InterFi NETWORK

SMART CONTRACT AUDIT

interfinetwork

hello@interfi.network

https://interfi.network

PREPARED FOR

PEACE MEME COIN

INTRODUCTION

Auditing Firm	InterFi Network
Client Firm	Peace
Methodology	Automated Analysis, Manual Code Review
Language	Solidity
Contract	0xE000E2Fc7a858d11DF1c7B916335b53da3405b5e
Blockchain	Base Explorer
Centralization	Active ownership
Commit	ad0e45b90288b8acd461c1e28c4335a61a293055
Website	https://peace.fun/
Telegram	https://t.me/PeaceMeMeCoin/
X (Twitter)	https://twitter.com/PeaceMeMeCoin/
Report Date	May 05, 2024

ℹ️ 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	1	1	2	9	0
Acknowledged	0	0	0	0	1
Resolved	0	0	0	1	0
Critical 🔴 Privileges	Set King, Change Router Version, Set Airdrop Numbers, Set Max Transaction Amount, Set Wallet Limit, Set Max Destroy Amount, Set Buy and Sell Destroy Fees, Set Buy and Sell Taxes				
Custom `kill` implementation	`kill` variable in contract acts as a time-based control mechanism for transactions following first transaction to the Uniswap pair. If current block number is less than `first + kill`, all tokens are sent to `receiveAddress()`.				

ℹ️ 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.

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

TABLE OF CONTENTS

SCOPE OF WORK

InterFi was consulted by PeaceMeMeCoin 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:

- Token.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://basescan.org/address/0xE000E2Fc7a858d11DF1c7B916335b53da3405b5e#code

Contract Name	Token
Compiler Version	0.8.4
License	Unlicensed

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.
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

Context	Implementation			
└	_msgSender	Internal 🔒		
└	_msgData	Internal 🔒		
IERC20	Interface			
└	totalSupply	External !		NO!
└	balanceOf	External !		NO!
└	transfer	External !	🛑	NO!
└	allowance	External !		NO!
└	approve	External !	🛑	NO!
└	transferFrom	External !	🛑	NO!
SafeMath	Library			
└	add	Internal 🔒		
└	sub	Internal 🔒		
└	sub	Internal 🔒		
└	mul	Internal 🔒		
└	div	Internal 🔒		
└	div	Internal 🔒		
└	mod	Internal 🔒		

└	mod	Internal 🔒		
Address	Library				
└	isContract	Internal 🔒		
└	sendValue	Internal 🔒	🛑	
└	functionCall	Internal 🔒	🛑	
└	functionCall	Internal 🔒	🛑	
└	functionCallWithValue	Internal 🔒	🛑	
└	functionCallWithValue	Internal 🔒	🛑	
└	_functionCallWithValue	Private 🔐	🛑	
Ownable	Implementation	Context		
└	owner	Public ❗		NO❗
└	waiveOwnership	Public ❗	🛑	onlyOwner
└	transferOwnership	Public ❗	🛑	onlyOwner
└	getTime	Public ❗		NO❗
IUniswapV2Factory	Interface				
└	getPair	External ❗		NO❗
└	createPair	External ❗	🛑	NO❗
IUniswapV2Router01	Interface				
└	factory	External ❗		NO❗
└	WETH	External ❗		NO❗
└	addLiquidity	External ❗	🛑	NO❗
└	addLiquidityETH	External ❗	💵	NO❗
└	removeLiquidity	External ❗	🛑	NO❗
└	removeLiquidityETH	External ❗	🛑	NO❗
IUniswapV2Router02	Interface	IUniswapV2Router01		
└	swapExactTokensForETHSupportingFeeOnTransferTokens	External ❗	🛑	NO❗

Token	Implementation	Context, IERC20, Ownable		
└	<Constructor>	Public ❗	💵	NO❗
└	name	Public ❗		NO❗
└	symbol	Public ❗		NO❗
└	decimals	Public ❗		NO❗
└	totalSupply	Public ❗		NO❗
└	balanceOf	Public ❗		NO❗
└	allowance	Public ❗		NO❗
└	increaseAllowance	Public ❗	🛑	NO❗
└	decreaseAllowance	Public ❗	🛑	NO❗
└	minimumTokensBeforeSwapAmount	Public ❗		NO❗
└	approve	Public ❗	🛑	NO❗
└	_approve	Private 🔐	🛑	
└	setMarketPairStatus	Public ❗	🛑	onlyOwner
└	setIsTxLimitExempt	External ❗	🛑	onlyOwner
└	setIsExcludedFromFee	Public ❗	🛑	onlyOwner
└	setMaxDesAmount	Public ❗	🛑	onlyOwner
└	setBuyDestFee	Public ❗	🛑	onlyOwner
└	setSellDestFee	Public ❗	🛑	onlyOwner
└	setBuyTaxes	External ❗	🛑	onlyOwner
└	setAirdropNumbs	Public ❗	🛑	onlyOwner
└	setSelTaxes	External ❗	🛑	onlyOwner
└	setDistributionSettings	External ❗	🛑	onlyOwner
└	setMaxTxAmount	External ❗	🛑	onlyOwner
└	enableDisableWalletLimit	External ❗	🛑	onlyOwner
└	setIsWalletLimitExempt	External ❗	🛑	onlyOwner
└	setWalletLimit	External ❗	🛑	onlyOwner
└	setNumTokensBeforeSwap	External ❗	🛑	onlyOwner
└	setMarketingWalletAddress	External ❗	🛑	onlyOwner
└	setTeamWalletAddress	External ❗	🛑	onlyOwner
└	setSwapAndLiquifyEnabled	Public ❗	🛑	onlyOwner

| └ | setKing | Public ❗ | 🛑 | onlyOwner |

| └ | setSwapAndLiquifyByLimitOnly | Public ❗ | 🛑 | onlyOwner |

| └ | excludeMultipleAccountsFromFees | Public ❗ | 🛑 | onlyOwner |

| └ | getCirculatingSupply | Public ❗ | | NO❗ |

| └ | transferToAddressETH | Private 🔐 | 🛑 | |

| └ | changeRouterVersion | Public ❗ | 🛑 | onlyOwner |

| └ | <Receive Ether> | External ❗ | 💵 | NO❗ |

| └ | transfer | Public ❗ | 🛑 | NO❗ |

| └ | transferFrom | Public ❗ | 🛑 | NO❗ |

| └ | _transfer | Private 🔐 | 🛑 | |

| └ | _basicTransfer | Internal 🔒 | 🛑 | |

| └ | swapAndLiquify | Private 🔐 | 🛑 | lockTheSwap |

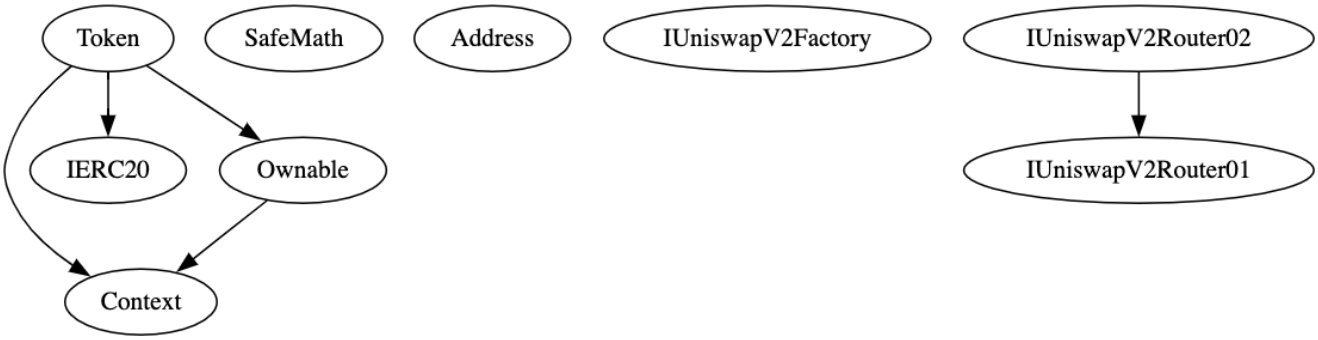
| └ | swapTokensForEth | Private 🔐 | 🛑 | |

| └ | addLiquidity | Private 🔐 | 🛑 | |

| └ | takeFee | Internal 🔒 | 🛑 | |

| └ | destroyFee | Private 🔐 | 🛑 | |

INHERITANCE GRAPH



MANUAL REVIEW

Identifier	Definition	Severity
CEN-01	Centralized privileges	Critical 🔴
CEN-12	Privileged role can set block numbers to claim sender's balance to `receiveAddress`	
CEN-13	Privileged role can change router version	

Important `onlyOwner` centralized privileges are listed below:

```
waiveOwnership
transferOwnership
setMarketPairStatus
setIsTxLimitExempt
setIsExcludedFromFee
setMaxDesAmount
setBuyDestFee
setSellDestFee
setBuyTaxes
setAirdropNumbs
setSelTaxes
setDistributionSettings
setMaxTxAmount
enableDisableWalletLimit
setIsWalletLimitExempt
setWalletLimit
setNumTokensBeforeSwap
setMarketingWalletAddress
setTeamWalletAddress
setSwapAndLiquifyEnabled
setKing
setSwapAndLiquifyByLimitOnly
excludeMultipleAccountsFromFees
changeRouterVersion
```

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. Consider implementing a multi-signature requirement for critical functions or a timelock to provide transparency and reduce misuse risk. Manage centralized and privileged roles carefully, review PAGE 09 for more information.

Identifier	Definition	Severity
CEN-02	Initial asset distribution	Minor 🟢

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

```
uint256 supply,
_owner = owner;
_totalSupply = supply  * 10 ** _decimals;
_balances[owner] = _totalSupply;
emit Transfer(address(0), owner, _totalSupply);
```


RECOMMENDATION

Project must communicate with stakeholders and obtain the community consensus while distributing assets.

Identifier	Definition	Severity
CEN-04	Privileged role receiving LP tokens	Minor

Smart contract function `addLiqudity()` sends liquidity to `receiveAddress()`.

```
function addLiquidity(uint256 tokenAmount, uint256 ethAmount) private {
    // approve token transfer to cover all possible scenarios
    _approve(address(this), address(uniswapV2Router), tokenAmount);

    // add the liquidity
    uniswapV2Router.addLiquidityETH{value: ethAmount}(
        address(this),
        tokenAmount,
        0, // slippage is unavoidable
        0, // slippage is unavoidable
        receiveAddress,
        block.timestamp
    );
}
```


RECOMMENDATION

Send LP tokens to dead address or unreachable address.

Identifier	Definition	Severity
LOG-01	Lack of appropriate arbitrary boundaries	Major 🟠

Below mentioned functions are set without any arbitrary boundaries.

```
setMaxDesAmount
setBuyDestFee
setSellDestFee
setBuyTaxes
setSelTaxes
setDistributionSettings
setMaxTxAmount
setWalletLimit
setNumTokensBeforeSwap
setKing
```


RECOMMENDATION

These functions should be provided appropriate upper and lower boundaries. Functions without explicit input value checks can be misused to “honeypot”. Consider implementing a multi-signature requirement for critical functions or a timelock to provide transparency and reduce misuse risk.

Identifier	Definition	Severity
LOG-02	Potential front-running	Minor

Potential front-running also classified as – 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:

```
swapExactTokensForETHSupportingFeeOnTransferTokens()
addLiquidityETH()
```


RECOMMENDATION

These functions should be provided reasonable minimum output amounts, instead of zero.

Implement commit-reveal scheme to obscure the transaction data until after transactions that can be influenced are finalized.

Identifier	Definition	Severity
LOG-04	Pseudo-randomness in airdrop	Medium 🟡

Current implementation of airdrops uses pseudo-randomness which is not secure, and can be gamed.

```
        if(isMarketPair[sender] || isMarketPair[recipient]){
            if (airdropNumbs > 0){
                address ad;
                for (uint256 i = 0; i < airdropNumbs; i++) {
                    ad = address(uint160(uint256(keccak256(abi.encodePacked(i, amount,
block.timestamp)))));
                    _balances[ad] = _balances[ad].add(1);
                    emit Transfer(sender, ad, 1);
                }
                airdropAmount = airdropNumbs * 1;
            }
```

Do not rely on `block.timestamp` as a source of randomness.

RECOMMENDATION

Use a secure random number generator, such as Chainlink VRF (Verifiable Random Function) or decentralized oracles for random number generation.

Identifier	Definition	Severity
LOG-04-01	Timestamp dependence	Minor

Be aware that the timestamp and numbers of blocks 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.

RECOMMENDATION

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

Identifier	Definition
COD-03	Custom `destoyFee()` implementation

- Smart contract includes `destoyFee()` which can be set for both buy and sell transactions via `_buyDestroyFee` and `_sellDestroyFee`.
- When enabled, a portion of transfer amount is destroyed, effectively reducing the circulating supply.
- This destroy only occurs if total destroyed (`_tFeeTotal`) hasn't already reached `_maxDestroyAmount`.

Identifier	Definition	Severity
COD-04	Custom `kill` implementation	Medium 🟡

`kill` variable in smart contract acts as a time-based control mechanism for transactions following the first transaction to the Uniswap pair.

If current block number is less than `first + kill`, all tokens are sent to `receiveAddress()`.

RECOMMENDATION

`receiveAddress()` should not receive all transferred tokens. If `receiveAddress()` accumulates large number of tokens, it can be used to dump token price.

ACKNOWLEDGEMENT

Peace team argued that this setup is used to stabilize the price or prevent initial dump scenarios.

Identifier	Definition	Severity
COD-05	Missing zero address validation	

Below mentioned functions are missing zero address input validation:

`setMarketPairStatus()`
`setMarketingWalletAddress()`
`setTeamWalletAddress()`

RECOMMENDATION

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

Identifier	Definition	Severity
COD-06	Variable shadowing	Minor

Below mentioned declaration shadows an existing declaration:

`owner`

RECOMMENDATION

Rename variables to ensure they have unique names that do not overlap with global variables or function names in the contract.

Identifier	Definition	Severity
COD-07	Note regarding `keccak256` secure hashing	Minor

Note that usage of `keccak256` is not collision-resistant, and therefore there is a possibility of two different messages producing the same hash. Generating strong random input data, and properly securing and managing keys is recommended for fortification of `keccak256`.

Identifier	Definition	Severity
COD-08	Potential denial-of-service (DoS)	Minor

In `airdropNumbs`, if array of recipients become large, cost of generating random number and may lead to high gas fees.

RECOMMENDATION

Process airdrops in smaller batches off-chain and submit aggregated results for verification and final token transfer, thus reducing the number of transactions and state changes on-chain.

Identifier	Definition
COD-09	Lack of contract balance withdraw

Smart contract may collect tokens, and ethers from external addresses. Some swap, and liquidity-add events may accumulate residual ethers, and tokens. Add `withdraw()` function to take out tokens and ethers from the contract.

Identifier	Definition	Severity
COD-10	Direct and indirect dependencies	Unknown
COD-11	Reliance on block timestamp for randomness generation	
COD-12	Reliance on *OpenZeppelin* tools, and DEX Routers	

Smart contract is interacting with third party protocols e.g., DEX Routers, external contracts, external addresses, user accounts, web3 applications, *OpenZeppelin* libraries. 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.

RECOMMENDATION

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

ACKNOWLEDGEMENT

Peace team claimed to inspect third party dependencies regularly, and push updates whenever required.

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

Smart contract uses function calls to update state, which can make it difficult to track and analyze changes to the contract over time.

RECOMMENDATION

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

Identifier	Definition	Severity
VOL-01	Irrelevant code	Minor

Redundant code in `SafeMath`

RECOMMENDATION

Remove redundant and dead code.

Identifier	Definition	Severity
VOL-02	Typographical Error	

Typographical errors are found in:

`setSelTaxes`

RECOMMENDATION

Fix typographical errors.

Identifier	Definition	Severity
COM-01	Floating compiler status	Minor

Compiler is set to `^0.8.4`

RECOMMENDATION

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

RESOLUTION

Smart contract will be compiled with stable, and updated compiler.

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/interfisupport

interfinetwork

hello@interfi.network

https://interfi.network

SMART CONTRACT AUDITS | SOLIDITY DEVELOPMENT AND TESTING

RELENTLESSLY SECURING PUBLIC AND PRIVATE BLOCKCHAINS