InterFi NETWORK

SMART CONTRACT AUDIT

interfinetwork

hello@interfi.network

https://interfi.network

PREPARED FOR

HAVOC V2

INTRODUCTION

Auditing Firm	InterFi Network
Client Firm	Havoc V2
Methodology	Automated Analysis, Manual Code Review
Language	Solidity
Contract	0x2bb2A7EA643C31A34024515D6Dd6295A5F241c1d
Blockchain	Ethereum Chain
Centralization	Active ownership
Commit	a31d02fc0737dc397630951dfe7e5a5f0071e547
Website	https://www.havocv2.com/
Telegram	https://t.me/HAVOCERC_PORTAL/
Twitter	https://twitter.com/HAVOC_ERC/
Medium	https://medium.com/@havocerc/
Report Date	September 04, 2022

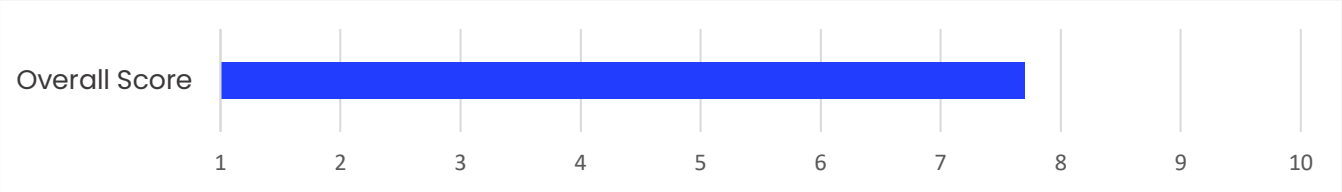
ℹ️ Verify the authenticity of this report on our website: https://www.interfi.network/audits

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 🟢
Open	0	2	4	6
Resolved	0	0	0	0
Status Unknown	0			
Noteworthy Centralized Privileges	Blacklist, Change Total Fees, Set Fees, Set Transaction Limit, Set Wallet Limit, Change Reflection			

Havoc V2's smart contract source codes have achieved the following score: **7.7**



ℹ 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.

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

TABLE OF CONTENTS

TABLE OF CONTENTS 4

SCOPE OF WORK 5

AUDIT METHODOLOGY 6

RISK CATEGORIES 8

CENTRALIZED PRIVILEGES 9

AUTOMATED ANALYSIS 10

INHERITANCE GRAPH 14

MANUAL REVIEW 15

DISCLAIMERS 31

ABOUT INTERFI NETWORK 34

SCOPE OF WORK

InterFi was consulted by Havoc V2 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:

- HAVOCV2.sol

ℹ️ 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://etherscan.io/address/0x2bb2a7ea643c31a34024515d6dd6295a5f241c1d#code	
Contract Name	HAVOCV2
Compiler Version	0.8.13
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	○ 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.

ℹ️ 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.

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

Status Type	Definition
Open	Risks are acknowledged, but not fixed.
Resolved	Risks are acknowledged and fixed.
Unknown	Risks have unknown impacts on contract logic.

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.

ℹ️ 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

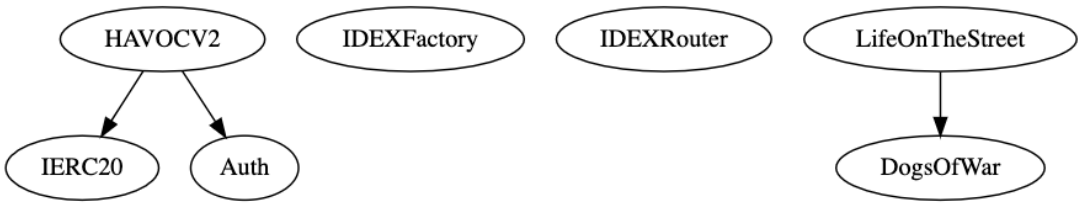
IERC20	Interface			
└	totalSupply	External !		NO!
└	decimals	External !		NO!
└	symbol	External !		NO!
└	name	External !		NO!
└	getOwner	External !		NO!
└	balanceOf	External !		NO!
└	transfer	External !	🛑	NO!
└	allowance	External !		NO!
└	approve	External !	🛑	NO!
└	transferFrom	External !	🛑	NO!
Auth	Implementation			
└	<Constructor>	Public !	🛑	NO!
└	isOwner	Public !		NO!
└	transferOwnership	Public !	🛑	onlyOwner
IDEXFactory	Interface			
└	createPair	External !	🛑	NO!
IDEXRouter	Interface			

└	factory	External ❗		NO❗
└	WETH	External ❗		NO❗
└	addLiquidity	External ❗	🛑	NO❗
└	addLiquidityETH	External ❗	💵	NO❗
└	swapExactTokensForTokensSupportingFeeOnTransferTokens	External ❗	🛑	NO❗
└	swapExactETHForTokensSupportingFeeOnTransferTokens	External ❗	💵	NO❗
└	swapExactTokensForETHSupportingFeeOnTransferTokens	External ❗	🛑	NO❗
DogsOfWar	Interface			
└	setDistributionCriteria	External ❗	🛑	NO❗
└	setShare	External ❗	🛑	NO❗
└	deposit	External ❗	💵	NO❗
└	process	External ❗	🛑	NO❗
└	cryHavoc	External ❗	🛑	NO❗
└	changeReflection	External ❗	🛑	NO❗
LifeOnTheStreet	Implementation	DogsOfWar		
└	<Constructor>	Public ❗	🛑	NO❗
└	<Receive Ether>	External ❗	💵	NO❗
└	changeReflection	External ❗	🛑	onlyToken
└	setDistributionCriteria	External ❗	🛑	onlyToken
└	setShare	External ❗	🛑	onlyToken
└	deposit	Public ❗	💵	NO❗
└	process	External ❗	🛑	NO❗
└	shouldDistribute	Public ❗		NO❗
└	distributeDividend	Internal 🔒	🛑	
└	cryHavoc	External ❗	🛑	onlyToken
└	getUnpaidEarnings	Public ❗		NO❗
└	getCumulativeDividends	Internal 🔒		
└	addShareholder	Internal 🔒	🛑	
└	removeShareholder	Internal 🔒	🛑	

HAVOCV2	Implementation	IERC20, Auth		
└	<Constructor>	Public ❗	🛑	Auth
└	<Receive Ether>	External ❗	💵	NO❗
└	setBots	External ❗	🛑	onlyOwner
└	changeReflection	External ❗	🛑	onlyOwner
└	openTrading	External ❗	🛑	onlyOwner
└	changeTotalFees	External ❗	🛑	onlyOwner
└	changeFeeAllocation	External ❗	🛑	onlyOwner
└	changeTxLimit	External ❗	🛑	onlyOwner
└	changeWalletLimit	External ❗	🛑	onlyOwner
└	changeIsFeeExempt	External ❗	🛑	onlyOwner
└	changeIsWltExempt	External ❗	🛑	onlyOwner
└	changeIsTxLimitExempt	External ❗	🛑	onlyOwner
└	setCampaignWallet	External ❗	🛑	onlyOwner
└	setLpWallet	External ❗	🛑	onlyOwner
└	setOwnerWallet	External ❗	🛑	onlyOwner
└	changeSwapBackSettings	External ❗	🛑	onlyOwner
└	setDistributionCriteria	External ❗	🛑	onlyOwner
└	delBot	External ❗	🛑	onlyOwner
└	_setIsDividendExempt	Internal 🔒	🛑	
└	setIsDividendExempt	External ❗	🛑	onlyOwner
└	getCirculatingSupply	Public ❗		NO❗
└	totalSupply	External ❗		NO❗
└	decimals	External ❗		NO❗
└	symbol	External ❗		NO❗
└	name	External ❗		NO❗
└	getOwner	External ❗		NO❗
└	balanceOf	Public ❗		NO❗
└	allowance	External ❗		NO❗
└	approve	Public ❗	🛑	NO❗
└	approveMax	External ❗	🛑	NO❗

└	transfer	External ❗	🛑	NO❗
└	transferFrom	External ❗	🛑	NO❗
└	_transfer	Internal 🔒	🛑	
└	_basicTransfer	Internal 🔒	🛑	
└	takeFee	Internal 🔒	🛑	
└	swapTokensForEth	Private 🔐	🛑	
└	addLiquidity	Private 🔐	🛑	
└	swapBack	Internal 🔒	🛑	lockTheSwap
└	manualSwapBack	External ❗	🛑	onlyOwner
└	clearStuckEth	External ❗	🛑	onlyOwner
└	manualProcessGas	External ❗	🛑	onlyOwner
└	checkPendingReflections	External ❗		NO❗
└	milkbone	External ❗	🛑	NO❗

INHERITANCE GRAPH



MANUAL REVIEW

Identifier	Definition	Severity
CEN-01	Centralization privileges of Havoc V2	Major 🟠

Centralized privileges are listed below:

```
setBots()
changeReflection()
changeTotalFees()
changeFeeAllocation()
changeTxLimit()
changeWalletLimit()
setCampaignWallet()
setLpWallet()
setOwnerWallet()
changeSwapBackSettings()
manualProcessGas()
clearStuckEth()
openTrading()
```


RECOMMENDATION

Deployer and/or contract owner private keys are secured carefully. Please refer to PAGE-09 CENTRALIZED PRIVILEGES for a detailed understanding.

Identifier	Definition	Severity
CEN-02	Initial asset distribution	Medium 🟡

All of the initially minted assets are sent to the contract deployer when deploying the contract. This can be an issue as the deployer and/or contract owner can distribute tokens without consulting the community.

```
_balances[_owner] = _totalSupply;
emit Transfer(address(0), _owner, _totalSupply);
```


RECOMMENDATION

Deployer and/or contract owner private keys are secured carefully. Please refer to PAGE-09 CENTRALIZED PRIVILEGES for a detailed understanding. The community should be consulted during the initial asset distribution process.

Identifier	Definition	Severity
CEN-03	Privileged role performing blacklist	Major 🟠

Privileged role can call `blacklist()`

```
    function setBots(address[] memory bots_) external onlyOwner {
        for (uint i = 0; i < bots_.length; i++) {
            bots[bots_[i]] = true;
        }
```


RECOMMENDATION

Remove blacklist – as it can intentionally stop an address from accessing smart contract function modules.

Identifier	Definition	Severity
CEN-04	Privileged role receiving LP tokens	Medium 🟡

Smart contract function `addLiqudity()` sends liquidity to `lpwallet()`

```
    function addLiquidity(uint256 tokenAmount, uint256 ethAmount) private {
        router.addLiquidityETH{value: ethAmount}(
            address(this),
            tokenAmount,
            0,
            0,
            lpWallet,
            block.timestamp
        );
    }
```

Smart contract owner can change LP wallet.


```
    function setLpWallet(address newLpWallet) external onlyOwner {
        lpWallet = newLpWallet;
    }
```

RECOMMENDATION

Send LP tokens to dead address or unreachable address.

Identifier	Definition	Severity
CEN-07	Authorizations and access controls	

Smart contract sets privileged roles

```
function isOwner(address account) public view returns (bool) {
    return account == owner;
}

function transferOwnership(address payable adr) public onlyOwner {
    owner = adr;
    emit OwnershipTransferred(adr);

function setOwnerWallet(address payable newOwnerWallet) external onlyOwner {
    tokenOwner = newOwnerWallet;
```


RECOMMENDATION

Private keys of all privileged roles are secured carefully. Please refer to PAGE-09 CENTRALIZED PRIVILEGES for a detailed understanding.

Identifier	Definition	Severity
CEN-08	Privileged role initiates launch	Minor 🟢

Privileged role can call `launch()`

```
    function openTrading() external onlyOwner {
        launchedAt = block.number;
        tradingOpen = true;
    }
```


RECOMMENDATION

Automate public launch. Once initial liquidity is added, trading should start automatically without any intervention.

Identifier	Definition	Severity
LOG-01	Lack of arbitrary limits	Medium 🟡

Below mentioned functions are set without any arbitrary limits.

```
changeTxLimit()
changeWalletLimit()
changeSwapBackSettings()
changeFeeAllocation()
manualProcessGas()
```


RECOMMENDATION

These functions should be provided arbitrary limits, e.g., put a `require` check that allows minimum transaction to at least 0.001% of the total supply.

Identifier	Definition	Severity
LOG-02	Potential sandwich attack	Minor 🟢

Potential sandwich attack happens when an attacker observes a transaction swapping tokens or adding liquidity without setting restrictions on slippage or minimum output amount. The attacker can manipulate the exchange rate by front-running a transaction to purchase assets and make profits by back-running a transaction to sell assets. Below mentioned functions are called without setting restrictions on slippage or minimum output:

```
addLiquidity()
swapExactTokensForETHSupportingFeeOnTransferTokens()
swapTokensForEth()
```


RECOMMENDATION

These functions should be provided reasonable minimum output amounts, instead of zero. Read more: https://coinmarketcap.com/alexandria/article/what-are-sandwich-attacks-in-defi-and-how-can-you-avoid-them

Identifier	Definition	Severity
LOG-03	Re-entrancy	Medium 🟡

Below mentioned functions are used without re-entrancy guard, or without any `require` check.

`milkbone()`

```
    function milkbone() external {
        lifeOnTheStreet.cryHavoc(msg.sender);
```


RECOMMENDATION

Re-entrancy guard is used to prevent re-entrant calls. Learn about re-entrancy guard: https://consensys.github.io/smart-contract-best-practices/attacks/reentrancy/

Identifier	Definition	Severity
COD-02	Timestamp manipulation via `block.timestamp` Avoid using `block.number` as timestamp	Minor 🟢

Be aware that the timestamp of the block can be manipulated by a miner. When the contract uses the timestamp to seed a random number, the miner can actually post a timestamp within 15 seconds of the block being validated, effectively allowing the miner to precompute an option more favorable to their chances, this is a critical exploit for contracts calculating random numbers, e.g., lottery.

RECOMMENDATION

To maintain block integrity, follow 15 seconds rule, and scale time dependent events accordingly.

Identifier	Definition	Severity
COD-04	Missing or unclear error messages	

RECOMMENDATION

Provide information strings for `require` related errors.

Identifier	Definition	Severity
COD-05	Missing zero address validation	

RECOMMENDATION

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

Identifier	Definition	Severity
COD-06	Unknown externally owned account	Minor 🟢

An externally owned account (EOA) has no code, and one can send messages from an externally owned account by creating and signing a transaction.

```
Line 341
address public campaignWallet = payable(0xBaC6A3636eC33FE1b3d380965386f190Bc957Ce4);
Line 342
address private whoLetTheDogsOut = payable(0x7Efa686efd1d689E7C6EEe6043569D9f5f5C570F)
```


RECOMMENDATION

Private keys of externally owned accounts must be secured carefully.

Identifier	Definition	Severity
COD-10	Third Party Dependencies	Minor 🟢

Smart contract is interacting with third party protocols e.g., Pancakeswap. The scope of the audit treats third party entities as black boxes and assumes their functional correctness. However, in the real world, third parties can be compromised, and exploited. Moreover, upgrades in third parties can create severe impacts, e.g., increased transactional fees, deprecation of previous routers, etc.

RECOMMENDATION

Inspect third party dependencies regularly, and mitigate severe impacts whenever necessary.

Identifier	Definition	Severity
COM-01	Floating compiler status	

Compiler is set to `^0.8.13`.

RECOMMENDATION

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

Identifier	Definition	Severity
COM-04	Potential resource exhaustion errors	Minor 🟢

```
function setBots(address[] memory bots_) external onlyOwner {
    for (uint i = 0; i < bots_.length; i++) {
        bots[bots_[i]] = true;
    }
}
```


RECOMMENDATION

Set an upper limit for multi-address calls, e.g., 100 wallets can be airdropped in a single transaction.

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.

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/interfiaudits

interfinetwork

hello@interfi.network

https://interfi.network

SMART CONTRACT AUDITS | SOLIDITY DEVELOPMENT AND TESTING

RELENTLESSLY SECURING PUBLIC AND PRIVATE BLOCKCHAINS