

SMART CONTRACT SECURITY AUDIT OF **DOGS CREW**



SMART CONTRACT AUDIT | SOLIDITY DEVELOPMENT & TESTING | PROJECT EVALUATION

RELENTLESSLY SECURING THE PUBLIC BLOCKCHAIN

Audit Introduction

| | |
|---------------------------|---|
| Auditing Firm | InterFi Network |
| Audit Architecture | InterFi Echelon Auditing Standard |
| Language | Solidity |
| Client Firm | Dogs Crew |
| Website | https://www.dogscrowgame.com/ |
| Telegram | https://t.me/DogsCrewAnnouncements/ |
| Twitter | https://twitter.com/DogsCrewGame/ |
| Instagram | https://instagram.com/dogscrownft/ |
| Discord | https://discord.gg/cnGyqPHkHB/ |
| Report Date | February 27, 2022 |

About Dogs Crew

The project is an NFT click to earn game with a stray dog theme (hence its name DOGS CREW), We will launch the token officially as soon as it is audited, we have KYC of all the components of the project.



Audit Summary

InterFi team has performed a line-by-line manual analysis and automated review of the smart contract. The smart contract was analyzed mainly for common smart contract vulnerabilities, exploits, and manipulation hacks. According to the smart contract audit:

- ❖ Dogs Crew's solidity source code has **MEDIUM RISK SEVERITY**
- ❖ Dogs Crew's smart contract has an **ACTIVE OWNERSHIP**
- ❖ Important owner privileges – **PAUSE – UNPAUSE CONTRACT, MINT, BURN, SET FEES, SET SWAP STATUS, BLACKLIST, SET PENALTY**
- ❖ Dogs Crew's smart contract owner has multiple "Write Contract" privileges. Centralization risk correlated to the active owner is **HIGH**

Be aware that smart contracts deployed on the blockchain aren't resistant to internal exploit, external vulnerability, or hack. For a detailed understanding of risk severity, source code vulnerability, functional hack, and audit disclaimer, kindly refer to the audit.

🔴 Token Contract address: **0xa0B5A4C83bDD66B7e00cCe277f315aB08b661AD1**

🔗 Blockchain: **Binance Smart Chain**

✅ Verify the authenticity of this report on InterFi's GitHub: <https://github.com/interfinetwork>



Table Of Contents

Audit Information

| | |
|------------------|---|
| Audit Scope..... | 5 |
|------------------|---|

Echelon Audit Standard

| | |
|--------------------------|---|
| Audit Methodology | 6 |
| Risk Classification..... | 8 |

Smart Contract Risk Assessment

| | |
|--------------------------------|----|
| Static Analysis..... | 9 |
| Software Analysis | 11 |
| Manual Analysis..... | 14 |
| SWC Attacks..... | 17 |
| Risk Status & Radar Chart..... | 19 |

Audit Summary

| | |
|-------------------------|----|
| Auditor's Verdict | 20 |
|-------------------------|----|

Legal Advisory

| | |
|----------------------------|----|
| Important Disclaimer | 21 |
| About InterFi Network..... | 22 |



Audit Scope

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

❖ DogsCrew.sol

Solidity Source Code On Blockchain (Verified Contract Source Code)

<https://bscscan.com/address/0xa0B5A4C83bDD66B7e00cCe277f315aB08b661AD1#code>

Contract Name: DevToken

Compiler Version: v0.8.4

Optimization Enabled: Yes with 200 runs

Solidity Source Code On InterFi GitHub

<https://github.com/interfinetwork/audited-codes/blob/main/DogsCrew.sol>

SHA-1 Hash

Solidity source code is audited at hash #0fde1b93ee05dd2e153e3058bcd9e7421950a503



Audit Methodology

The scope of this report is to audit the smart contract source code of Dogs Crew. InterFi has scanned the contract and reviewed the project for common vulnerabilities, exploits, hacks, and back-doors. Below is the list of commonly known smart contract vulnerabilities, exploits, and hacks:

Category

Smart Contract Vulnerabilities

- ❖ Re-entrancy
- ❖ Unhandled Exceptions
- ❖ Transaction Order Dependency
- ❖ Integer Overflow
- ❖ Unrestricted Action
- ❖ Incorrect Inheritance Order
- ❖ Typographical Errors

Requirement Violation

- ❖ Ownership Takeover
- ❖ Gas Limit and Loops

Source Code Review

- ❖ Deployment Consistency
- ❖ Repository Consistency
- ❖ Data Consistency
- ❖ Token Supply Manipulation

Functional Assessment

- ❖ Access Control and Authorization
- ❖ Operations Trail and Event Generation
- ❖ Assets Manipulation
- ❖ Liquidity Access



InterFi's Echelon Audit Standard

The aim of InterFi's "Echelon" standard is to analyze the smart contract and identify the vulnerabilities and the hacks in the smart contract. Mentioned are the steps used by ECHELON-1 to assess the smart contract:

1. Solidity smart contract source code reviewal:
 - ❖ Review of the specifications, sources, and instructions provided to InterFi to make sure we understand the size, scope, and functionality of the smart contract.
 - ❖ Manual review of code, which is the process of reading source code line-by-line to identify potential vulnerabilities.
2. Static, Manual, and Software analysis:
 - ❖ Test coverage analysis is the process of determining whether the test cases are covering the code and how much code is exercised when we run those test cases.
 - ❖ Symbolic execution is analyzing a program to determine what inputs cause each part of a program to execute.
3. Best practices review, which is a review of the smart contracts to improve efficiency, effectiveness, clarify, maintainability, security, and control based on the established industry and academic practices, recommendations, and research.
4. Specific, itemized, actionable recommendations to help you take steps to secure your smart contracts

Automated 3P frameworks used to assess the smart contract vulnerabilities

- ❖ Slither
- ❖ Consensys MythX, Mythril
- ❖ SWC Registry
- ❖ Solidity Coverage
- ❖ Open Zeppelin Code Analyzer
- ❖ Solidity Code Compiler



Risk Classification

Smart contracts are generally designed to manipulate and hold funds denominated in ETH/BNB. This makes them very tempting attack targets, as a successful attack may allow the attacker to directly steal funds from the contract. Below are the typical risk levels of a smart contract:

Vulnerable: A contract is vulnerable if it has been flagged by a static analysis tool as such. As we will see later, this means that some contracts may be vulnerable because of a false positive.

Exploitable: A contract is exploitable if it is vulnerable and the vulnerability could be exploited by an external attacker. For example, if the “vulnerability” flagged by a tool is in a function that requires owning the contract, it would be vulnerable but not exploitable.

Exploited: A contract is exploited if it received a transaction on the main network which triggered one of its vulnerabilities. Therefore, a contract can be vulnerable or even exploitable without having been exploited.

Smart Contract Security Audit



































| Risk severity | Meaning |
|------------------------|--|
| ! High | This level vulnerabilities could be exploited easily and can lead to asset loss, data loss, asset, or data manipulation. They should be fixed right away. |
| ! Medium | This level vulnerabilities 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 |
| ! Low | This level vulnerabilities should be fixed, as they carry an inherent risk of future exploits, and hacks which may or may not impact the smart contract execution. |
| ! Informational | This level vulnerabilities can be ignored. They are code style violations and informational statements in the code. They may not affect the smart contract execution |



Static Analysis

| Symbol | Meaning |
|---|--------------------------|
|  | Function can be modified |
|  | Function is payable |
|  | Function is locked |
|  | Function can be accessed |
| ! | Important functionality |

```

| **DevToken** | Implementation | Context, Ownable, Pausable, Establishments |||
| L | <Constructor> | Public ! |  | NO ! |
| L | decimals | External ! |  | NO ! |
| L | symbol | External ! |  | NO ! |
| L | name | External ! |  | NO ! |
| L | totalSupply | External ! |  | NO ! |
| L | balanceOf | External ! |  | NO ! |
| L | balanceOfDogsUSD | External ! |  | NO ! |
| L | _mint | Internal   |
| L | _burn | Internal   |
| L | burn | Public ! |  | onlyOwner |
| L | mint | Public ! |  | onlyOwner |
| L | transfer | External ! |  | whenNotPaused |
| L | _transfer | Internal   |
| L | getOwner | External ! |  | NO ! |
| L | allowance | External ! |  | NO ! |
| L | approve | External ! |  | whenNotPaused |
| L | _approve | Internal   |
| L | transferFrom | External ! |  | whenNotPaused |
| L | increaseAllowance | Public ! |  | whenNotPaused |
| L | decreaseAllowance | Public ! |  | whenNotPaused |
| L | editBlackList | Public ! |  | onlyOwner |
| L | blockedAccount | Public ! |  | NO ! |
| L | swaDOUSDFromDOGSC | Public ! |  | whenNotPaused |
| L | lifeContracts | Public ! |  | NO ! |
| L | sendAttack | Public ! |  | NO ! |
| L | calculateProfit | Internal  |
| L | randMod | Public ! |  | NO ! |
| L | setAttackActive | Public ! |  | onlyOwner |
| L | setSwapActive | Public ! |  | onlyOwner |
| L | setPriceSwapActive | Public ! |  | onlyOwner |

```



```

| L | changePercentageDamaged | Public ! | ● | onlyOwner |
| L | changePenalty | Public ! | ● | onlyOwner |
| L | withdraw | Public ! | ● | onlyOwner |
|||||
| **Context** | Implementation | |||
| L | <Constructor> | Public ! | ● | NO ! |
| L | _msgSender | Internal 🔒 | | |
| L | _msgData | Internal 🔒 | | |
|||||
| **Ownable** | Implementation | Context |||
| L | <Constructor> | Public ! | ● | NO ! |
| L | owner | Public ! | | NO ! |
| L | isOwner | Public ! | | NO ! |
| L | renounceOwnership | Public ! | ● | onlyOwner |
| L | transferOwnership | Public ! | ● | onlyOwner |
| L | _transferOwnership | Internal 🔒 | ● | |
|||||
| **Pausable** | Implementation | Ownable |||
| L | pause | Public ! | ● | onlyOwner whenNotPaused |
| L | unpause | Public ! | ● | onlyOwner whenPaused |
| L | getStatusPause | Public ! | | NO ! |
|||||
| **Establishments** | Implementation | Ownable |||
| L | registerEstablishment | Public ! | ● | onlyOwner |
| L | updateEstablishment | Public ! | ● | onlyOwner |
| L | deleteEstablishment | Public ! | ● | onlyOwner |
| L | getEstablishmentCount | Public ! | | NO ! |
| L | getEstablishment | Public ! | | NO ! |
|||||
| **SafeMath** | 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 🔒 | | |

```



Software Analysis

Function Signatures

```

39509351 => increaseAllowance(address,uint256)
313ce567 => decimals()
95d89b41 => symbol()
06fdde03 => name()
18160ddd => totalSupply()
70a08231 => balanceOf(address)
cd5047b0 => balanceOfDogsUSD(address)
4e6ec247 => _mint(address,uint256)
6161eb18 => _burn(address,uint256)
9dc29fac => burn(address,uint256)
40c10f19 => mint(address,uint256)
a9059cbb => transfer(address,uint256)
30e0789e => _transfer(address,address,uint256)
893d20e8 => getOwner()
dd62ed3e => allowance(address,address)
095ea7b3 => approve(address,uint256)
104e81ff => _approve(address,address,uint256)
23b872dd => transferFrom(address,address,uint256)
a457c2d7 => decreaseAllowance(address,uint256)
de57d5a5 => editBlackList(address,bool)
a152d160 => blockedAccount(address)
e127032f => swaD0USDFromD0GSC(uint256,bool)
6e56ea1c => lifeContracts(uint256,string)
84e75e33 => sendAttack(uint256,uint256)
e972261d => calculateProfit(uint256,uint256)
805553e8 => randMod(uint256)
59527a18 => setAttackActive(bool)
a44e49bb => setSwapActive(bool)
5502b329 => setPriceSwapActive(uint256)
4a9fd273 => changePercentageDamaged(uint256)
4a22a125 => changePenalty(uint256)
3ccfd60b => withdraw()
119df25f => _msgSender()
8b49d47e => _msgData()
8da5cb5b => owner()
8f32d59b => isOwner()
715018a6 => renounceOwnership()
f2fde38b => transferOwnership(address)
d29d44ee => _transferOwnership(address)
8456cb59 => pause()
3f4ba83a => unpause()
50b7b447 => getStatusPause()
4690e61c => registerEstablishment(string,uint256,uint256,uint256,uint256,uint256,bool,uint256)
743afc7b => updateEstablishment(string,uint256,uint256,uint256,uint256,uint256,bool,uint256)
d66e4588 => deleteEstablishment(uint256)

```



```
e6ec5092 => getEstablishmentCount()
42d65ad1 => getEstablishment(uint256)
884557bf => tryAdd(uint256,uint256)
a29962b1 => trySub(uint256,uint256)
6281efa4 => tryMul(uint256,uint256)
736ecb18 => tryDiv(uint256,uint256)
38dc0867 => tryMod(uint256,uint256)
771602f7 => add(uint256,uint256)
b67d77c5 => sub(uint256,uint256)
c8a4ac9c => mul(uint256,uint256)
a391c15b => div(uint256,uint256)
f43f523a => mod(uint256,uint256)
e31bdc0a => sub(uint256,uint256,string)
b745d336 => div(uint256,uint256,string)
71af23e8 => mod(uint256,uint256,string)
```

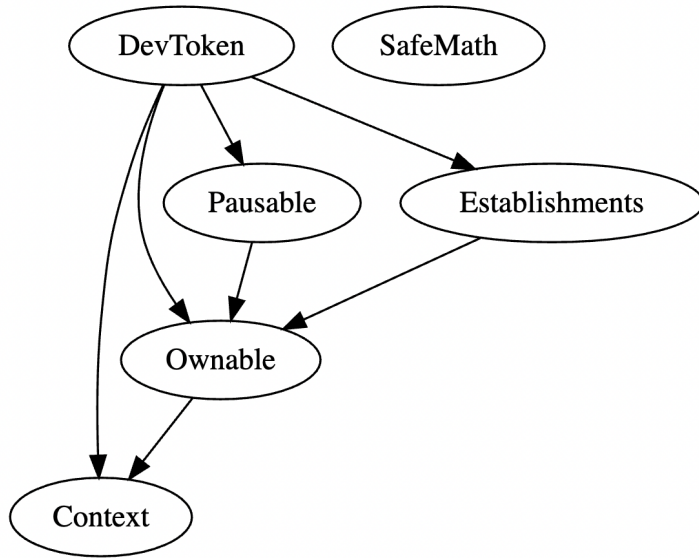
InterFi

.....

Smart Contract Security Audit



Inheritance Graph



InterFi

Smart Contract
Security Audit



Manual Analysis

| Function | Description | Tested | Verdict |
|---------------------------|---|--------|-----------------|
| Total Supply | provides information about the total token supply | Yes | Passed |
| Balance Of | provides account balance of the owner's account | Yes | Passed |
| Transfer | executes transfers of a specified number of tokens to a specified address | Yes | Passed |
| Approve | allow a spender to withdraw a set number of tokens from a specified account | Yes | Passed |
| Allowance | returns a set number of tokens from a spender to the owner | Yes | Passed |
| Burn | executes transfers of a specified number of tokens to a burn address | Yes | Passed |
| Mint | executes the creation of a specified number of tokens and adds it to the total supply | Yes | ! Medium |
| Blacklist | stops specified wallets from interacting with the smart contract function modules | Yes | ! Low |
| Pause | stops or locks all function modules of the smart contract | Yes | ! Low |
| Transfer Ownership | executes transfer of contract ownership to a specified wallet | Yes | Passed |
| Renounce Ownership | executes transfer of contract ownership to a dead address | Yes | Passed |



Best Practices

- ❖ The smart contract utilizes "SafeMath" function to avoid common smart contract vulnerabilities.

```
string private _name = "DogsCrew";
library SafeMath {
function add(uint256 a, uint256 b) internal pure returns (uint256) {
    uint256 c = a + b;
    require(c >= a, "SafeMath: addition overflow");

function sub(uint256 a, uint256 b) internal pure returns (uint256) {
    return sub(a, b, "SafeMath: subtraction overflow");

    uint256 c = a * b;
    require(c / a == b, "SafeMath: multiplication overflow");

    return c;

function div(uint256 a, uint256 b) internal pure returns (uint256) {
    return div(a, b, "SafeMath: division by zero");

function mod(uint256 a, uint256 b) internal pure returns (uint256) {
    return mod(a, b, "SafeMath: modulo by zero");
```

Smart Contract Security Audit

Note

- ❖ Active smart contract owner: 0x4c54d42ab8a14e0142df679a075e4c4de767d8d0
- ❖ Be aware that active smart contract owner privileges constitute an elevated impact to smart contract safety and security.
- ❖ Smart contract owner can **pause or un-pause** the smart contract function modules.
- ❖ Smart contract owner can **set swap status**, this function module can be used to stop the users from buying or selling the assets.

```
function setSwapActive(bool val) public onlyOwner {
    swapActive = val;
```



- ❖ Smart contract owner can **blacklist** certain wallets from interacting with the contract function modules.

```
function editBlackList(address _address, bool _block)
    public
    onlyOwner
    blacklist[_address] = _block;
```

- ❖ Smart contract owner can mint tokens after initial deployment.

```
function _mint(address account, uint256 amount) internal {
    require(account != address(0), "DevToken: cannot mint to zero address");
    // Increase total supply
    _totalSupply = _totalSupply.add(amount);
```

- ❖ Smart contract has a **low severity issue** which may or may not create any functional vulnerability.

```
.....
{
    "resource": "/DogsCrew.sol",
    "owner": "_generated_diagnostic_collection_name_#0",
    "severity": 8, (! Low Severity)
    " Expected identifier, got 'LParen'",
    "source": "solc",
}
```



SWC Attacks

| SWC ID | Description | Verdict |
|---------|---------------------------------------|-----------------|
| SWC-101 | Integer Overflow and Underflow | Passed |
| SWC-102 | Outdated Compiler Version | ! Informational |
| SWC-103 | Floating Pragma | Passed |
| SWC-104 | Unchecked Call Return Value | Passed |
| SWC-105 | Unprotected Ether Withdrawal | Passed |
| SWC-106 | Unprotected SELF-DESTRUCT Instruction | Passed |
| SWC-107 | Re-entrancy | Passed |
| SWC-108 | State Variable Default Visibility | Passed |
| SWC-109 | Uninitialized Storage Pointer | Passed |
| SWC-110 | Assert Violation | Passed |
| SWC-111 | Use of Deprecated Solidity Functions | Passed |
| SWC-112 | Delegate Call to Untrusted Callee | Passed |
| SWC-113 | DoS with Failed Call | Passed |
| SWC-114 | Transaction Order Dependence | Passed |
| SWC-115 | Authorization through tx.origin | Passed |
| SWC-116 | Block values as a proxy for time | Passed |
| SWC-117 | Signature Malleability | Passed |
| SWC-118 | Incorrect Constructor Name | ! Low |

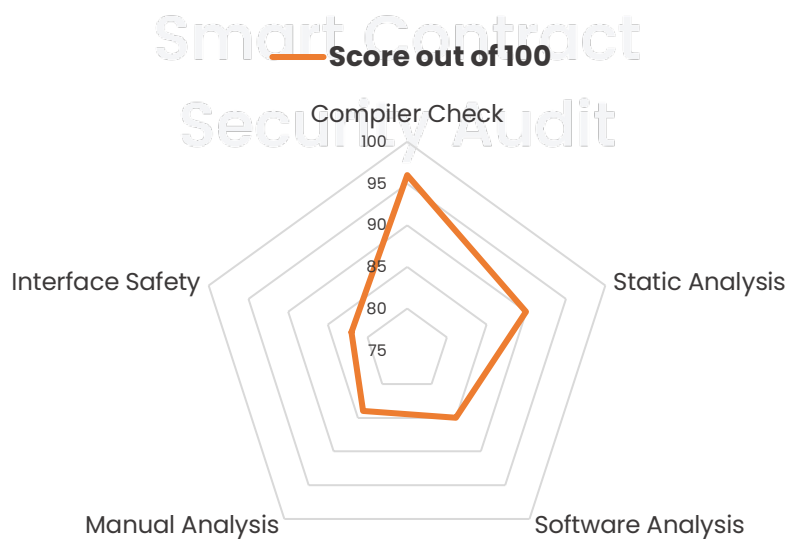


| | | |
|----------------|---|---------------|
| SWC-119 | Shadowing State Variables | Passed |
| SWC-120 | Weak Sources of Randomness from Chain Attributes | Passed |
| SWC-121 | Missing Protection against Signature Replay Attacks | Passed |
| SWC-122 | Lack of Proper Signature Verification | Passed |
| SWC-123 | Requirement Violation | Passed |
| SWC-124 | Write to Arbitrary Storage Location | Passed |
| SWC-125 | Incorrect Inheritance Order | Passed |
| SWC-126 | Insufficient Gas Griefing | Passed |
| SWC-127 | Arbitrary Jump with Function Type Variable | Passed |
| SWC-128 | DoS With Block Gas Limit | Passed |
| SWC-129 | Typographical Error | ! Low |
| SWC-130 | Right-To-Left-Override control character (U+202E) | Passed |
| SWC-131 | Presence of unused variables | Passed |
| SWC-132 | Unexpected Ether balance | Passed |
| SWC-133 | Hash Collisions With Multiple Variable Length Arguments | Passed |
| SWC-134 | Message call with the hardcoded gas amount | Passed |
| SWC-135 | Code With No Effects (Irrelevant/Dead Code) | Passed |
| SWC-136 | Unencrypted Private Data On-Chain | Passed |



Risk Status & Radar Chart

| Risk Severity | Status |
|------------------------|--|
| ! High | No high severity issues identified |
| ! Medium | 1 medium severity issues identified |
| ! Low | 4 low severity issues identified <ul style="list-style-type: none"> ❖ Please Review Report |
| ! Informational | 2 informational severity issues identified <ul style="list-style-type: none"> ❖ Active Ownership ❖ Outdated Compiler |
| Verified | 54 functions and instances verified and checked |



Auditor's Verdict

InterFi team has performed a line-by-line manual analysis and automated review of the smart contract. The smart contract was analyzed mainly for common smart contract vulnerabilities, exploits, and manipulation hacks.

- ❖ Dogs Crew's solidity source code has **MEDIUM RISK SEVERITY**
- ❖ Dogs Crew's smart contract has an **ACTIVE OWNERSHIP**
- ❖ Dogs Crew's smart contract owner has multiple "Write Contract" privileges. Centralization risk correlated to the active owner is **HIGH**

InterFi

Note for stakeholders

- Smart Contract Security Audit
- ❖ Be aware that active smart contract owner privileges constitute an elevated impact on smart contract safety and security.
 - ❖ If the smart contract is not deployed on any blockchain at the time of the audit, the contract can be modified or altered before blockchain development. Verify contract's deployment status in the audit report.
 - ❖ Make sure that the project team's KYC/identity is verified by an independent firm.
 - ❖ Always check if the contract's liquidity is locked. A longer liquidity lock plays an important role in the project's longevity. It is recommended to have multiple liquidity providers.
 - ❖ Examine the unlocked token supply in the owner, developer, or team's private wallets. Understand the project's tokenomics, and make sure the tokens outside of the LP Pair are vested or locked for a longer period.
 - ❖ Ensure that the project's official website is hosted on a trusted platform, and is using an active SSL certificate. The website's domain should be registered for a longer period.



Important Disclaimer

InterFi Network provides contract development, testing, auditing and project evaluation services for blockchain projects. The purpose of the audit is to analyze the on-chain smart contract source code and to provide a basic overview of the project. **This report should not be transmitted, disclosed, referred to, or relied upon by any person for any purpose without InterFi's prior written consent.**

InterFi provides the easy-to-understand assessment of the project, and the smart contract (otherwise known as the source code). The audit makes no statements or warranties on the security of the code. It also cannot be considered as enough assessment regarding the utility and safety of the code, bug-free status, or any other statements of the contract. While we have used all the data at our disposal to provide the transparent analysis, it is important to note that you should not rely on this report only – we recommend proceeding with several independent audits and a public bug bounty program to ensure the security of smart contracts. **Be aware that smart contracts deployed on a blockchain aren't resistant to external vulnerability, or a hack. Be aware that active smart contract owner privileges constitute an elevated impact on smart contract safety and security. Therefore, InterFi does not guarantee the explicit security of the audited smart contract.**

The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed.

This report should not be considered as an endorsement or disapproval of any project or team.

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. Do conduct your due diligence and consult your financial advisor before making any investment decisions.



About InterFi Network

InterFi Network provides intelligent blockchain solutions. InterFi is developing an ecosystem that is seamless and responsive. Some of our services: Blockchain Security, Token Launchpad, NFT Marketplace, etc. **InterFi's mission is to interconnect multiple services like Blockchain Security, DeFi, Gaming, and Marketplace under one ecosystem that is seamless, multi-chain compatible, scalable, secure, fast, responsive, and easy to use.**

InterFi is built by a decentralized team of UI experts, contributors, engineers, and enthusiasts from all over the world. Our team currently consists of 6+ core team members, and 10+ casual contributors. **InterFi provides manual, static, and automatic smart contract analysis, to ensure that project is checked against known attacks and potential vulnerabilities.**

To learn more, visit <https://interfi.network>

To view our audit portfolio, visit <https://github.com/interfinetwork>....

To book an audit, message <https://t.me/interfiaudits>





@INTERFINETWORK

RELENTLESSLY SECURING THE PUBLIC BLOCKCHAIN | MADE IN CANADA 🇨🇦