



SMART CONTRACT AUDIT



interfinetwork



hello@interfi.network



<https://interfi.network>

PREPARED FOR

DRAGONKING NFT



INTRODUCTION

Auditing Firm	InterFi Network
Client Firm	DragonKing NFT
Methodology	Automated Analysis, Manual Code Review
Language	Solidity
Token Proxy	0x61770c92000114B3C0AB5E11918C708dD670d43F
Token Implementation	0x6a26bBc85f6DcD18994805F407fbBA09a37E1F8f
Blockchain	Binance Smart Chain
Centralization	Active ownership
Commit	c04c6005c1ec2c23454033f61281df05046927b4
Website	
Telegram	
X (Twitter)	
Discord	
Report Date	October 05, 2023


 Verify the authenticity of this report on our website: <https://www.github.com/interfinetwork>




EXECUTIVE SUMMARY

InterFi has performed the automated and manual analysis of solidity codes. Solidity codes were reviewed for common contract vulnerabilities and centralized exploits. Here's a quick audit summary:

Status	Critical ●	Major ●	Medium ●	Minor ●	Unknown ●
Open	0	2	1	6	1
Acknowledged	1	1	0	0	0
Resolved	0	0	0	1	0
Noteworthy Privileges	Review PAGE 19 for centralized and controlled privileges				

 Please note that smart contracts deployed on blockchains aren't resistant to exploits, vulnerabilities and/or hacks. Blockchain and cryptography assets utilize new and emerging technologies. These technologies present a high level of ongoing risks. For a detailed understanding of risk severity, source code vulnerability, and audit limitations, kindly review the audit report thoroughly.

 Please note that centralization privileges regardless of their inherited risk status - constitute an elevated impact on smart contract safety and security.


 Please note **DKNFT** contract is upgradeable, smart contract implementation can be changed at any given time. Audited implementation: 0x6a26bBc85f6DcD18994805F407fbBA09a37E1F8f.



TABLE OF CONTENTS

TABLE OF CONTENTS	4
SCOPE OF WORK.....	5
AUDIT METHODOLOGY	6
RISK CATEGORIES	8
CENTRALIZED PRIVILEGES	9
AUTOMATED ANALYSIS.....	10
MANUAL REVIEW.....	19
DISCLAIMERS	33
ABOUT INTERFI NETWORK	36

INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI
CONFIDENTIAL AUDIT REPORT CONFIDENTIAL AUDIT REPORT CONFIDENTIAL AUDIT REPORT CONFIDENTIAL AUDIT REPORT CONFIDENTIAL



SCOPE OF WORK

InterFi was consulted by DragonKing NFT to conduct the smart contract audit of their solidity source codes. The audit scope of work is strictly limited to mentioned solidity file(s) only:

- DKNFT.sol

 If source codes are not deployed on the main net, they can be modified or altered before main-net deployment. Verify the contract's deployment status below:

Public Contract Link	
https://bscscan.com/address/0x6a26bBc85f6DcD18994805F407fbBA09a37E1F8f#code	
Contract Name	DKNFT
Compiler Version	0.8.19
License	MIT



AUDIT METHODOLOGY

Smart contract audits are conducted using a set of standards and procedures. Mutual collaboration is essential to performing an effective smart contract audit. Here's a brief overview of InterFi's auditing process and methodology:

CONNECT

- The onboarding team gathers source codes, and specifications to make sure we understand the size, and scope of the smart contract audit.

AUDIT

- Automated analysis is performed to identify common contract vulnerabilities. We may use the following third-party frameworks and dependencies to perform the automated analysis:
 - Remix IDE Developer Tool
 - Open Zeppelin Code Analyzer
 - SWC Vulnerabilities Registry
 - DEX Dependencies, e.g., Pancakeswap, Uniswap
- Simulations are performed to identify centralized exploits causing contract and/or trade locks.
- A manual line-by-line analysis is performed to identify contract issues and centralized privileges.

We may inspect below mentioned common contract vulnerabilities, and centralized exploits:

Centralized Exploits	<ul style="list-style-type: none">○ Token Supply Manipulation○ Access Control and Authorization○ Assets Manipulation○ Ownership Control○ Liquidity Access○ Stop and Pause Trading○ Ownable Library Verification
----------------------	---



Common Contract Vulnerabilities

- Integer Overflow
- Lack of Arbitrary limits
- Incorrect Inheritance Order
- Typographical Errors
- Requirement Violation
- Gas Optimization
- Coding Style Violations
- Re-entrancy
- Third-Party Dependencies
- Potential Sandwich Attacks
- Irrelevant Codes
- Divide before multiply
- Conformance to Solidity Naming Guides
- Compiler Specific Warnings
- Language Specific Warnings

REPORT

- The auditing team provides a preliminary report specifying all the checks which have been performed and the findings thereof.
- The client's development team reviews the report and makes amendments to solidity codes.
- The auditing team provides the final comprehensive report with open and unresolved issues.

PUBLISH






- The client may use the audit report internally or disclose it publicly.

 It is important to note that there is no pass or fail in the audit, it is recommended to view the audit as an unbiased assessment of the safety of solidity codes.



RISK CATEGORIES

Smart contracts are generally designed to hold, approve, and transfer tokens. This makes them very tempting attack targets. A successful external attack may allow the external attacker to directly exploit. A successful centralization-related exploit may allow the privileged role to directly exploit. All risks which are identified in the audit report are categorized here for the reader to review:

Risk Type	Definition
Critical 	These risks could be exploited easily and can lead to asset loss, data loss, asset, or data manipulation. They should be fixed right away.
Major 	These risks are hard to exploit but very important to fix, they carry an elevated risk of smart contract manipulation, which can lead to high-risk severity.
Medium 	These risks should be fixed, as they carry an inherent risk of future exploits, and hacks which may or may not impact the smart contract execution. Low-risk re-entrancy-related vulnerabilities should be fixed to deter exploits.
Minor 	These risks do not pose a considerable risk to the contract or those who interact with it. They are code-style violations and deviations from standard practices. They should be highlighted and fixed nonetheless.
Unknown 	These risks pose uncertain severity to the contract or those who interact with it. They should be fixed immediately to mitigate the risk uncertainty.

All statuses which are identified in the audit report are categorized here for the reader to review:

Status Type	Definition
Open	Risks are open.
Acknowledged	Risks are acknowledged, but not fixed.
Resolved	Risks are acknowledged and fixed.



CENTRALIZED PRIVILEGES

Centralization risk is the most common cause of cryptography asset loss. When a smart contract has a privileged role, the risk related to centralization is elevated.

There are some well-intended reasons have privileged roles, such as:

- Privileged roles can be granted the power to pause() the contract in case of an external attack.
- Privileged roles can use functions like, include(), and exclude() to add or remove wallets from fees, swap checks, and transaction limits. This is useful to run a presale and to list on an exchange.

Authorizing privileged roles to externally-owned-account (EOA) is dangerous. Lately, centralization-related losses are increasing in frequency and magnitude.

- The client can lower centralization-related risks by implementing below mentioned practices:
- Privileged role's private key must be carefully secured to avoid any potential hack.
- Privileged role should be shared by multi-signature (multi-sig) wallets.
- Authorized privilege can be locked in a contract, user voting, or community DAO can be introduced to unlock the privilege.
- Renouncing the contract ownership, and privileged roles.
- Remove functions with elevated centralization risk.

 Understand the project's initial asset distribution. Assets in the liquidity pair should be locked. Assets outside the liquidity pair should be locked with a release schedule.



AUTOMATED ANALYSIS

Symbol	Definition
	Function modifies state
	Function is payable
	Function is internal
	Function is private
	Function is important

```

| **AddressUpgradeable** | Library | |||
|  | isContract | Internal  |  | |
|  | sendValue | Internal   |  | |
|  | functionCall | Internal   |  | |
|  | functionCall | Internal   |  | |
|  | functionCallWithValue | Internal   |  | |
|  | functionCallWithValue | Internal   |  | |
|  | functionStaticCall | Internal  |  | |
|  | functionStaticCall | Internal  |  | |
|  | functionDelegateCall | Internal   |  | |
|  | functionDelegateCall | Internal   |  | |
|  | verifyCallResultFromTarget | Internal  |  | |
|  | verifyCallResult | Internal  |  | |
|  | _revert | Private  |  | |
|||||
| **Initializable** | Implementation | |||
|  | _disableInitializers | Internal   |  | |
|  | _getInitializedVersion | Internal  |  | |
|  | _isInitializing | Internal  |  | |
|||||

```



```

| **ContextUpgradeable** | Implementation | Initializable | |||
|  L | __Context_init | Internal | 🔒 | 🔴 | onlyInitializing |
|  L | __Context_init_unchained | Internal | 🔒 | 🔴 | onlyInitializing |
|  L | _msgSender | Internal | 🔒 | | |
|  L | _msgData | Internal | 🔒 | | |
| |||||
| **OwnableUpgradeable** | Implementation | Initializable, ContextUpgradeable | |||
|  L | __Ownable_init | Internal | 🔒 | 🔴 | onlyInitializing |
|  L | __Ownable_init_unchained | Internal | 🔒 | 🔴 | onlyInitializing |
|  L | owner | Public | ! | | NO ! |
|  L | _checkOwner | Internal | 🔒 | | |
|  L | renounceOwnership | Public | ! | 🔴 | onlyOwner |
|  L | transferOwnership | Public | ! | 🔴 | onlyOwner |
|  L | _transferOwnership | Internal | 🔒 | 🔴 | |
| |||||
| **IERC1822ProxiableUpgradeable** | Interface | | |||
|  L | proxiableUUID | External | ! | | NO ! |
| |||||
| **IERC1967Upgradeable** | Interface | | |||
| |||||
| **IBeaconUpgradeable** | Interface | | |||
|  L | implementation | External | ! | | NO ! |
| |||||
| **StorageSlotUpgradeable** | Library | | |||
|  L | getAddressSlot | Internal | 🔒 | | |
|  L | getBooleanSlot | Internal | 🔒 | | |
|  L | getBytes32Slot | Internal | 🔒 | | |
|  L | getUint256Slot | Internal | 🔒 | | |
|  L | getStringSlot | Internal | 🔒 | | |
|  L | getStringSlot | Internal | 🔒 | | |
|  L | getBytesSlot | Internal | 🔒 | | |
|  L | getBytesSlot | Internal | 🔒 | | |

```



|||||

| ****ERC1967UpgradeUpgradeable**** | Implementation | Initializable, IERC1967Upgradeable |||| ^L | __ERC1967Upgrade_init | Internal 🔒 | 🔴 | onlyInitializing || ^L | __ERC1967Upgrade_init_unchained | Internal 🔒 | 🔴 | onlyInitializing || ^L | _getImplementation | Internal 🔒 | | || ^L | _setImplementation | Private 🔒 | 🔴 | || ^L | _upgradeTo | Internal 🔒 | 🔴 | || ^L | _upgradeToAndCall | Internal 🔒 | 🔴 | || ^L | _upgradeToAndCallUUPS | Internal 🔒 | 🔴 | || ^L | _getAdmin | Internal 🔒 | | || ^L | _setAdmin | Private 🔒 | 🔴 | || ^L | _changeAdmin | Internal 🔒 | 🔴 | || ^L | _getBeacon | Internal 🔒 | | || ^L | _setBeacon | Private 🔒 | 🔴 | || ^L | _upgradeBeaconToAndCall | Internal 🔒 | 🔴 | |

|||||

| ****UUPSUpgradeable**** | Implementation | Initializable, IERC1822ProxiableUpgradeable, ERC1967UpgradeUpgradeable |||| ^L | __UUPSUpgradeable_init | Internal 🔒 | 🔴 | onlyInitializing || ^L | __UUPSUpgradeable_init_unchained | Internal 🔒 | 🔴 | onlyInitializing || ^L | proxiableUUID | External ! | | notDelegated || ^L | upgradeTo | Public ! | 🔴 | onlyProxy || ^L | upgradeToAndCall | Public ! | 🔒 | onlyProxy || ^L | _authorizeUpgrade | Internal 🔒 | 🔴 | |

|||||

| ****IERC165Upgradeable**** | Interface | |||| ^L | supportsInterface | External ! | | NO ! |

|||||

| ****IERC1155Upgradeable**** | Interface | IERC165Upgradeable |||| ^L | balanceOf | External ! | | NO ! || ^L | balanceOfBatch | External ! | | NO ! || ^L | setApprovalForAll | External ! | 🔴 | NO ! |

```

|  | isApprovedForAll | External ! | |NO ! |
|  | safeTransferFrom | External ! | ● |NO ! |
|  | safeBatchTransferFrom | External ! | ● |NO ! |
|||||

```

```

| **IERC20Upgradeable** | Interface | |||
|  | totalSupply | External ! | |NO ! |
|  | balanceOf | External ! | |NO ! |
|  | transfer | External ! | ● |NO ! |
|  | allowance | External ! | |NO ! |
|  | approve | External ! | ● |NO ! |
|  | transferFrom | External ! | ● |NO ! |
|||||

```

```

| **IERC20MetadataUpgradeable** | Interface | IERC20Upgradeable |||
|  | name | External ! | |NO ! |
|  | symbol | External ! | |NO ! |
|  | decimals | External ! | |NO ! |
|||||

```

```

| **ERC20Upgradeable** | Implementation | Initializable, ContextUpgradeable,
IERC20Upgradeable, IERC20MetadataUpgradeable |||
|  | __ERC20_init | Internal 🔒 | ● | onlyInitializing |
|  | __ERC20_init_unchained | Internal 🔒 | ● | onlyInitializing |
|  | name | Public ! | |NO ! |
|  | symbol | Public ! | |NO ! |
|  | decimals | Public ! | |NO ! |
|  | totalSupply | Public ! | |NO ! |
|  | balanceOf | Public ! | |NO ! |
|  | transfer | Public ! | ● |NO ! |
|  | allowance | Public ! | |NO ! |
|  | approve | Public ! | ● |NO ! |
|  | transferFrom | Public ! | ● |NO ! |
|  | increaseAllowance | Public ! | ● |NO ! |
|  | decreaseAllowance | Public ! | ● |NO ! |

```



```

|  | _transfer | Internal | 🟡 | 🔴 | |
|  | _mint | Internal | 🟡 | 🔴 | |
|  | _burn | Internal | 🟡 | 🔴 | |
|  | _approve | Internal | 🟡 | 🔴 | |
|  | _spendAllowance | Internal | 🟡 | 🔴 | |
|  | _beforeTokenTransfer | Internal | 🟡 | 🔴 | |
|  | _afterTokenTransfer | Internal | 🟡 | 🔴 | |

```

```

|||||

```

```

| **IERC721Upgradeable** | Interface | IERC165Upgradeable |||

```

```

|  | balanceOf | External | ! | | NO ! |
|  | ownerOf | External | ! | | NO ! |
|  | safeTransferFrom | External | ! | 🔴 | NO ! |
|  | safeTransferFrom | External | ! | 🔴 | NO ! |
|  | transferFrom | External | ! | 🔴 | NO ! |
|  | approve | External | ! | 🔴 | NO ! |
|  | setApprovalForAll | External | ! | 🔴 | NO ! |
|  | getApproved | External | ! | | NO ! |
|  | isApprovedForAll | External | ! | | NO ! |

```

```

|||||

```

```

| **IERC721MetadataUpgradeable** | Interface | IERC721Upgradeable |||

```

```

|  | name | External | ! | | NO ! |
|  | symbol | External | ! | | NO ! |
|  | tokenURI | External | ! | | NO ! |

```

```

|||||

```

```

| **IERC721ReceiverUpgradeable** | Interface | |||

```

```

|  | onERC721Received | External | ! | 🔴 | NO ! |

```

```

|||||

```

```

| **ERC165Upgradeable** | Implementation | Initializable, IERC165Upgradeable |||

```

```

|  | __ERC165_init | Internal | 🟡 | 🔴 | onlyInitializing |
|  | __ERC165_init_unchained | Internal | 🟡 | 🔴 | onlyInitializing |
|  | supportsInterface | Public | ! | | NO ! |

```

```

|||||

```



| ****MathUpgradeable**** | Library | |||

| L | max | Internal 🔒 | | |

| L | min | Internal 🔒 | | |

| L | average | Internal 🔒 | | |

| L | ceilDiv | Internal 🔒 | | |

| L | mulDiv | Internal 🔒 | | |

| L | mulDiv | Internal 🔒 | | |

| L | sqrt | Internal 🔒 | | |

| L | sqrt | Internal 🔒 | | |

| L | log2 | Internal 🔒 | | |

| L | log2 | Internal 🔒 | | |

| L | log10 | Internal 🔒 | | |

| L | log10 | Internal 🔒 | | |

| L | log256 | Internal 🔒 | | |

| L | log256 | Internal 🔒 | | |

|||||

| ****SignedMathUpgradeable**** | Library | |||

| L | max | Internal 🔒 | | |

| L | min | Internal 🔒 | | |

| L | average | Internal 🔒 | | |

| L | abs | Internal 🔒 | | |

|||||

| ****StringsUpgradeable**** | Library | |||

| L | toString | Internal 🔒 | | |

| L | toString | Internal 🔒 | | |

| L | toHexString | Internal 🔒 | | |

| L | toHexString | Internal 🔒 | | |

| L | toHexString | Internal 🔒 | | |

| L | equal | Internal 🔒 | | |

|||||

| ****ERC721Upgradeable**** | Implementation | Initializable, ContextUpgradeable,
ERC165Upgradeable, IERC721Upgradeable, IERC721MetadataUpgradeable |||



```

| L | __ERC721_init | Internal 🔒 | 🔴 | onlyInitializing |
| L | __ERC721_init_unchained | Internal 🔒 | 🔴 | onlyInitializing |
| L | supportsInterface | Public ! | | NO ! |
| L | balanceOf | Public ! | | NO ! |
| L | ownerOf | Public ! | | NO ! |
| L | name | Public ! | | NO ! |
| L | symbol | Public ! | | NO ! |
| L | tokenURI | Public ! | | NO ! |
| L | _baseURI | Internal 🔒 | | |
| L | approve | Public ! | 🔴 | NO ! |
| L | getApproved | Public ! | | NO ! |
| L | setApprovalForAll | Public ! | 🔴 | NO ! |
| L | isApprovedForAll | Public ! | | NO ! |
| L | transferFrom | Public ! | 🔴 | NO ! |
| L | safeTransferFrom | Public ! | 🔴 | NO ! |
| L | safeTransferFrom | Public ! | 🔴 | NO ! |
| L | _safeTransfer | Internal 🔒 | 🔴 | |
| L | _ownerOf | Internal 🔒 | | |
| L | _exists | Internal 🔒 | | |
| L | _isApprovedOrOwner | Internal 🔒 | | |
| L | _safeMint | Internal 🔒 | 🔴 | |
| L | _safeMint | Internal 🔒 | 🔴 | |
| L | _mint | Internal 🔒 | 🔴 | |
| L | _burn | Internal 🔒 | 🔴 | |
| L | _transfer | Internal 🔒 | 🔴 | |
| L | _approve | Internal 🔒 | 🔴 | |
| L | _setApprovalForAll | Internal 🔒 | 🔴 | |
| L | _requireMinted | Internal 🔒 | | |
| L | _checkOnERC721Received | Private 🔒 | 🔴 | |
| L | _beforeTokenTransfer | Internal 🔒 | 🔴 | |
| L | _afterTokenTransfer | Internal 🔒 | 🔴 | |

```




```
|  L | __unsafe_increaseBalance | Internal | 🔒 | 🔴 | |
```

```
|||||
```

```
| **CountersUpgradeable** | Library | |||
```

```
|  L | current | Internal | 🔒 | | |
```

```
|  L | increment | Internal | 🔒 | 🔴 | |
```

```
|  L | decrement | Internal | 🔒 | 🔴 | |
```

```
|  L | reset | Internal | 🔒 | 🔴 | |
```

```
|||||
```

```
| **SafeMathUpgradeable** | Library | |||
```

```
|  L | tryAdd | Internal | 🔒 | | |
```

```
|  L | trySub | Internal | 🔒 | | |
```

```
|  L | tryMul | Internal | 🔒 | | |
```

```
|  L | tryDiv | Internal | 🔒 | | |
```

```
|  L | tryMod | Internal | 🔒 | | |
```

```
|  L | add | Internal | 🔒 | | |
```

```
|  L | sub | Internal | 🔒 | | |
```

```
|  L | mul | Internal | 🔒 | | |
```

```
|  L | div | Internal | 🔒 | | |
```

```
|  L | mod | Internal | 🔒 | | |
```

```
|  L | sub | Internal | 🔒 | | |
```

```
|  L | div | Internal | 🔒 | | |
```

```
|  L | mod | Internal | 🔒 | | |
```

```
|||||
```

```
| **IPancakePair** | Interface | |||
```

```
|  L | sync | External | ! | 🔴 | NO ! |
```

```
|  L | getReserves | External | ! | | NO ! |
```

```
|||||
```

```
| **DKNFT** | Implementation | Initializable, ERC721Upgradeable, OwnableUpgradeable, UUPSUpgradeable |||
```

```
|  L | initialize | Public | ! | 🔴 | initializer |
```

```
|  L | setUSDTPair | External | ! | 🔴 | onlyOwner |
```

```
|  L | _authorizeUpgrade | Internal | 🔒 | 🔴 | onlyOwner |
```



L	setNFTLimit	Public	!	●	onlyOwner
L	setRewardCondition	Public	!	●	onlyOwner
L	setDragonKingToken	Public	!	●	onlyOwner
L	setBaseURI	Public	!	●	onlyOwner
L	tokenURI	Public	!		NO!
L	_baseURI	Internal	🔒		
L	balanceOfDragonKingToken	Public	!		NO!
L	safeMint	Public	!	●	onlyOwner
L	setSnapshot	Public	!	●	onlyOwner
L	setSupportNFTS	Public	!	●	onlyOwner
L	setNFTExcludeProvider	External	!	●	onlyOwner
L	setProcessGasLimit	Public	!	●	onlyOwner
L	setNftActiveAmount	Public	!	●	onlyOwner
L	getNeedDKAmount	Public	!		NO!
L	nft	Public	!	●	NO!
L	process	External	!	●	NO!



MANUAL REVIEW

Identifier	Definition	Severity
CEN-01	Centralized privileges	Major 🟡
CEN-02	Privileged role can mint NFT assets	

Important onLy0wner centralized privileges are listed below:

```

renounceOwnership()
transferOwnership()
setUSDTPair()
_authorizeUpgrade()
setNFTLimit()
setRewardCondition()
setDragonKingToken()
setBaseURI()
safeMint()
setSnapshot()
setSupportNFTS()
setNFTExcludeProvider()
setProcessGasLimit()
setNftActiveAmount()

```

RECOMMENDATION

Deployers', owners', administrators', and all other privileged roles' private-keys/access-keys/admin-keys should be secured carefully. These entities can have a single point of failure that compromises the security of the project. Manage centralized and privileged roles carefully, review PAGE 09 for more information.

Implement multi-signature wallets: Require multiple signatures from different parties to execute certain sensitive functions within contracts. This spreads control and reduces the risk of a single party having complete authority.




Use a decentralized governance model: Implement a governance model that enables token holders or other stakeholders to participate in decision-making processes. This can include voting on contract upgrades, parameter changes, or any other critical decisions that impact the contract's functioning.

ACKNOWLEDGEMENT

DragonKing team has argued that privileged roles are used as intended, and commented to use multi-signature wallets to manage centralization wherever possible.

INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI
CONFIDENTIAL AUDIT REPORT CONFIDENTIAL AUDIT REPORT CONFIDENTIAL AUDIT REPORT CONFIDENTIAL AUDIT REPORT CONFIDENTIAL



Identifier	Definition	Severity
CEN-09	Use of proxy and upgradeability	Critical 

Privileged role can initiate contract implementation. Contract upgradeability allows privileged roles to change current contract implementation.

```
contract DKNFT is
    Initializable,
    ERC721Upgradeable,
    OwnableUpgradeable,
    UUPSUpgradeable
{
    using SafeMathUpgradeable for uint256;
    using AddressUpgradeable for address;
    using CountersUpgradeable for CountersUpgradeable.Counter;
```

RECOMMENDATION

Test and validate current contract thoroughly before deployment. While proxy contracts are great for robust deployments while maintaining the upgradeable flexibility, proxy codes are prone to new security or logical issues that may compromise the project.

Use `_disableInitializers` in upgradeable implementation to add a safety measure that prevents initializer functions from being called more than once, reducing the risk of unintended behavior or vulnerabilities.

ACKNOWLEDGEMENT

Project team confirmed that contract uses proxy mechanism to have future contract upgradeability, and contract flexibility.



Identifier	Definition	Severity
LOG-01	Lack of appropriate arbitrary boundaries	Minor ●

Below mentioned functions are set without any arbitrary boundaries.

```
setNFTLimit()  
setRewardCondition()  
safeMint()  
setNFTExcludeProvider()  
setProcessGasLimit()  
setNftActiveAmount()
```

INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI
CONFIDENTIAL AUDIT REPORT CONFIDENTIAL AUDIT REPORT CONFIDENTIAL AUDIT REPORT CONFIDENTIAL AUDIT REPORT CONFIDENTIAL

RECOMMENDATION

These functions should be provided appropriate input validation require checks.



Identifier	Definition	Severity
LOG-02	Note regarding front-running	Minor ●

In **DKNFT** contract, there are no transaction sequencing or ordering mechanisms that would make front-running possible. This contract primarily deals with NFT minting, rewards, and internal state updates but does not involve complex interactions with external systems that are susceptible to front-running. However, absence of direct front-running vulnerabilities in this contract does not guarantee the absence of such vulnerabilities, as front-running is a by-product of public blockchain, and public transactions can be front-run easily.

INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI
CONFIDENTIAL AUDIT REPORT CONFIDENTIAL AUDIT REPORT CONFIDENTIAL AUDIT REPORT CONFIDENTIAL AUDIT REPORT CONFIDENTIAL



Identifier	Definition	Severity
LOG-03	Re-entrancy	Major 🟡

Below mentioned functions do not adhere to Checks-Effects-Interactions pattern, and are used without a re-entrancy guard:


```
nft()  
process()
```

RECOMMENDATION

Use mutex or re-entrancy guard to deter re-entrant calls. If possible, replace low-level calls like `call` with higher-level alternative transfer.

Use Checks-Effects-Interactions pattern strictly. Make sure state changes are done before any transfers or external calls.



Identifier	Definition	Severity
COD-05	Missing zero address validation	Minor 

Below mentioned functions are missing zero address input validation:

```
setUSDTPair()  
setDragonKingToken()  
safeMint()  
setSupportNFTS()  
setNFTExcludeProvider()  
nft()
```

INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI
CONFIDENTIAL AUDIT REPORT CONFIDENTIAL AUDIT REPORT CONFIDENTIAL AUDIT REPORT CONFIDENTIAL AUDIT REPORT CONFIDENTIAL

RECOMMENDATION

Validate if the modified address is dead(0) or not.



Identifier	Definition
COD-09	Lack of contract balance withdraw

Smart contract may collect tokens, and ethers from external addresses.

INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI
CONFIDENTIAL AUDIT REPORT CONFIDENTIAL AUDIT REPORT CONFIDENTIAL AUDIT REPORT CONFIDENTIAL AUDIT REPORT CONFIDENTIAL

RECOMMENDATION

Add `withdraw()` function to take out tokens and ethers from the contract.



Identifier	Definition	Severity
COD-10	Direct and indirect dependencies	Unknown 🟡
DKN-01	Trust in token DragonKing token and USDT pair	
DKN-02	External contract dependencies	Major 🟠

Smart contracts are interacting with third party protocols e.g., Market makers, External contracts e.g., token contract, USDT pair, USDT contract, ERC20 contracts, Web 3 applications, Open Zeppelin tools. The scope of the audit treats these entities as black boxes and assumes their functional correctness. However, in the real world, all of them can be compromised, and exploited. Moreover, upgrades in these entities can create severe impacts, e.g., increased transactional fees, deprecation of previous routers, etc.

External dependencies must be monitored regularly. **DKNFT** smart contract should only interact with trusted contracts.

0xB1a8F29b538FaDD9939Fad59Bc0768EEb920fB54
 0x946d3e512067AbF95e340c153c3cEBfB04125B44
 0xa8ED503516A3570Ae426Be4F8412450c236519C5
 0x0529d2760e0DB2D7Ff853B7cBcc5cF2706228005
 0x8546a2CAdA887f7579844E8F4f241fe513036289

RECOMMENDATION

Inspect third party dependencies regularly, and mitigate severe impacts whenever necessary. Make sure external dependencies are trustworthy, secure, and audited.



Identifier	Definition	Severity
COD-11	Volatile logic	Minor ●


- Smart contract interacts with external contracts (ERC20Upgradeable and IPancakePair) without proper error handling.
- In process function, smart contract transfers tokens to NFT owners without checking if they are contracts or not.
- In process function, setting fixed gas limits can lead to transaction failures.

INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI
CONFIDENTIAL AUDIT REPORT CONFIDENTIAL AUDIT REPORT CONFIDENTIAL AUDIT REPORT CONFIDENTIAL AUDIT REPORT CONFIDENTIAL

RECOMMENDATION

Fix logical non-conformities.



Identifier	Definition	Severity
COD-12	Lack of event-driven architecture	Minor 

Smart contracts use function calls to update state, which can make it difficult to track and analyze changes to contracts over time.

INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI
CONFIDENTIAL AUDIT REPORT CONFIDENTIAL AUDIT REPORT CONFIDENTIAL AUDIT REPORT CONFIDENTIAL AUDIT REPORT

RECOMMENDATION

Use events to track state changes. Events improve transparency and provide a more granular view of contracts' activity.



Identifier	Definition	
VOL-01	Potential DoS attack	Medium 🟡
DKN-03	Inadequate function access restrictions	


nft() function has no access restrictions. If it's spammed with invalid NFT addresses, it may lead to high gas consumption and denial-of-service (DoS) attacks.

TERFI
CONFIDENTIALINTERFI
CONFIDENTIAL

RECOMMENDATION

Implement rate limiting or access restrictions in mentioned function.



Identifier	Definition	Severity
COM-01	Floating compiler status	Minor 

Compiler is set to ^0.8.19

INTERFI
CONFIDENTIAL

INTERFI
CONFIDENTIAL


RECOMMENDATION

Pragma should be fixed to the version that you're indenting to deploy your contracts with.

RESOLUTION

DragonKing team will deploy contracts with stable compiler version.



Identifier	Definition	Severity
COM-04	Potential resource exhaustion errors	Minor 

Below mentioned functions may throw out of gas errors upon executing:

```
setNFTExcludeProvider()
```

```
process()
```

INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI
CONFIDENTIAL AUDIT REPORT CONFIDENTIAL AUDIT REPORT CONFIDENTIAL AUDIT REPORT CONFIDENTIAL AUDIT REPORT CONFIDENTIAL

RECOMMENDATION

Set upper bounds for multi-address calls.



DISCLAIMERS

InterFi Network provides the easy-to-understand audit of solidity source codes (commonly known as smart contracts).

The smart contract for this particular audit was analyzed for common contract vulnerabilities, and centralization exploits. This audit report makes no statements or warranties on the security of the code. This audit report does not provide any warranty or guarantee regarding the absolute bug-free nature of the smart contract analyzed, nor do they provide any indication of the client's business, business model or legal compliance. This audit report does not extend to the compiler layer, any other areas beyond the programming language, or other programming aspects that could present security risks. Cryptographic tokens are emergent technologies, they carry high levels of technical risks and uncertainty. You agree that your access and/or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. This audit report could include false positives, false negatives, and other unpredictable results.

CONFIDENTIALITY

This report is subject to the terms and conditions (including without limitations, description of services, confidentiality, disclaimer and limitation of liability) outlined in the scope of the audit provided to the client. This report should not be transmitted, disclosed, referred to, or relied upon by any individual for any purpose without InterFi Network's prior written consent.

NO FINANCIAL ADVICE

This audit report does not indicate the endorsement of any particular project or team, nor guarantees its security. No third party should rely on the reports in any way, including to make any decisions to buy or sell a product, service or any other asset. The information provided in this report does not constitute investment advice, financial advice, trading advice, or any other sort of advice and you should not treat any of the report's content as such. This audit report should not be used in any way



to make decisions around investment or involvement. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort.

FOR AVOIDANCE OF DOUBT, SERVICES, INCLUDING ANY ASSOCIATED AUDIT REPORTS OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.

TECHNICAL DISCLAIMER

ALL SERVICES, AUDIT REPORTS, SMART CONTRACT AUDITS, OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF ARE PROVIDED "AS IS" AND "AS AVAILABLE" AND WITH ALL FAULTS AND DEFECTS WITHOUT WARRANTY OF ANY KIND. TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, INTERFI NETWORK HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESSED, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO SERVICES, AUDIT REPORT, OR OTHER MATERIALS. WITHOUT LIMITING THE FOREGOING, INTERFI NETWORK SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM THE COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

WITHOUT LIMITING THE FOREGOING, INTERFI NETWORK MAKES NO WARRANTY OF ANY KIND THAT ALL SERVICES, AUDIT REPORTS, SMART CONTRACT AUDITS, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF, WILL MEET THE CLIENT'S OR ANY OTHER INDIVIDUAL'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULT, BE COMPATIBLE OR WORK WITH ANY SOFTWARE, SYSTEM, OR OTHER SERVICES, OR BE SECURE, ACCURATE, COMPLETE, FREE OF HARMFUL CODE, OR ERROR-FREE.

TIMELINESS OF CONTENT

The content contained in this audit report is subject to change without any prior notice. InterFi Network does not guarantee or warrant the accuracy, timeliness, or completeness of any report you access using the internet or other means, and assumes no obligation to update any information following the publication.



LINKS TO OTHER WEBSITES

This audit report provides, through hypertext or other computer links, access to websites and social accounts operated by individuals other than InterFi Network. Such hyperlinks are provided for your reference and convenience only and are the exclusive responsibility of such websites' and social accounts' owners. You agree that InterFi Network is not responsible for the content or operation of such websites and social accounts and that InterFi Network shall have no liability to you or any other person or entity for the use of third-party websites and social accounts. You are solely responsible for determining the extent to which you may use any content at any other websites and social accounts to which you link from the report.

INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI
CONFIDENTIAL AUDIT REPORT CONFIDENTIAL AUDIT REPORT CONFIDENTIAL AUDIT REPORT CONFIDENTIAL AUDIT REPORT CONFIDENTIAL



ABOUT INTERFI NETWORK

InterFi Network provides intelligent blockchain solutions. We provide solidity development, testing, and auditing services. We have developed 150+ solidity codes, audited 1000+ smart contracts, and analyzed 500,000+ code lines. We have worked on major public blockchains e.g., Ethereum, Binance, Cronos, Doge, Polygon, Avalanche, Metis, Fantom, Bitcoin Cash, Velas, Oasis, etc.

InterFi Network is built by engineers, developers, UI experts, and blockchain enthusiasts. Our team currently consists of 4 core members, and 6+ casual contributors.

Website: <https://interfi.network>

Email: hello@interfi.network

GitHub: <https://github.com/interfinetwork>

Telegram (Engineering): <https://t.me/interfiaudits>

Telegram (Onboarding): <https://t.me/interfisupport>



 interfinetwork

 hello@interfi.network

 <https://interfi.network>

SMART CONTRACT AUDITS | SOLIDITY DEVELOPMENT AND TESTING
RELENTLESSLY SECURING PUBLIC AND PRIVATE BLOCKCHAINS