

# SMART CONTRACT SECURITY AUDIT OF **bitBYKE**



SMART CONTRACT AUDIT | TEAM KYC | PROJECT EVALUATION


# Summary

Auditing Firm	InterFi Network
Architecture	InterFi “Echelon” Auditing Standard
Smart Contract Audit Approved By	Chris   Blockchain Specialist at InterFi Network
Project Overview Approved By	Albert   Marketing Specialist at InterFi Network
Platform	Solidity
Mandatory Audit Check	Static, Software, Auto Intelligent & Manual Analysis
Report Date	May 21st, 2022

## 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:

- ❖ BitBYKE’s smart contract source code has **LOW RISK SEVERITY**.
- ❖ BitBYKE has **PASSED** the smart contract audit.
- ❖ Owner only instances to look for: **MAX TX LIMIT**

 **Smart contract audit passed with warning. For the detailed understanding of risk severity, source code vulnerability, and functional test, kindly refer to the audit.**

 **Verify the authenticity of this report on InterFi’s GitHub: <https://github.com/interfiaudit>**



# Table Of Contents

## Project Information

<b>Overview .....</b>	<b>4</b>
-----------------------	----------

## InterFi “Echelon” Audit Standard

<b>Audit Scope &amp; Methodology .....</b>	<b>6</b>
--------------------------------------------	----------

<b>InterFi’s Risk Classification .....</b>	<b>8</b>
--------------------------------------------	----------

## Smart Contract Risk Assessment

<b>Static Analysis .....</b>	<b>9</b>
------------------------------	----------

<b>Software Analysis .....</b>	<b>13</b>
--------------------------------	-----------

<b>Manual Analysis.....</b>	<b>15</b>
-----------------------------	-----------

<b>SWC Attacks .....</b>	<b>19</b>
--------------------------	-----------

<b>Risk Status &amp; Radar Chart .....</b>	<b>21</b>
--------------------------------------------	-----------

## Report Summary

<b>Auditor’s Verdict .....</b>	<b>22</b>
--------------------------------	-----------

## Legal Advisory

<b>Important Disclaimer .....</b>	<b>23</b>
-----------------------------------	-----------

<b>About InterFi Network.....</b>	<b>24</b>
-----------------------------------	-----------



# Project Overview

InterFi was consulted by BitBYKE to conduct the smart contract security audit of their solidity source code.

## About BitBYKE

DEXB BitBYKE has all the features of a centralized exchange, although it is decentralized.

Project	<b>BitBYKE - DEXB</b>
Blockchain	<b>Binance Smart Chain</b>
Language	<b>Solidity</b>
Contract	0x9F9bAf38B6Ae39f929c2DF5b3296f7ea55F39cCb
Website	<a href="https://bitbyke.app/">https://bitbyke.app/</a>
Telegram	<a href="https://t.me/bitbyke">https://t.me/bitbyke</a>
Youtube	<a href="https://www.youtube.com/channel/UCANWC9S_o388XSAmRUI3Ilg">https://www.youtube.com/channel/UCANWC9S_o388XSAmRUI3Ilg</a>
Medium	<a href="https://www.medium.com/@bitbyke">https://www.medium.com/@bitbyke</a>
Twitter	<a href="https://www.twitter.com/bitbyke">https://www.twitter.com/bitbyke</a>
Github	<a href="https://github.com/bitbyke/">https://github.com/bitbyke/</a>
Instagram	<a href="https://www.instagram.com/bitbyke">https://www.instagram.com/bitbyke</a>





## **Solidity Source Code On Blockchain** (Verified Contract Source Code)

<https://bscscan.com/token/0x9F9bAf38B6Ae39f929c2DF5b3296f7ea55F39cCb>

**Contract : BitBYKE**

**CompilerVersion:v0.6.12**

**Optimization Enabled: Yes with 200 runs**

## **Solidity Source Code On InterFi GitHub**

<https://github.com/interfiaduit>

## **SHA-1 Hash**

**Solidity source code is audited at hash #83ab4af5513156829136a505fd98566d85632f91**



# Audit Scope & Methodology

The scope of this report is to audit the smart contract source code of GalayNFT. 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
Source Code Review	❖ Requirement Violation
	❖ Ownership Takeover
	❖ Gas Limit and Loops
	❖ 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 smartcontract:**

**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-byline to identify potential vulnerabilities.**

**2. Static, Manual, and Software analysis:**

- ❖ **Test coverage analysis, which 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, which is analysing a program to determine what inputs causes 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**
- ❖ **Consensys Surya**
- ❖ **Open Zeppelin CodeAnalyzer**
- ❖ **Solidity Code Compiler**



# InterFi's 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 which requires to own 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.

Risk severity	Meaning
<b>! Critical</b>	This level vulnerabilities could be exploited easily, and can lead to asset loss, data loss, asset manipulation, or data manipulation. They should be fixed right away.
<b>! High</b>	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 critical risk severity
<b>! Medium</b>	This level vulnerabilities are should be fixed, as they carry an inherent risk of future exploits, and hacks which may or may not impact the smart contract execution.
<b>! Low</b>	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





# Smart Contract – Static Analysis

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






































```

| **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 |  |  |
|
|
|
|
|  | _msgSender | Internal |  |  |
|  | _msgData | Internal |  |  |
|
|
| **Address** | Library |   || |
|  | isContract | Internal |  |  |
|  | sendValue | Internal |  |  |
|  | functionCall | Internal |  |  |
|  | functionCall | Internal |  |  |
|  | functionCallWithValue | Internal |  |  |
|  | functionCallWithValue | Internal |  |  |
|  | _functionCallWithValue | Private |  |  |
|
|
|
|

```



```

| **Ownable** | Implementation | Context ||| |
| |<Constructor> | Internal |    | |
| | owner | Public ! | ! | |NO! |
| | renounceOwnership | Public ! |   | onlyOwner|
| | transferOwnership | Public ! |   | onlyOwner|
|||||
| **IUniswapV2Factory** | Interface | |||
| | feeTo | External ! | ! | |NO! |
| | feeToSetter | External ! | ! | |NO! |
| | getPair | External ! | ! | |NO! |
| | allPairs | External ! | ! | |NO! |
| | allPairsLength | External ! | ! | |NO! |
| | createPair | External ! |   |NO! |
| | setFeeTo | External ! |   |NO! |
| | setFeeToSetter | External ! |   |NO! |
|||||
| **IUniswapV2Pair** | Interface | |||
| | name | External ! | ! | |NO! |
| | symbol | External ! | ! | |NO! |
| | decimals | External ! | ! | |NO! |
| | totalSupply | External ! | ! | |NO! |
| | balanceOf | External ! | ! | |NO! |
| | allowance | External ! | ! | |NO! |
| | approve | External ! |   |NO! |
| | transfer | External ! |   |NO! |
| | transferFrom | External ! |   |NO! |
| | DOMAIN_SEPARATOR | External ! | ! | |NO! |
| | PERMIT_TYPEHASH | External ! | ! | |NO! |
| | nonces | External ! | ! | |NO! |
| | permit | External ! |   |NO! |
| | MINIMUM_LIQUIDITY | External ! | ! | |NO! |
| | factory | External ! | ! | |NO! |
| | token0 | External ! | ! | |NO! |
| | token1 | External ! | ! | |NO! |
| | getReserves | External ! | ! | |NO! |
| | price0CumulativeLast | External ! | ! | |NO! |
| | price1CumulativeLast | External ! | ! | |NO! |
| | kLast | External ! | ! | |NO! |
| | mint | External ! |   |NO! |
| | swap | External ! |   |NO! |
| | skim | External ! |   |NO! |
| | sync | External ! |   |NO! |
| | initialize | External ! |   |NO! |
|||||
| **IUniswapV2Router01** | Interface | |||
| | factory | External ! | ! | |NO! |
| | WETH | External ! | ! | |NO! |
| | addLiquidity | External ! |   |NO! |
| | addLiquidityETH | External ! | ! |   |NO! |
| | removeLiquidity | External ! |   |NO! |

```



```

| L | removeLiquidityETH | External ! |   | NO!! |
| L | removeLiquidityWithPermit | External ! |   | NO!! |
| L | removeLiquidityETHWithPermit | External ! |   | NO!! |
| L | swapExactTokensForTokens | External ! |   | NO!! |
| L | swapTokensForExactTokens | External ! |   | NO!! |
| L | swapExactETHForTokens | External ! |   | NO! |
| L | swapTokensForExactETH | External ! |   | NO!! |
| L | swapExactTokensForETH | External ! |   | NO!! |
| L | swapETHForExactTokens | External ! |   | NO! |
| L | quote | External ! |  | NO!! |
| L | getAmountOut | External ! |  | NO!! |
| L | getAmountIn | External ! |  | NO!! |
| L | getAmountsOut | External ! |  | NO!! |
| L | getAmountsIn | External ! |  | NO!! |
|||||
| **IUniswapV2Router02** | Interface | IUniswapV2Router01 |||
| L | removeLiquidityETHSupportingFeeOnTransferTokens | External ! |   | NO!! |
| L | removeLiquidityETHWithPermitSupportingFeeOnTransferTokens | External ! |   | NO!! |
| L | swapExactTokensForTokensSupportingFeeOnTransferTokens | External ! |   | NO!! |
| L | swapExactETHForTokensSupportingFeeOnTransferTokens | External ! |   | NO! |
| L | swapExactTokensForETHSupportingFeeOnTransferTokens | External ! |   | NO!! |
|||||
| **** | Implementation | Context, IERC20, Ownable |||
| L | <Constructor> | Public ! |   | NO!! |
| L | name | Public ! |  | NO!! |
| L | symbol | Public ! |  | NO!! |
| L | decimals | Public ! |  | NO!! |
| L | totalSupply | Public ! |  | NO!! |
| L | balanceOf | Public ! |  | NO!! |
| L | transfer | Public ! |   | NO!! |
| L | allowance | Public ! |  | NO!! |
| L | approve | Public ! |   | NO!! |
| L | transferFrom | Public ! |   | NO!! |
| L | increaseAllowance | Public ! |   | NO!! |
| L | decreaseAllowance | Public ! |   | NO!! |
| L | isExcludedFromReward | Public ! |  | NO!! |
| L | totalFees | Public ! |  | NO!! |
| L | deliver | Public ! |   | NO!! |
| L | reflectionFromToken | Public ! |  | NO!! |
| L | tokenFromReflection | Public ! |  | NO!! |
| L | excludeFromReward | Public ! |   | onlyOwner |
| L | includeInReward | External ! |   | onlyOwner |
| L | <Receive Ether> | External ! |   | NO! |
| L | _distributeFee | Private    ||
| L | _getValues | Private   ||
| L | _getTValues | Private   ||
| L | _getRValues | Private   ||
| L | _getRate | Private   ||
| L | _getCurrentSupply | Private   ||
| L | _takeLiquidityAndMarketing | Private    ||

```



```

|  | calculateTaxFee | Private |  |  |  |
|  | calculateMarketingFee | Private |  |  |  |
|  | calculateLiquidityFee | Private |  |  |  |
|  | removeAllFee | Private |  |  |  |
|  | restoreAllFee | Private |  |  |  |
|  | isExcludedFromFee | Public | ! |  | NO ! |
|  | _approve | Private |  |  |  |
|  | _transfer | Private |  |  |  |
|  | swapAndLiquify | Private |  |  | lockTheSwap |
|  | swapTokensForEth | Private |  |  |  |
|  | addLiquidity | Private |  |  |  |
|  | _tokenTransfer | Private |  |  |  |
|  | _transferStandard | Private |  |  |  |
|  | _transferToExcluded | Private |  |  |  |
|  | _transferFromExcluded | Private |  |  |  |
|  | _transferBothExcluded | Private |  |  |  |
|  | transferToMarketing | Private |  |  |  |
|  | excludeFromFee | Public | ! |  | onlyOwner |
|  | includeInFee | Public | ! |  | onlyOwner |
|  | enableAllFees | External | ! |  | onlyOwner |
|  | disableAllFees | External | ! |  | onlyOwner |
|  | setMarketingWallet | External | ! |  | onlyOwner |
|  | setNumTokensToAddLiquidity | External | ! |  | onlyOwner |
|  | setMaxTxPercent | External | ! |  | onlyOwner |
|  | setSwapAndLiquifyEnabled | Public | ! |  | onlyOwner

```

## Smart Contract Security Audit



# Smart Contract – Software Analysis

## Function Signatures

```

11902160 => _getTValues(uint256)
16279055 => isContract(address)
39509351 => increaseAllowance(address,uint256)
75128141 => calculateTaxFee(uint256)
92104301 => _transferFromExcluded(address,address,uint256,ValuesStruct)
18160ddd => totalSupply()
70a08231 => balanceOf(address) a9059cbb
          => transfer(address,uint256)
dd62ed3e => allowance(address,address)
095ea7b3 => approve(address,uint256)
23b872dd => transferFrom(address,address,uint256)
771602f7 => add(uint256,uint256)
b67d77c5 => sub(uint256,uint256) e31bdc0a
          => sub(uint256,uint256,string)
c8a4ac9c => mul(uint256,uint256) a391c15b
          => div(uint256,uint256) b745d336
          => div(uint256,uint256,string)
f43f523a => mod(uint256,uint256) 71af23e8
          => mod(uint256,uint256,string)
119df25f => _msgSender()
8b49d47e => _msgData()
24a084df => sendValue(address,uint256) a0b5ffb0
          => functionCall(address,bytes) 241b5886
          => functionCall(address,bytes,string)
2a011594 => functionCallWithValue(address,bytes,uint256) d525ab8a
          => functionCallWithValue(address,bytes,uint256,string)
36455e42 => _functionCallWithValue(address,bytes,uint256,string)
8da5cb5b => owner()
715018a6 => renounceOwnership() f2fde38b
          => transferOwnership(address)
017e7e58 => feeTo()
094b7415 => feeToSetter()
e6a43905 => getPair(address,address)
1e3dd18b => allPairs(uint256) 574f2ba3
          => allPairsLength()
c9c65396 => createPair(address,address)
f46901ed => setFeeTo(address)
a2e74af6 => setFeeToSetter(address)
06fdde03 => name()
95d89b41 => symbol()
313ce567 => decimals()
3644e515 => DOMAIN_SEPARATOR()
30adf81f => PERMIT_TYPEHASH()
7ecele00 => nonces(address)

```



d505accf => permit(address,address,uint256,uint256,uint8,bytes32,bytes32)



```

ba9a7a56 => MINIMUM_LIQUIDITY()
c45a0155 => factory()
0dfe1681 => token0()
d21220a7 => token1()
0902f1ac => getReserves()
5909c0d5 => price0CumulativeLast()
5a3d5493 => price1CumulativeLast()
7464fc3d => kLast()
6a627842 => mint(address)
022c0d9f => swap(uint256,uint256,address,bytes)
bc25cf77 => skim(address)
fff6cae9 => sync()
485cc955 => initialize(address,address)
ad5c4648 => WETH()

```

### Inheritance Graph



Smart Contract  
Security Audit



# Smart Contract – 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
Buy Back	is an action in which the project buys back its tokens from the existing holders usually at a market price	NA	NA
Burn	executes transfers of a specified number of tokens to a burn address	NA	NA
Mint	executes creation of a specified number of tokens and adds it to the total supply	NA	NA
Rebase	circulating token supply adjusts (increases or decreases) automatically according to a token's price fluctuations	NA	NA
Blacklist	stops specified wallets from interacting with the smart contract function modules	NA	NA
Lock	stops or locks all function modules of the smart contract	NA	NA





Function	Description	Tested	Verdict
Dividend	<b>executes transfers of a specified dividend token to a specified address</b>	NA	NA
Airdrop	<b>executes transfers of a specified number of tokens to a specified address</b>	NA	NA
Max Transaction	<b>a non-whitelisted wallet can only transfer a specified number of tokens</b>	Yes	! Low
Max Wallet	<b>a non-whitelisted wallet can only hold a specified number of tokens</b>	NA	NA
Anti Bot	<b>stops some or all bot wallets from interacting with the smart contract</b>	NA	NA
Transfer Ownership	<b>executes transfer of contract ownership to a specified wallet</b>	Yes	Passed
Renounce Ownership	<b>executes transfer of contract ownership to a dead address</b>	Yes	Passed



## Best Practices

- ❖ **Owner cannot stop or pause the smart contract.**
- ❖ **Owner cannot lock or burn the user assets.**
- ❖ **Owner cannot mint tokens after initial contract creation/deployment.**
- ❖ **The smart contract utilizes “SafeMath” function to avoid common smart contract vulnerabilities.**

```
string private _name = "EloInu";

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");
```

## Warning

- ❖ **Active smart contract owner: 0x26b41f2c425200d2f83089969ecdcd9fe145a841**
- ❖ *Be aware that active smart contract owner privileges constitute an elevated impact to smart contract's safety and security.*
- ❖ **Smart contract owner can enable or disable the buy and sell fees.**
- ❖ **Smart contract owner can change max transaction %. There's no threshold on max tx, the smart contract owner can change the value to “zero”.**



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

```
{
  "resource": " /DEXB.sol",
  "owner": "_generated_diagnostic_collection_name_#0",
  "severity": 8, (! Low Severity)
  " Expected pragma, import directive or contract/interface/library definition",
  "source": "solc",
}
```

# InterFi

Smart Contract  
Security Audit



# Smart Contract – SWC Attacks

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

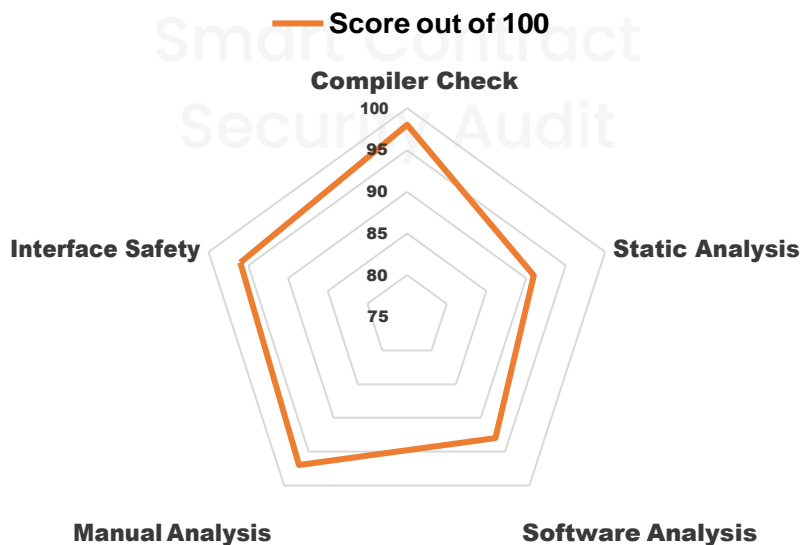


SWC-119	<b>Shadowing State Variables</b>	Passed
SWC-120	<b>Weak Sources of Randomness from Chain Attributes</b>	Passed
SWC-121	<b>Missing Protection against Signature Replay Attacks</b>	Passed
SWC-122	<b>Lack of Proper Signature Verification</b>	Passed
SWC-123	<b>Requirement Violation</b>	Passed
SWC-124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



# Smart Contract - Risk Status & Radar Chart

Risk Severity	Status
<b>! Critical</b>	<b>None critical severity issues identified</b>
<b>! High</b>	<b>None high severity issues identified</b>
<b>! Medium</b>	<b>None medium severity issues identified</b>
<b>! Low</b>	<b>1 low severity issue identified</b>
<b>Verified</b>	<b>54 functions and instances verified and checked</b>
<b>Safety Score</b>	<b>96 out of 100</b>



## 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.**

**BitBYKE's smart contract source code has **LOW RISK SEVERITY**.**

**BitBYKE has **PASSED** the smart contract audit.**

InterFi

### Note for stakeholders

- ❖ **Be aware that active smart contract owner privileges constitute an elevated impact on smart contract's safety and security.**
- ❖ **Make sure that the project team's KYC/identity is verified by an independent firm, e.g., InterFi.**
- ❖ **Always check if the contract's liquidity is locked. A longer liquidity lock plays an important role in 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 of time.**
- ❖ **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 of time.**



## Important Disclaimer

**InterFi Network provides contract auditing and project verification services for blockchain projects. The purpose of the audit is to analyse the on-chain smart contract source code, and to provide basic overview of the project.** This report should not be transmitted, disclosed, referred to, or relied upon by any person for any purposes 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 an 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 from external vulnerability, or a hack. Be aware that active smart contract owner privileges constitute an elevated impact to smart contract's 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 on 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 own 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/interfiAudit> .....

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





{{gINTERFINETWORK

RELENTLESSLY SECURING THE PUBLIC BLOCKCHAIN | MADE IN CANADA 🇨🇦