https://medium.com/@nirvanafinance>  
(Last updated on Aug 3, 2022, with 277 followers.)
- g. Official Documentation: <https://docs.nirvana.finance/mechanics/summary>

### 4. Project Team Info:

No information about the project team can be found.

## 2/ Related Incident or Scam

### 1. Incident on July 28, 2022

#### a. General info:

Nirvana Finance was exploited via a flash loan attack forcing the protocol's \$ANA token price to collapse by about 85%. Nirvana Finance is an adaptive yield platform that utilizes the \$ANA token to generate wealth through an adaptive yield, with a built-in rising floor price. The attack happened on the decentralized lending platform Solend<sup>[40]</sup> where the hacker proceeded to borrow amounts of USDT and USDC tokens leveraging \$ANA as collateral. According to Nirvana Finance's post-mortem<sup>[41]</sup>, the attack caused a loss of over \$10M in assets.

(By Certik Incident Analysis Report)<sup>[42]</sup>

**Nirvana ANA Price Chart (ANA)**

Last updated 04:34PM UTC. Currency in USD.

☆ Add To Watchlist

Price Market Cap Live Chart

24h 7d 14d 30d 90d 180d 1y Max



Logarithmic Linear

Apr 12, 2022 → Jun 2, 2023





The price of \$ANA crashed<sup>[43]</sup>

#### b. Details:

Key Accounts Involved are:

1. Nirvana Treasury Account:

<https://solana.fm/address/CxuuSEv67PzNkMxqCvHeDUr6HKaadoz8NhTfxbQSJnaG>

2. Nirvana Hacker Account:

<https://solana.fm/address/76w4SBe2of2wWUsx2FjkkwD29rRznfvEkBa1upSbTAWH>

Both accounts have been tagged on @solanafm<sup>[44]</sup> explorer.

The exploit resulted in inaccurate pricing for the \$ANA token. The attacker manipulated inputs to the program, then was able to buy the token at an artificially low price. Since the act of purchasing \$ANA from Nirvana Finances' native AMM pushes the price upward, the hacker was then able to sell their \$ANA for a high price, making a profit. The attacker executed the flash loan which netted about \$3,574,635 USDT.

The attacker first borrowed \$10,250,000 USDC from the Solend Protocol<sup>[45]</sup> and used it to buy \$ANA.

The attacker then manipulates the price of \$ANA from \$8 to \$24 by calling the Buy 3 command in the contract.

### Logs

```

> Compute Budget Program ┌─ Instruction
  Program returned success
> Solend Program ┌─ Instruction
  Program log: Instruction: Flash Loan
  Invoking Token Program
  Program log: Instruction: Transfer
  Program Token Program ┌─ consumed 3052 of 577942 compute units
  Program returned success
  Invoking Unknown (62o4UiW394cbFxVHbCyuA7DDeRL26bnpfDDPXpm7PRR) Program
  Invoking Unknown (nirkXSE28jCQoK8SmKWqxXz3L9vbSRGKS24iYJj8Aeo) Program
  Program log: Instruction: Buy3
  Program log: Oracle feed BJUgj6YCnFBZ49wF54ddBVA9qu8TeqkFtkbqmZcee8uW latest price: 1
  Program log: Wallet: 76w4SBe2of2wWUsx2FjkkwD29rRznfvEkBa1upSbTAWH
  Program log: Amount of ANA: 0
  Program log: Minimum accepted ANA: 0
  Program log: Total spend tokens: 102500000000000
  Program log: Token: EPjFWdd5AufqSSqeM2qN1xzybapC8G4wEGGkZwyTDt1v
  Program log: Total spend USD: 10250000.000000
  Program log: Max ANA bought: 1174554.9489805557292141757547
  Program log: New ANA price: 24.271378102250000000

```

With the inflated price they then swapped the \$ANA for about \$3,490,563 USDT from the Nirvana treasury and the rest back to USDC.



Then, \$10.28M USDC was returned to Solend Pool and retained the rest.

```
Invoking Unknown (nirkXSE28jCQoK8SmKWqxXz3L9vbSRGKS24iYJj8Aeo) Program
Program log: Instruction: Swap
Program log: Is buy: false
Program log: Amount of ANA: 153986943362
Program log: Expected cost: 0
Program log: Wallet: 76w4SBe2of2wWUsx2FjkkwD29rRznfvEkBa1upSbTAWH
Program log: Token: Es9vMFraCERmJfrF4H2FYD4KCoNkY11McCe8BenwNYB
Program log: Price offset 0.000000
Program log: Total cost: 3490563.697785
Program log: New ANA price: 22.731508676605000000
```

The hacker converted the full USDT amount into USDCet, transferring the funds into an ETH account *0xB9AE2624Ab08661F010185d72Dd506E199E67C09*<sup>[47]</sup> through Wormhole.

## 2/ Alerts

The incident was first reported by @0xFA2<sup>[48]</sup>, Co-Founder & Firefighter of @solanafm<sup>[49]</sup> at 4:48 AM Jul 28, 2022.



...

1/

On 28 July, adaptive yield protocol @nirvana\_fi was exploited for \$3.49M, forcing the protocol's \$ANA token price to collapse over 85%.

The SolanaFM team broke down the key movements involved during the exploit.

Nirvana Hacker Account:  
[solana.fm/address/76w4SB...](https://solana.fm/address/76w4SB...)

ASSET	SYMBOL	QUANTITY	PRICE	CHANGE	VALUE
Hubble Protocol Token	HBB	0.000003	\$0.211284	-158%	\$0.000006339

4:48 AM · Jul 28, 2022

57 Retweets 36 Quotes 137 Likes 16 Bookmarks

[Twitter of @0xFA2 \[50\]](#)

Then Nirvana Finance's official Twitter<sup>[51]</sup> retweeted this about 4 hours later at 8:17 AM Jul 28, 2022, to confirm this attack.



Nirvana Finance  
@nirvana\_fi

...

The Nirvana protocol suffered an exploit today.

The Nirvana team is investigating the attack and will make an announcement to the community as soon as possible.

8:17 AM · Jul 28, 2022



**Nirvana Finance**  
@nirvana\_fi

...

Please be advised:

ANA has lost its collateral, and NIRV has lost its peg. Until the thief restores funds, these tokens will not have exchange value.  
Be very careful with trading NIRV & ANA, as they currently have no guaranteed value.

10:52 AM · Jul 28, 2022

[Twitter of @nirvana\\_fi \[52\]](#)

Nirvana Finance's official Twitter followed up on July 28 with a thread<sup>[53]</sup> to ask hackers to return the money.



**Nirvana Finance**  
@nirvana\_fi

...

To The Nirvana Hacker:

On behalf of the Nirvana Finance community, we humbly ask that you return the stolen funds from our treasury. 1/5

5:03 PM · Jul 28, 2022

41 Retweets 156 Quotes 201 Likes 16 Bookmarks



**Nirvana Finance** @nirvana\_fi · Jul 28, 2022

...

Please be aware your CEX connected wallet has been flagged and we are working with a variety of resources to uncover your identity, recover the stolen funds, and make our community whole. 2/5

6 2 33



**Nirvana Finance** @nirvana\_fi · Jul 28, 2022

...

In recognition of your discovery of a vulnerability in our protocol, we are willing to offer a white hat bounty of \$300,000 and a cessation of investigation. 3/5

5 11 38



**Nirvana Finance** @nirvana\_fi · Jul 28, 2022

...

Please accept this good faith request and return our treasury for the good of the whole Nirvana community. You have not taken money from VCs or large funds—the treasury you have taken represents the collective hopes of everyday people. 4/5

10 6 54



**Nirvana Finance** @nirvana\_fi · Jul 28, 2022

...

Please reach out to us at recovery@nirvana.finance to open a dialogue. 5/5

18 7 51

On August 3<sup>rd</sup>, the official ‘*Technical Post Mortem*’<sup>[54]</sup> was published on Medium.

The screenshot shows a Medium post titled "Technical Post Mortem" by Nirvana. The post discusses a "Post-hack deep dive" into what happened during the exploit. It explains that the hacker manipulated inputs to buy ANA tokens at a low price from Nirvana's native AMM, then sold them at a high price to profit from the spread. The post has 5947 total views and 48 total shares. It includes a "Listen to article" button and a duration of 4:28. The Nirvana logo is visible in the top left corner.

# Technical Post Mortem

Nirvana · Follow  
Published in Nirvana Finance · 2 min read · Aug 3, 2022

Post-hack deep dive

What happened?

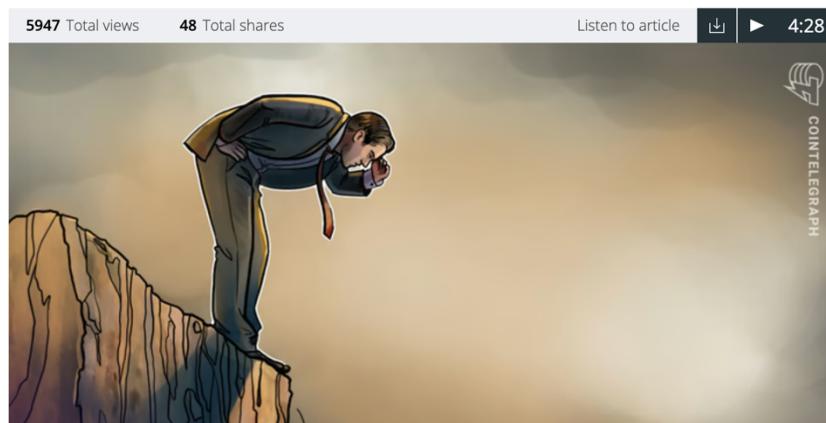
The exploit in Nirvana resulted in inaccurate pricing for the ANA token. By manipulating inputs to the program, the hacker was able to buy the token at an artificially low price. Since the act of purchasing ANA from Nirvana's native AMM pushes the price upward, the hacker was then able to sell their ANA for a high price, making a profit from the spread.

Some media reported the incident later:

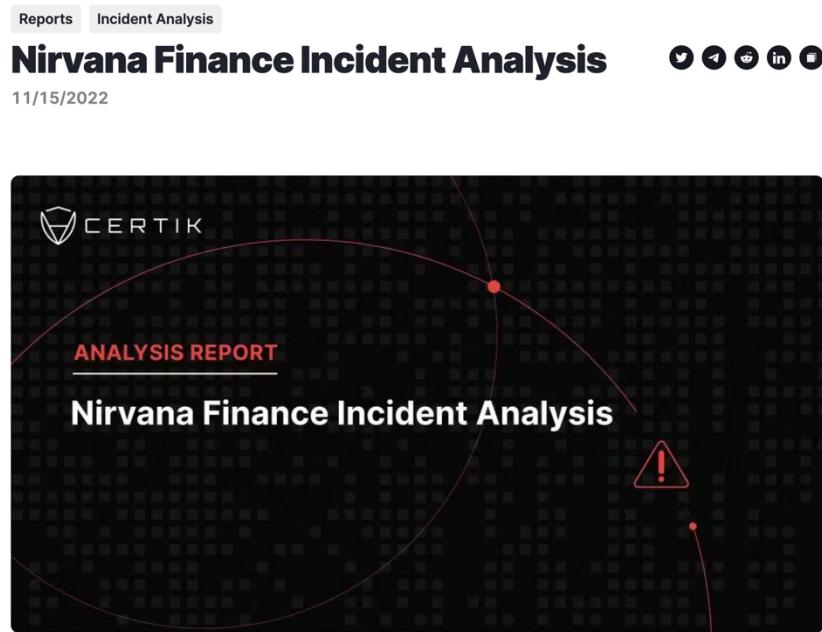
- 1) Coin Telegraph<sup>[55]</sup>

## Solana-based stablecoin NIRV drops 85% following \$3.5M exploit

The \$3.5 million flash loan attack Solana-based Nirvana Finance saw the price of its stablecoin NIRV and native token ANA fall around 85% apiece.



2) Certik<sup>[56]</sup>



3) SlowMist<sup>[57]</sup>

SlowMist @SlowMist\_Team ...

Event: [@nirvana\\_fi](#) Flashloan Attack

Nirvana, a stablecoin project on the [#Solana](#) blockchain suffered a \$3.57M loss after being exploited via a flashloan attack.

The funds were then bridge to [#Ethereum](#) and has yet been transferred to a new wallet.

Nirvana Finance @nirvana\_fi · Jul 28, 2022  
The Nirvana protocol suffered an exploit today.

The Nirvana team is investigating the attack and will make an announcement to the community as soon as possible.

7:44 AM · Jul 30, 2022

\*Many other media reported on this incident. Not all of them are listed here.

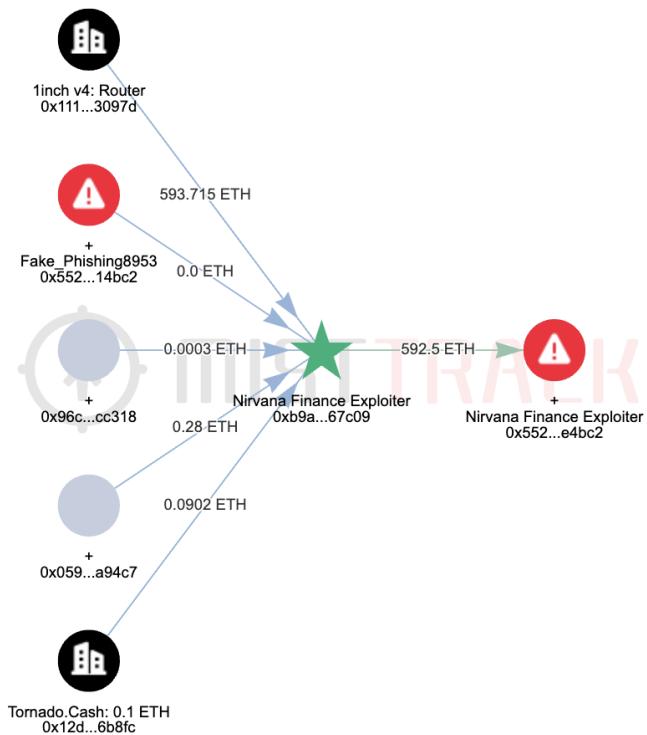
## 4/ The Funds

Nirvana Finance Hacker's Account:

`76w4SBe2of2wWUsx2FjkkwD29rRznfvEkBa1upSbTAWH`<sup>[58]</sup>

The hacker converted the full USDT amount into USDCet, transferring the funds into an ETH account `0xB9AE2624Ab08661F010185d72Dd506E199E67C09`<sup>[59]</sup> through Wormhole.

Then they transferred 592.5 ETH into an ETH account `0x552f5ce2d38d5f9fefcd4724be84f6d79b2e4bc2`<sup>[60]</sup>



Later, the fund was transferred to Thorchain, a contract address, `0xd37bbe5744d730a1d98d8dc97c42f0ca46ad7146`<sup>[61]</sup>

