



SOLIDProof
Bring trust into your projects

**Blockchain Security | Smart Contract Audits | KYC
Development | Marketing**

MADE IN GERMANY

STAKEX from DEGENX

AUDIT

SECURITY ASSESSMENT

22. May, 2024

FOR



SolidProof_io



@solidproof_io



Introduction	4
Disclaimer	4
Project Overview	5
Summary	5
Social Medias	5
Audit Summary	6
File Overview	7
Imported packages	9
Audit Information	10
Vulnerability & Risk Level	10
Auditing Strategy and Techniques Applied	11
Methodology	11
Overall Security	12
Upgradeability	12
Ownership	13
Ownership Privileges	14
Minting tokens	14
Burning tokens	15
Blacklist addresses	16
Fees and Tax	17
Lock User Funds	18
Components	19
Exposed Functions	19
StateVariables	19
Capabilities	20
Inheritance Graph	21
Centralization Privileges	22
Audit Results	23
Critical issues	23
High issues	23



Medium issues	23
Low issues	23
Informational issues	24





Introduction

[SolidProof.io](#) is a brand of the officially registered company Future Visions Deutschland. We're mainly focused on Blockchain Security, such as Smart Contract Audits and KYC verification for project teams.

Solidproof.io assesses potential security issues in the smart contracts implementations, reviews for potential inconsistencies between the code base and the whitepaper/documentation, and provides suggestions for improvement.

Disclaimer

[SolidProof.io](#) reports are not, nor should they be considered, an “endorsement” or “disapproval” of any particular project or team. These reports are not, nor should they be considered, an indication of the economics or value of any “product” or “asset” created by any team. SolidProof.io does not cover testing or auditing the integration with external contracts or services (such as Uniswap, PancakeSwap, etc.).

SolidProof.io Audits do not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analysed, nor do they provide any indication of the technology proprietors. SolidProof Audits should not be used in any way to make decisions around investment or involvement with any particular project. These reports in no way provide investment advice, nor should be leveraged as investment advice of any sort.

SolidProof.io Reports represent an extensive auditing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology. Blockchain technology and cryptographic assets present a high level of ongoing risk. SolidProof's position is that each company and individual are responsible for their own due diligence and continuous security. SolidProof in no way claims any guarantee of the security or functionality of the technology we agree to analyse.



Project Overview

Summary

Project Name	DegenX Finance
Website	https://dgnx.finance/
About the project	<p>DEGENX is multichain ecosystem that offers a suite of decentralized applications (dApps) and services to provide solutions for projects and individuals in the DeFi space.</p> <p>DEGENX is multichain ecosystem that offers a suite of decentralized applications (dApps) and services to provide solutions for projects and individuals in the DeFi space.</p>
Chain	Avalanche
Language	Solidity
Codebase Link	Provided as Files (Private Repo)
Commit	N/A
Unit Tests	Provided

Social Medias

Telegram	https://t.me/DegenXportal
Twitter	https://twitter.com/degenecosystem
Facebook	N/A
Instagram	https://instagram.com/degenecosystem
Github	https://github.com/DEGENTOKENTEAM
Reddit	https://www.reddit.com/user/degentrader_sd
Medium	https://medium.com/@degentraderteam
Discord	https://discord.gg/BMaVtEVkgC
Youtube	https://youtube.com/@DGNX.FINANCE-DEGENX?sub_confirmation=1
TikTok	https://www.tiktok.com/@degen_traders
LinkedIn	N/A



Audit Summary

Version	Delivery Date	Changelog
v1.0	22. May 2024	<ul style="list-style-type: none">• Layout Project• Automated- /Manual-Security Testing• Summary

Note - The following audit report presents a comprehensive security analysis of the smart contract utilized in the project that includes malicious outside manipulation of the contract's functions. This analysis did not include functional testing (or unit testing) of the contract/s logic. We cannot guarantee 100% logical correctness of the contract as we did not functionally test it. This includes internal calculations in the formulae used in the contract.





File Overview

The Team provided us with the files that should be tested in the security assessment. This audit covered the following files listed below with an SHA-1 Hash.

File Name	SHA-1 Hash
contracts/diamond/helpers/ GenericErrors.sol	bf8733c5c5ef44c0fab16a60432a0bcab02cd73b
contracts/diamond/helpers/ Constants.sol	f8124ef60f121ea8950463a3ddcae6c8c6981856
contracts/diamond/helpers/ structs/Stake.sol	127496e3d2441a7a0114b697c11585a1b036d98f
contracts/diamond/helpers/ structs/ RewardAddParams.sol	df57de0a8de60cfc1d14ad4650ed04caaf1d408d
contracts/diamond/helpers/ structs/RewardEstimation.sol	85a8fc12757b5e073d062275456f0f6c92d3f840
contracts/diamond/helpers/ structs/SwapCandidate.sol	8e169a992ad42e5e265f54b138c1b7713f65f107
contracts/diamond/helpers/ structs/StakeBucket.sol	588d39cc32c811a3c14387e76dd57b7e1fbee58
contracts/diamond/helpers/ structs/TokenInfo.sol	fb54baf36ea7429b25604ad809bcbf1da7861c00
contracts/diamond/helpers/ Enums.sol	fc859410835d7f9bc7b2dcc7c3ad08dbc858cb3c
contracts/diamond/helpers/ Functions.sol	a131f4a9f29d397409f849d1830847fa2ca07020
contracts/diamond/ Diamond.sol	33a5ae9fda831cf0788076e8c68ae76cf30275c3
contracts/diamond/libraries/ LibStakeXManagement.sol	204065a10f52bc5fe7b9aee3fed936c4e6e2fad0
contracts/diamond/libraries/ LibStakeXPublic.sol	1096e46cf3186974d649984ac9c1699adf07ae58
contracts/diamond/libraries/ LibStakeXShared.sol	0e427c71a501a1693f6c1ed1173c1e921f4d637d



contracts/diamond/libraries/ LibDiamond.sol	8b88293ea9b17ce5c3a909e925958b4ced822d81
contracts/diamond/libraries/ LibStakeXNFTStorage.sol	5b93c108ef91d2e2b10b6e5932fdf73201d12219
contracts/diamond/libraries/ LibStakeXCore.sol	71c7f189e60f33e1756257b02761ff0ee4636312
contracts/diamond/libraries/ LibStakeXStorage.sol	547cdc58ff6fad92572b4e7eb55113c2f47e3c5f
contracts/diamond/ upgradInitializers/ DiamondInit.sol	857f02c46e8c9f23b3714631e43adf2acf782762
contracts/diamond/facets/ StakeXNFTFacet.sol	fb7b76b6859b9abd429ba740750c354fd56e992 d
contracts/diamond/facets/ StakeXManagementFacet.sol	1080cb464181d3dcd68122d695929697fada6e00
contracts/diamond/facets/ AccessControlEnumerableFacet.sol	7cb7492cde6018892a18805fcceffefcc8d88c05
contracts/diamond/facets/ DiamondLoupeFacet.sol	e7def897bcfc8a7900975cbe8a95b0631db20c44
contracts/diamond/facets/ StakeXNFTComposerFacet.sol	c0ba6a24ed591c4bf3719bedfbd8f1fafb06236f
contracts/diamond/facets/ StakeXCoreFacet.sol	97cb19a84500bba7848e44fc13bbe8f8a260f7c7
contracts/diamond/facets/ StakeXNFTRendererFacet.sol	b81390ceddce17ae278fb309b815c511417a1b3c
contracts/diamond/facets/ DiamondCutFacet.sol	03cf892635603d0a25b69feaa766fa599057ea81
contracts/diamond/facets/ StakeXPublicFacet.sol	d76d2450398af53d05e45c132d8b87de94c9ca86

Please note: Files with a different hash value than in this table have been modified after the security check, either intentionally or unintentionally. A different hash value may (but need not) indicate a changed state or potential vulnerability that was not the subject of this scan.



Imported packages

Used code from other Frameworks/Smart Contracts (direct imports).

Dependency / Import Path	Count
@openzeppelin/contracts/access/IAccessControlEnumerable.sol	1
@openzeppelin/contracts/token/ERC20/IERC20.sol	3
@openzeppelin/contracts/token/ERC20/extensions/IERC20Metadata.sol	5
@openzeppelin/contracts/token/ERC20/utils/SafeERC20.sol	3
@openzeppelin/contracts/utils/Base64.sol	1
@openzeppelin/contracts/utils/Strings.sol	2
@openzeppelin/contracts/utils/structs/EnumerableSet.sol	1
@solidstate/contracts/interfaces/IERC165.sol	1
@solidstate/contracts/interfaces/IERC721.sol	1
@solidstate/contracts/token/ERC721/SolidStateERC721.sol	1
@solidstate/contracts/token/ERC721/metadata/ERC721MetadataStorage.sol	1

Note for Investors: We only audited contracts mentioned in the scope above. All contracts related to the project apart from that are not a part of the audit, and we cannot comment on its security and are not responsible for it in any way.



Audit Information

Vulnerability & Risk Level

Risk represents the probability that a certain source threat will exploit vulnerability and the impact of that event on the organization or system. The risk Level is computed based on CVSS version 3.0.

Level	Value	Vulnerability	Risk (Required Action)
Critical	9 - 10	A vulnerability that can disrupt the contract functioning in a number of scenarios, or creates a risk that the contract may be broken.	Immediate action to reduce risk level.
High	7 - 8.9	A vulnerability that affects the desired outcome when using a contract, or provides the opportunity to use a contract in an unintended way.	Implementation of corrective actions as soon as possible.
Medium	4 - 6.9	A vulnerability that could affect the desired outcome of executing the contract in a specific scenario.	Implementation of corrective actions in a certain period.
Low	2 - 3.9	A vulnerability that does not have a significant impact on possible scenarios for the use of the contract and is probably subjective.	Implementation of certain corrective actions or accepting the risk.
Informational	0 - 1.9	A vulnerability that have informational character but is not effecting any of the code.	An observation that does not determine a level of risk



Auditing Strategy and Techniques Applied

Throughout the review process, care was taken to check the repository for security-related issues, code quality, and compliance with specifications and best practices. To this end, our team of experienced pen-testers and smart contract developers reviewed the code line by line and documented any issues discovered.

We check every file manually. We use automated tools only so that they help us achieve faster and better results.

Methodology

The auditing process follows a routine series of steps:

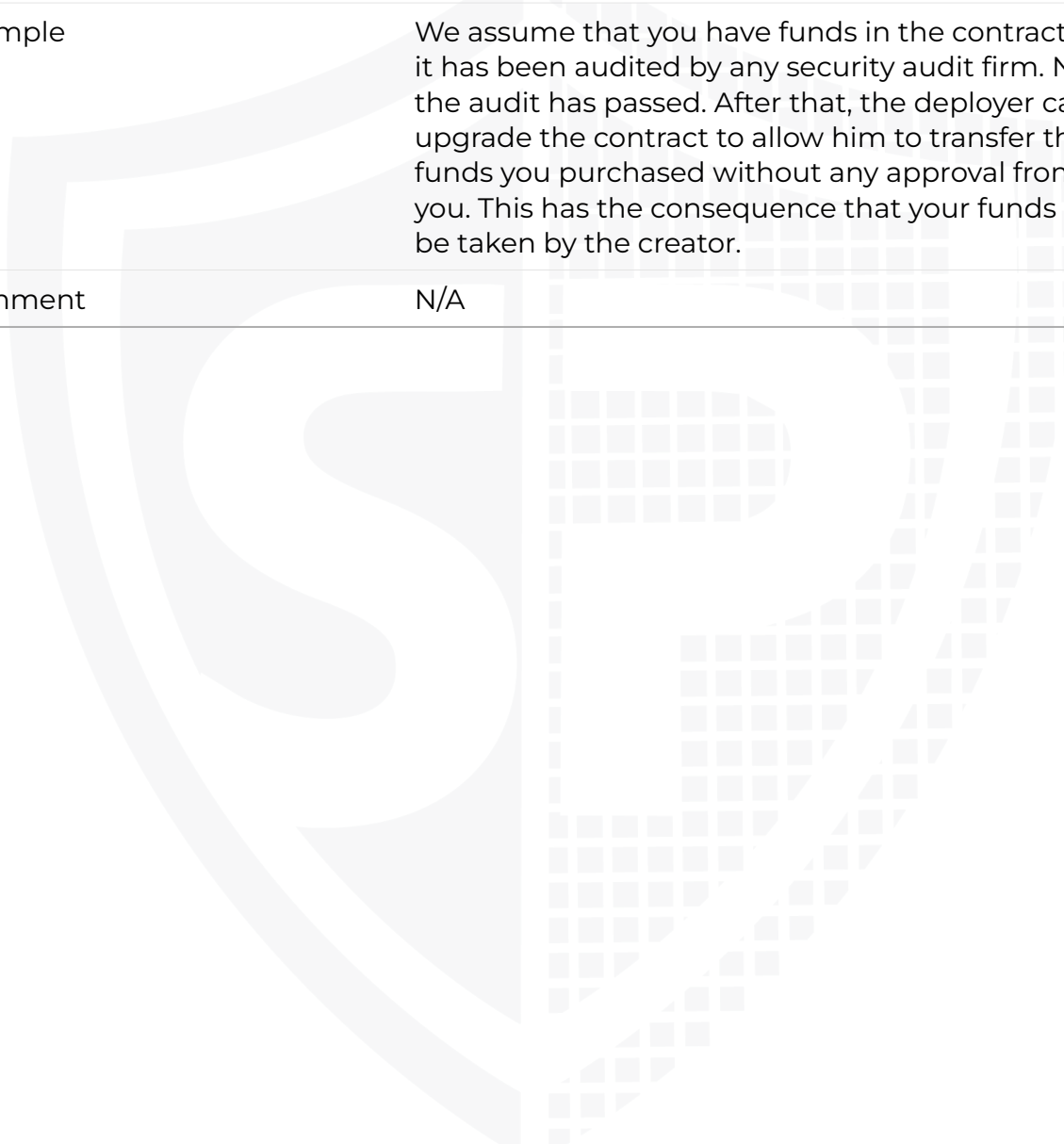
1. Code review that includes the following:
 - a. Review the specifications, sources, and instructions provided to SolidProof to ensure we understand the smart contract's size, scope, and functionality.
 - b. Manual review of the code, i.e., reading the source code line by line to identify potential vulnerabilities.
 - c. Comparison to the specification, i.e., verifying that the code does what is described in the specifications, sources, and instructions provided to SolidProof.
2. Testing and automated analysis that includes the following:
 - a. Test coverage analysis determines whether test cases cover code and how much code is executed when those test cases are executed.
 - b. Symbolic execution is analysing a program to determine what inputs cause each part of a program to execute.
3. Review best practices, i.e., smart contracts to improve efficiency, effectiveness, clarity, maintainability, security, and control based on best practices, recommendations, and research from industry and academia.
4. Concrete, itemized and actionable recommendations to help you secure your smart contracts.



Overall Security Upgradeability

Contract is an upgradeable ✘ **Deployer can update the contract with new functionalities**

Description	The deployer can replace the old contract with a new one with new features. Be aware of this, because the owner can add new features that may have a negative impact on your investments.
Example	We assume that you have funds in the contract and it has been audited by any security audit firm. Now the audit has passed. After that, the deployer can upgrade the contract to allow him to transfer the funds you purchased without any approval from you. This has the consequence that your funds can be taken by the creator.
Comment	N/A





Ownership

The ownership is not renounced **✗ The owner is not renounce**

<p>Description</p>	<p>The owner has not renounced the ownership that means that the owner retains control over the contract’s operations, including the ability to execute functions that may impact the contract’s users or stakeholders. This can lead to several potential issues, including:</p> <ul style="list-style-type: none"> • Centralizations • The owner has significant control over contract’s operations
<p>Comment</p>	<p>N/A</p>

Note — If the contract is not deployed then we would consider the ownership to be not renounced. Moreover, if there are no ownership functionalities then the ownership is automatically considered renounced.



Ownership Privileges

These functions can be dangerous. Please note that abuse can lead to financial loss. We have a guide where you can learn more about these Functions.

Minting tokens


Minting tokens refers to the process of creating new tokens in a cryptocurrency or blockchain network. This process is typically performed by the project's owner or designated authority, who can add new tokens to the network's total supply.

Contract owner cannot mint new tokens		<input checked="" type="checkbox"/> The owner cannot mint new tokens
Description	The owner is not able to mint new tokens once the contract is deployed.	
Comment	N/A	



Burning tokens

Burning tokens is the process of permanently destroying a certain number of tokens, reducing the total supply of a cryptocurrency or token. This is usually done to increase the value of the remaining tokens, as the reduced supply can create scarcity and potentially drive up demand.

Contract owner cannot burn tokens		 The owner cannot burn tokens
Description	The owner is not able burn tokens without any allowances.	
Comment	N/A	



Blacklist addresses

Blacklisting addresses in smart contracts is the process of adding a certain address to a blacklist, effectively preventing them from accessing or participating in certain functionalities or transactions within the contract. This can be useful in preventing fraudulent or malicious activities, such as hacking attempts or money laundering.

Contract owner cannot blacklist addresses **✔ The owner cannot blacklist addresses**

Description	The owner is not able blacklist addresses to lock funds.
Comment	N/A





Fees and Tax

In some smart contracts, the owner or creator of the contract can set fees for certain actions or operations within the contract. These fees can be used to cover the contract's cost, such as paying for gas fees or compensating the contract's owner for their time and effort in developing and maintaining the contract.

Contract owner can set fees greater than 25% ✘ Stake fees could go up to 50%	
Description	<p>For example, a decentralized exchange (DEX) smart contract may charge a fee for each trade executed on the platform. This fee can be set by the owner of the contract and may be a percentage of the trade value or a flat fee.</p> <p>In other cases, the owner of the smart contract may set fees for accessing or using certain features of the contract. For instance, a subscription-based service smart contract may charge a monthly or yearly fee for access to premium features.</p> <p>It's important to note that the fees set by the owner of a smart contract may not be the same as the gas fees required to execute the contract on the blockchain. Gas fees are generally set by the network and vary based on factors such as network congestion and the complexity of the transaction. The fees set by the contract owner, on the other hand, are independent of gas fees and are typically charged in addition to gas fees.</p>
Example	<p>Our assumption is that the owner can adjust the stake fees up to 50%. If the transfer fee is set to 50%, it implies that the Half amount of tokens you intend to send will be sent to the address specified as the recipient in the contract. This implies that the recipient will never have the intended amount of tokens in their wallet as half of it has all been used up in paying for the staking fee.</p>
Comment	N/A



Lock User Funds

In a smart contract, locking refers to the process of restricting access to certain tokens or assets for a specified period of time. When tokens or assets are locked in a smart contract, they cannot be transferred or used until the lock-up period has expired or certain conditions have been met.

Owner cannot lock the contract **The owner cannot lock the contract**

Description	The owner is not able to lock the contract by any functions or updating any variables.
-------------	--

Comment	N/A
---------	-----





External/Public functions

External/public functions are functions that can be called from outside of a contract, i.e., they can be accessed by other contracts or external accounts on the blockchain. These functions are specified using the function declaration's external or public visibility modifier.

State variables


State variables are variables that are stored on the blockchain as part of the contract's state. They are declared at the contract level and can be accessed and modified by any function within the contract. State variables can be defined with a visibility modifier, such as public, private, or internal, which determines the access level of the variable.

Components

 Contracts	 Libraries	 Interfaces	 Abstract
11	8	0	0


Exposed Functions

This section lists functions that are explicitly declared public or payable. Please note that getter methods for public stateVars are not included.

 Public	 Payable
82	3



External	Internal	Private	Pure	View
81	126	1	14	62

StateVariables

Total	 Public
12	0



Capabilities

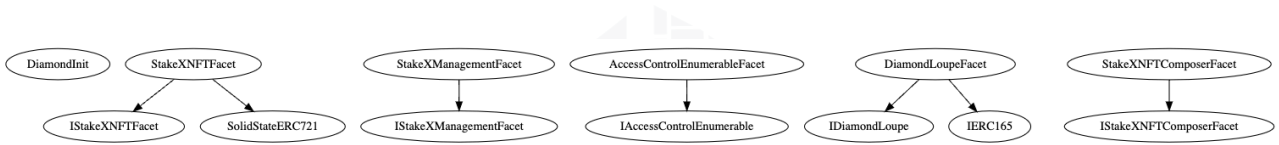
Solidity Versions observed	Transfers ETH	 Can Receive Funds	 Uses Assembly	Delegate Call
^0.8.0 0.8.19 ^0.8.17 ^0.8.19	No	Yes	Yes	Yes





Inheritance Graph

An inheritance graph is a graphical representation of the inheritance hierarchy among contracts. In object-oriented programming, inheritance is a mechanism that allows one class (or contract, in the case of Solidity) to inherit properties and methods from another class. It shows the relationships between different contracts and how they are related to each other through inheritance.





Centralization Privileges

Centralization can arise when one or more parties have privileged access or control over the contract's functionality, data, or decision-making. This can occur, for example, if a single entity controls the contract or if certain participants have special permissions or abilities that others do not.

In the project, some authorities have access to the following functions:

File	Privileges
StakeXmanagementFacet	<ul style="list-style-type: none"> • Add Rewards and Stake Buckets • Update Stake Bucket Shares • Enable/Disable stake bucket, target and reward token • Enable/Disable deposit restriction • Set Staking fee • Enable/Disable Protocol
StakeXNFTComposerFacet	<ul style="list-style-type: none"> • Set NFT Config • Add/Update/Remove Later • Update Layer Order and Assign Config to Buckets

Recommendations

To avoid potential hacking risks, the client should manage the private key of the privileged account with care. Additionally, we recommend enhancing the security practices of centralized privileges or roles in the protocol through a decentralized mechanism or smart-contract-based accounts, such as multi-signature wallets.

Here are some suggestions of what the client can do:

- Consider using multi-signature wallets: Multi-signature wallets require multiple parties to sign off on a transaction before it can be executed, providing an extra layer of security, e.g. Gnosis Safe
- Use of a timelock at least with a latency of, e.g. 48-72 hours for awareness of privileged operations
- Introduce a DAO/Governance/Voting module to increase transparency and user involvement
- Consider Renouncing the ownership so that the owner can no longer modify any state variables of the contract. Make sure to set up everything before renouncing.



Audit Results

Critical issues

No critical issues

High issues

No high issues

Medium issues

No medium issues

Low issues

No Low issues



Informational issues

#1 | NatSpec documentation missing

File	Severity	Location	Status
All	Informational	N/A	Open

Description - If you started to comment on your code, comment on all other functions, variables etc.



Legend for the Issue Status

Attribute or Symbol	Meaning
Open	The issue is not fixed by the project team.
Fixed	The issue is fixed by the project team.
Acknowledged(ACK)	The issue has been acknowledged or declared as part of business logic.



**Blockchain Security | Smart Contract Audits | KYC
Development | Marketing**

MADE IN GERMANY