



PRISMA SHIELD



GAUSS

CODE VERIFICATION AUDIT REPORT

NobleSwap DEX

AUG 22 2023



Table of Contents

Overview	03
Summary of Results	06
Contract Addresses	07
Miscellaneous Addresses	08
Disclaimer	09



Overview

This code verification audit report verifies that the NobleSwap DEX contracts have been forked exactly from the official PancakeSwap DEX contracts, with no functional changes.

This report does NOT constitute an audit of the PancakeSwap DEX contracts, and therefore any potential vulnerabilities in the PancakeSwap DEX contracts may also be present in the NobleSwap DEX contracts.

This verification was done by comparing the source code of the deployed NobleSwap DEX contracts with the corresponding source code of [the deployed PancakeSwap DEX contracts on the BNB smart chain](#), and verifying that there are no functional changes. The only allowed changes were to the arguments of some of the contracts that are necessary for the overall system to work correctly, except for one contract which had an unused feature removed from it (more details in page 5).

Overview

Only the NobleBar contract was compared against PancakeSwap's SyrupBar contract on their official Github. It contains a fix from the officially deployed SyrupBar contract on the BNB smart chain, which contains a vulnerability, and is no longer officially supported by PancakeSwap. This carries the risk of including any other potential bugs from the SyrupBar contract on Github which hasn't been officially deployed and widely used.

It has been verified that the contract owner/admin of the relevant contracts has been set to 0x9291b5c6aAC5CCB9feEBA86dF5A31cc8f471F86a, which is an EOA for testnet experiments. The team has confirmed that all private keys are secured and backed up, and a Gnosis Safe multisig address will be used once the contracts are deployed on mainnet.


Moreover, the treasury address used in the relevant contracts is 0x118fB74e803EB08b731c7996393E7B04600F8271 which is also an EOA. The team has confirmed that it will be changed to a multisig address upon mainnet deployment.

Overview

The SmartChefFactory and SmartChefInitializable contracts had the PancakeProfile system removed. The team's response to this was that they will not be using that system and that it does not affect the core functionality of the contracts, as it is only used to keep track of points earned by staking which is then used elsewhere for PancakeSwap's other products.

Finally, the boost contracts are not deployed and used in MasterChefV2 and NoblePool. The team acknowledged that the boost mechanism will not be used at launch.

Summary of Results

Project	Pass/Fail	Comments
NobleSwap DEX	Passed 	No functional changes

Contract Addresses

NobleFactory

[0x3FFb082bD33EdDdBdf691B9E66F9aD6b8Dc45227](#)

NobleRouter

[0x6BA8bF59251A5b9d2525065bB9391f03EFcbd39C](#)

NobleToken

[0xC66edF8eCC0Fc72b10cB749146e9de9837C9359E](#)

NobleBar

[0x75cc29F63C1d7b57736CfACF12f436e96B54ae6C](#)

MasterChef

[0x779F6a45c33eF6BdE58F4878905C6f647Ec9BbC6](#)

MasterChefV2

[0x5F70F388D28bf17E2019001e41f6fdfcC272FA5D](#)

ERC721NFTMarketPlace

[0xB6A8f6c2bDF123Fd2801561008fe838Ca60133af](#)

NoblePool

[0x592A280cd900C84bB2d444664e979B0688930df1](#)

SmartChefFactory

[0x3424d2810AEf8675D5a5D3E6C13A580AFE57361a](#)

wGANG

[0x624814Bca9A5d5620E350264f839b93f766B60a2](#)

Miscellaneous Addresses

Dummy MasterChefV2 token

[0x255A431F973c8671EE1783cA25aC1582b8b60F2E](#)

Dummy NoblePool token

[0xB63b0faF9FFcA69de407331400bD745D627ACC4E](#)

Admin Address

[0x9291b5c6aAC5CCB9feEBA86dF5A31cc8f471F86a](#)

Treasury Address

[0x118fB74e803EB08b731c7996393E7B04600F8271](#)

Disclaimer

The information in this report objectively compares the smart contracts being verified against other smart contracts that are widely used. It does not ensure the correctness or authenticity of any software or dApp that interacts with or claims to interact with any smart contract.

This report does not constitute any advice whatsoever. You are solely responsible for conducting your own due diligence and consulting your financial advisor before making any investment decisions. Trust in project owners is required to invest in this protocol as a Prisma Shield audit or code verification does not ensure the fulfillment of roadmap deliverables and allocation of funds. Our reports do not amount to any form of warranty or guarantee that the reviewed smart contracts are void of any weaknesses, vulnerabilities, or bugs. Prisma Shield and its founders, employees, owners, and associates are not liable for any damage or loss of funds. Please ensure trust in the team prior to investing as this report does not guarantee the promised use of your funds.



Introducing Deep Logic
Smart Contract
Auditing to Web3



prismashield.com



prismashield@gmail.com



[PrismaShield](https://twitter.com/PrismaShield)



[PrismaShield](https://t.me/PrismaShield)