



INVESTIGATIVE INTELLIGENCE REPORT

Project Name:

CRYSTAL NODES



ASSURE DEFITM
THE VERIFICATION **GOLD STANDARD**



Project Name:

CRYSTAL NODES

Project Name: **Crystal Nodes**
Blockchain: **BSC**
Token (If Applicable): **\$PECT**

Token Contract Address:
0xd562552d5626b9e9e19c71646a29605ac6ed46ed

Quantity of Responsible Parties w/ Identification on
File with **Assure DeFi LLC: 1**
Nationality of Responsible Parties: **FRANCE**

Date Investigation Was Opened:
3/22/22

Alleged Scam/Fraud Type:
Fraud, Rugpull

CONTACT INFORMATION FOR LAW ENFORCEMENT TO OBTAIN KYC & IDENTITY DETAIL INFORMATION ON FILE WITH ASSURE DEFI:

Direct Contact

Email: chapo@assureteam.io
Twitter DM: [www.twitter.com/el_crypto_chapo/](https://twitter.com/el_crypto_chapo/)
Telegram DM: https://t.me/el_crypto_chapo/

Mailing Address

Assure DeFi LLC
c/o United States Corporation Agents, Inc
411 Wolf Ledges Parkway, Suite 201
Akron, OH 44311

Estimate of Injured Parties:

< 150

Estimate Funds Stolen:

~\$25,000

Last Known Location of Funds:

Self-Custody Wallet(s)

*See details below in BlockChain Forensics/Funds Tracing Section of Report.



BACKGROUND INFORMATION

Crystal Nodes billed itself as a Defi as a Service protocol on BSC where you could purchase nodes to earn daily rewards.

The project launched on the **3/22/2022** and within just a few hours liquidity was pulled and all socials of the project were deleted.

In between the time of launch and the liquidity being pulled investors complained that they were unable to sell during this period and others even claimed that BUSD they had used to buy pPECT during the whitelist period were unable to claim their nodes on launch due to the website being taken down.

Entries from our fraud reporting form below:

Briefly describe the nature of the alleged fraud:

They told me I won the whitelist giveaway. They request me that i need busd and exchange for their token pPECT before launch. On the launch day, we then will use the pPECT that we had to exchange for their actual token to purchase nodes. But, too bad the site is down and gone!

The Developer rugged the project; Selling was never possible and the liquidity pool was stolen. After that the discord channel was closed and also other members were not able to join.



BLOCKCHAIN ANALYSIS

Prospect contract owner address flow:

1 | Owner **calls** `setExcludeFromFees()` for Presale contract - Mar-22-2022 04:21:25 PM +UTC

2 | Owner **ends** Presale contract - Mar-22-2022 04:57:00 PM +UTC

3 | Owner **adds** liquidity: - Mar-22-2022 04:58:03 PM +UTC

4 | **Set** transfer tax fee to 110 - Mar-22-2022 04:58:51 PM +UTC

Given that the transfer tax is calculated as stated below:

```
44 - function _transfer(address from, address to, uint amount) internal override {
45     require(!_isBlacklisted[from] && !_isBlacklisted[to], "Blacklisted address");
46
47 -     if(taxOnSell && !isExcludedFromFees[from] && isSellingLessThanStaked(from, to, amount)) {
48         uint amountToDao = amount * percentTaxToDAO / 10**2;
49         super._transfer(from, DAO, amountToDao);
50         super._transfer(from, to, amount - amountToDao);
51     }
52 -     else {
53         super._transfer(from, to, amount);
54     }
```

The Dao will be getting the whole amount.

5 | **Set** ratio sell stake to 110, which will help validate `isSellingLessThanStaked` – Mar-22-2022 05:01:42 PM +UTC

6 | **Set** `0x944f8d88d8750ef611827120908de36f28f8230f` as pool address, which gives ability for the address to call `mint()` function – Mar-22-2022 05:14:08 PM +UTC

```
110 - function mint(address account, uint256 amount) external onlyPool {
111     require(account != address(0), "ERC20: mint to the zero address");
112     _mint(account, amount);
113 }
114
```

Continued

Pool address flow:

1 | **Call** mint() function on Prospect contract, minting
115,792,089,237,316,000,000,000,000,000,000,000,000,000,000 PROSPECT tokens —
Mar-22-2022 05:17:08 PM +UTC

2 | **Swap** 115,322,792,000 PROSPECT to 24,509 BUSD — Mar-22-2022 05:17:59 PM +UTC

3 | **Swap** 24,509 BUSD to 24,507 USDC — Mar-22-2022 05:20:29 PM +UTC

4 | **Swap** out 24,505 USDC to Avalanche network — Mar-22-2022 05:22:14 PM +UTC

5 | **Transfer** 24,537 to 0x60d642aaaf9d0e80d1aeb8fe1626ba808e0ad48b —
Mar-23-2022 02:43:35 PM +UTC

Address 0x60d642aaaf9d0e80d1aeb8fe1626ba808e0ad48b flow:

1 | **Swap** 24,537 USDC to 24,531 DAI — Mar-23-2022 02:54:41 PM +UTC



SUMMARY / CONCLUSION

Based on the information gathered regarding the case, our experts concluded that none of the funds were redistributed to the users.

Given the addresses used throughout the chain of transactions involved in moving the funds from the liquidity pool it is believed that someone possessing the private keys of the project redistributed the funds from to himself.



RECOMMENDED ACTION ITEMS/NEXT STEPS FOR ADVERSELY AFFECTED PARTIES

Trying to recover funds by contacting the owner of the project.

Trying to recover funds by using legal agencies/authorities

Investors should contact authorities and make a formal complaint providing this report as an evidence package. Links to reporting agencies below.

File law enforcement reports with the following agencies:

#1: Europol CyberCrime

<https://www.europol.europa.eu/report-a-crime/report-cybercrime-online>

#2: AMF (French Financial Authority)

<https://www.amf-france.org/fr/signaler-une-arnaque-ou-une-anomalie>



NEXT STEPS FOR ASSURE

- **Assure will provide guidance on additional appropriate jurisdictions & agencies to which injured parties can file reports as applicable.**
- **Fully cooperate with law enforcement agencies upon official requests as received**

RESOURCES

If you have additional information related to this case, please submit via Assure DeFi's scam reporting form using the following link:

<https://www.assuredefi.io/scam-reporting-form>

Contact Assure DeFi directly via the following channels:

Twitter Direct Message:

www.twitter.com/assuredefi/

Email: chapo@assuredefi.io



ASSURE DEFI™
THE VERIFICATION **GOLD STANDARD**