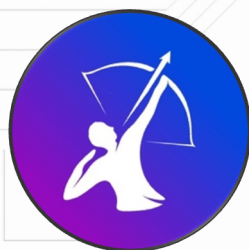




# SMART CONTRACT SECURITY AUDIT OF TIGRIS TRADE



SMART CONTRACT AUDIT | SOLIDITY DEVELOPMENT & TESTING | PROJECT EVALUATION

RELENTLESSLY SECURING THE PUBLIC BLOCKCHAIN

# Audit Introduction

<b>Auditing Firm</b>	InterFi Network
<b>Audit Architecture</b>	InterFi Echelon Auditing Standard
<b>Language</b>	Solidity
<b>Client Firm</b>	Tigris Trade
<b>Website</b>	<a href="https://www.tigris.trade/">https://www.tigris.trade/</a>
<b>Twitter</b>	<a href="https://twitter.com/tigristrades/">https://twitter.com/tigristrades/</a>
<b>Discord</b>	<a href="https://discord.com/invite/HkUVgx5rWg/">https://discord.com/invite/HkUVgx5rWg/</a>
<b>Report Date</b>	August 30, 2022

## About Tigris Trade

Tigris Trade is a Truly Decentralized Leveraged Trading platform.

Tigris pioneers the use of NFT-based open positions, resulting in a smarter and more reliable trading experience that is accessible to all. We believe top-notch user experience and advanced trading features can be and should be made trustless and autonomous.

Our custom price oracle solution offers near-instant trade execution on guaranteed spot prices, and community-powered liquidity allows for the lowest fees in the ecosystem.

Every open position is minted as a tradable NFT that we call Open Trade NFTs. Ultimately, we intend to create a new type of collateral debt market based on these NFTs.



# Audit Summary

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

- ❖ Tigris Trade's solidity source codes have **LOW RISK SEVERITY**
- ❖ Tigris Trade's smart contracts have **ACTIVE OWNERSHIP**
- ❖ Centralization risk correlated to the active owner is **HIGH**
- ❖ Important owner privileges – **SET FEES, SET PAUSED, SET MAX GAS PRICE, SET BLOCK DELAY, SET LIQUIDITY PERCENT, SET MINTER, SET PROTOCOL, SET ALLOWED ASSET, MINT, MINT MANY**
- ❖ Important minter privileges – **MINT, MINT FOR, BURN, BURN FROM, EXECUTE LIMIT ORDER**

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, exploitability, and audit disclaimer, kindly refer to the audit.

✅ 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
Centralization Risk.....	9

## **Smart Contract Risk Assessment**

Static Analysis.....	10
Function Signatures .....	14
Manual Analysis.....	17
SWC Attacks .....	21
Risk Status & Radar Chart.....	23

## **Audit Summary**

Auditor's Verdict .....	24
-------------------------	----

## **Legal Advisory**

Important Disclaimer .....	25
About InterFi Network.....	26



# Audit Scope

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

- ❖ NativeStableVault.sol
- ❖ GovNFT.sol
- ❖ PairsContract.sol
- ❖ Position.sol
- ❖ StableToken.sol
- ❖ StableVault.sol
- ❖ Trading.sol
- ❖ MetaContext.sol
- ❖ TradingLibrary.sol

InterFi

## Solidity Source Code On GitHub

//Private Repository

Smart Contract  
Security Audit

## SHA-1 Hash

Solidity source code is audited at hash #8be4aadbdc3987e79928c22307db2f648a435f6



# Audit Methodology

The scope of this report is to audit the smart contract source code of Tigris Trade. InterFi has scanned contracts and reviewed codes for common vulnerabilities, exploits, hacks, and backdoors. Due to being out of scope, InterFi has not tested contracts on testnet to assess any functional flaws. 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
- ❖ Gas Limit and Loops

### Source Code Review

- ❖ Deployment Consistency
- ❖ Repository Consistency
- ❖ Data Consistency
- ❖ Token Supply Manipulation
- ❖ Access Control and Authorization
- ❖ Operations Trail and Event Generation
- ❖ Assets Manipulation
- ❖ Ownership Control
- ❖ Liquidity Access



## **InterFi's Echelon Audit Standard**

The aim of InterFi's "Echelon" standard is to analyze smart contracts and identify the vulnerabilities and the hacks. Kindly note, InterFi does not test smart contracts on testnet. It is recommended that smart contracts are thoroughly tested prior to the audit submission. Mentioned are the steps used by InterFi to audit smart contracts:

1. Solidity smart contract source code reviewal:
  - ❖ Review of the specifications, sources, and instructions provided to InterFi to make sure we understand the size, and scope of the smart contract audit.
  - ❖ 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**

- ❖ Consensys Tools
- ❖ 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
<b>! High</b>	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.
<b>! Medium</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 high-risk severity
<b>! Low</b>	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.
<b>! Informational</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





# Centralization Risk

Centralization risk is the most common cause of decentralized finance hacks. When a smart contract has an active contract ownership, the risk related to centralization is elevated. There are some well-intended reasons to be an active contract owner, such as:

- ❖ Contract owner can be granted the power to `pause()` or `lock()` the contract in case of an external attack.
- ❖ Contract owner 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 a full centralized power to a single body can be dangerous. Unfortunately, centralization related risks are higher than common smart contract vulnerabilities. Centralization of ownership creates a risk of rug pull scams, where owners cash out tokens in such quantities that they become valueless. **Most important question to ask here is, how to mitigate centralization risk?** Here's InterFi's recommendation to lower the risks related to centralization hacks:

- ❖ Smart contract owner's private key must be carefully secured to avoid any potential hack.
- ❖ Smart contract ownership should be shared by multi-signature (multi-sig) wallets.
- ❖ Smart contract ownership can be locked in a contract, user voting, or community DAO can be introduced to unlock the ownership.

## Centralization Status


- ❖ Tigris Trade's smart contracts have **active ownership**.



# Static Analysis

Symbol	Meaning
	Function can modify state
	Function is payable
	Function is locked
	Function can be accessed
!	Important functionality

```

| **IWNative** | Interface | |||
| L | deposit | External ! |  |NO ! |
| L | withdraw | External ! |  |NO ! |
|||||
| **NativeStableVault** | Implementation | StableVault, INativeStableVault |||
| L | <Constructor> | Public ! |  | StableVault |
| L | depositNative | Public ! |  |NO ! |
| L | withdrawNative | External ! |  |NO ! |
| L | <Receive Ether> | External ! |  |NO ! |
|||||
| **GovNFT** | Implementation | ERC721, ILayerZeroReceiver, MetaContext, IGovNFT |||
| L | <Constructor> | Public ! |  | ERC721 |
| L | _baseURI | Internal  | | |
| L | setBaseURI | External ! |  | onlyOwner |
| L | _mint | Internal  |  | |
| L | _bridgeMint | Internal  |  | |
| L | _burn | Internal  |  | |
| L | _transfer | Internal  |  | |
| L | mintMany | External ! |  | onlyOwner |
| L | mint | External ! |  | onlyOwner |
| L | crossChain | Public ! |  |NO ! |
| L | lzReceive | External ! |  |NO ! |
| L | estimateFees | External ! | |NO ! |
| L | setGas | External ! |  | onlyOwner |
| L | setEndpoint | External ! |  | onlyOwner |
| L | safeTransferMany | External ! |  |NO ! |
| L | safeTransferFromMany | External ! |  |NO ! |
| L | approveMany | External ! |  |NO ! |
| L | claim | External ! |  |NO ! |
| L | distribute | External ! |  |NO ! |
| L | pending | Public ! | |NO ! |

```



```

| L | addAsset | External ! | ● | onlyOwner |
| L | setAllowedAsset | External ! | ● | onlyOwner |
| L | assetsLength | Public ! | | NO ! |
| L | allowedAsset | External ! | | NO ! |
| L | _msgSender | Internal 🔒 | | |
| L | _msgData | Internal 🔒 | | |
|||||
| **PairsContract** | Implementation | Ownable, IPairsContract |||
| L | createReferralCode | External ! | ● | NO ! |
| L | setReferred | External ! | ● | onlyProtocol |
| L | getReferred | External ! | | NO ! |
| L | getReferral | External ! | | NO ! |
| L | idToAsset | Public ! | | NO ! |
| L | idToOi | Public ! | | NO ! |
| L | setAssetChainlinkFeed | External ! | ● | onlyOwner |
| L | addAsset | External ! | ● | onlyOwner |
| L | updateAssetLeverage | External ! | ● | onlyOwner |
| L | setAssetBaseFundingRate | External ! | ● | onlyOwner |
| L | updateAssetFeeMultiplier | External ! | ● | onlyOwner |
| L | pauseAsset | External ! | ● | onlyOwner |
| L | setMaxBaseFundingRate | External ! | ● | onlyOwner |
| L | setProtocol | External ! | ● | onlyOwner |
| L | modifyLongOi | External ! | ● | onlyProtocol |
| L | modifyShortOi | External ! | ● | onlyProtocol |
|||||
| **Position** | Implementation | ERC721Enumerable, MetaContext, IPosition |||
| L | ownerOf | Public ! | | NO ! |
| L | isMinter | Public ! | | NO ! |
| L | trades | Public ! | | NO ! |
| L | openPositions | Public ! | | NO ! |
| L | openPositionsIndexes | Public ! | | NO ! |
| L | assetOpenPositions | Public ! | | NO ! |
| L | assetOpenPositionsIndexes | Public ! | | NO ! |
| L | limitOrders | Public ! | | NO ! |
| L | limitOrderIndexes | Public ! | | NO ! |
| L | <Constructor> | Public ! | ● | ERC721 |
| L | _baseURI | Internal 🔒 | | |
| L | setBaseURI | External ! | ● | onlyOwner |
| L | updateFunding | External ! | ● | onlyMinter |
| L | mint | External ! | ● | onlyMinter |
| L | executeLimitOrder | External ! | ● | onlyMinter |
| L | modifyMargin | External ! | ● | onlyMinter |
| L | reducePosition | External ! | ● | onlyMinter |
| L | modifyTp | External ! | ● | onlyMinter |
| L | modifySl | External ! | ● | onlyMinter |
| L | burn | External ! | ● | onlyMinter |
| L | assetOpenPositionsLength | External ! | | NO ! |
| L | limitOrdersLength | External ! | | NO ! |
| L | getCount | External ! | | NO ! |
| L | userTrades | External ! | | NO ! |

```



```

| L | openPositionsSelection | External ! | NO ! | |
| L | setMinter | External ! | onlyOwner |
| L | _msgSender | Internal | | |
| L | _msgData | Internal | | |
|||||
| **StableToken** | Implementation | ERC20Permit, MetaContext |||
| L | <Constructor> | Public ! | ERC20Permit ERC20 |
| L | burnFrom | Public ! | onlyMinter |
| L | mintFor | Public ! | onlyMinter |
| L | setMinter | Public ! | onlyOwner |
| L | _msgSender | Internal | | |
| L | _msgData | Internal | | |
|||||
| **IERC20Mintable** | Interface | IERC20 |||
| L | mintFor | External ! | NO ! |
| L | burnFrom | External ! | NO ! |
| L | decimals | External ! | NO ! |
|||||
| **ERC20Permit** | Interface | IERC20 |||
| L | permit | External ! | NO ! |
|||||
| **StableVault** | Implementation | MetaContext, IStableVault |||
| L | <Constructor> | Public ! | NO ! |
| L | deposit | Public ! | NO ! |
| L | depositWithPermit | External ! | NO ! |
| L | withdraw | External ! | NO ! |
| L | listToken | External ! | onlyOwner |
| L | delistToken | External ! | onlyOwner |
|||||
| **IStable** | Interface | IERC20 |||
| L | burnFrom | External ! | NO ! |
| L | mintFor | External ! | NO ! |
|||||
| **ExtendedIERC20** | Interface | IERC20 |||
| L | decimals | External ! | NO ! |
|||||
| **ERC20Permit** | Interface | IERC20 |||
| L | permit | External ! | NO ! |
|||||
| **Trading** | Implementation | MetaContext, ITrading |||
| L | <Constructor> | Public ! | NO ! |
| L | initiateMarketOrder | External ! | NO ! |
| L | initiateCloseOrder | External ! | NO ! |
| L | initiateLimitOrder | External ! | NO ! |
| L | cancelLimitOrder | External ! | NO ! |
| L | addMargin | External ! | NO ! |
| L | updateTpSl | External ! | NO ! |
| L | executeLimitOrder | External ! | NO ! |
| L | liquidatePosition | External ! | NO ! |
| L | limitClose | External ! | NO ! |

```



```

| L | _closePosition | Internal | 🔒 | 🔴 | |
| L | _handleOpenFees | Internal | 🔒 | 🔴 | |
| L | _handleCloseFees | Internal | 🔒 | 🔴 | |
| L | _handleDeposit | Internal | 🔒 | 🔴 | |
| L | updateFunding | Internal | 🔒 | 🔴 | |
| L | _setReferral | Internal | 🔒 | 🔴 | |
| L | validateTrade | Internal | 🔒 | | |
| L | _checkSl | Internal | 🔒 | | |
| L | _checkOwner | Internal | 🔒 | | |
| L | _checkGas | Internal | 🔒 | | |
| L | _checkDelay | Internal | 🔒 | 🔴 | |
| L | setBlockDelay | External | ! | 🔴 | onlyOwner |
| L | setLiqPercent | External | ! | 🔴 | onlyOwner |
| L | setMaxWinPercent | External | ! | 🔴 | onlyOwner |
| L | setValidSignatureTimer | External | ! | 🔴 | onlyOwner |
| L | setMinNodeCount | External | ! | 🔴 | onlyOwner |
| L | setAllowedMargin | External | ! | 🔴 | onlyOwner |
| L | setMinPositionSize | External | ! | 🔴 | onlyOwner |
| L | setPaused | External | ! | 🔴 | onlyOwner |
| L | setMaxGasPrice | External | ! | 🔴 | onlyOwner |
| L | setFees | External | ! | 🔴 | onlyOwner |
| L | setNode | External | ! | 🔴 | onlyOwner |
| L | setChainlinkEnabled | External | ! | 🔴 | onlyOwner |
| L | getLiqPrice | External | ! | | NO ! |
| L | <Receive Ether> | External | ! | 📡 | NO ! |
|||||
| **MetaContext** | Implementation | Ownable |||
| L | setTrustedForwarder | External | ! | 🔴 | onlyOwner |
| L | isTrustedForwarder | External | ! | | NO ! |
| L | _msgSender | Internal | 🔒 | | |
| L | _msgData | Internal | 🔒 | | |
|||||
| **IPrice** | Interface | |||
| L | latestAnswer | External | ! | | NO ! |
| L | decimals | External | ! | | NO ! |
|||||
| **TradingLibrary** | Library | |||
| L | pnl | External | ! | | NO ! |
| L | liqPrice | External | ! | | NO ! |
| L | verifyAndCreatePrice | External | ! | 🔴 | NO ! |
| L | median | Private | 🔒 | | |
| L | swap | Private | 🔒 | | |
| L | sort | Private | 🔒 | | |

```



# Function Signatures

```

059513a6 => mintMany(uint256)
1249c58b => mint()
5deccd72 => crossChain(uint16,bytes,address,uint256[])
001d3567 => lzReceive(uint16,bytes,uint64,bytes)
40a7bb10 => estimateFees(uint16,address,bytes,bool,bytes)
dd51faa2 => setGas(uint256)
aaaaeb8e => setEndpoint(ILayerZeroEndpoint256)
d6651c70 => safeTransferMany(address,uint256[])
3206e3e7 => safeTransferFromMany(address,address,uint256[])
99bb8134 => approveMany(address,uint256[])
1e83409a => claim(address)
fb932108 => distribute(address,uint256)
19bc9ae8 => pending(address,address)
298410e5 => addAsset(address)
d9a3aa3c => setAllowedAsset(address,bool)
f50477a2 => assetsLength()
f35da34c => allowedAsset(address)
119df25f => _msgSender()
8b49d47e => _msgData()
e20c8548 => setReferred(address,bytes32)
d113f04c => getReferred(address)
82e58d51 => getReferral(bytes32)
c688fca7 => idToAsset(uint256)
e8ea9945 => idToOi(uint256,address)
4dde1793 => setAssetChainlinkFeed(uint256,address)
533d5c44 => addAsset(uint256,string,address,uint256,uint256,uint256)
74e0246b => updateAssetLeverage(uint256,uint256,uint256)
0ef567e2 => setAssetBaseFundingRate(uint256,uint256)
0fdef288 => updateAssetFeeMultiplier(uint256,uint256)
200defdd => pauseAsset(uint256,bool)
6b3c17bb => setMaxBaseFundingRate(uint256)
0a9d793d => setProtocol(address)
87a64cfa => modifyLongOi(uint256,address,bool,uint256)
620b9584 => modifyShortOi(uint256,address,bool,uint256)
6352211e => ownerOf(uint256)
aa271e1a => isMinter(address)
1e6c598e => trades(uint256)
cc35b490 => openPositions()
a933574a => openPositionsIndexes(uint256)
2a119020 => assetOpenPositions(uint256)
1df3d4a3 => assetOpenPositionsIndexes(uint256,uint256)
a3e2b495 => limitOrders(uint256)
c42e74ae => limitOrderIndexes(uint256,uint256)
55ea731c => updateFunding(uint256,address,uint256,uint256,uint256)
13fc2321 => mint(MintTrade)
d19a8a4a => executeLimitOrder(uint256,uint256,uint256)
4a6907e9 => modifyMargin(uint256,uint256,uint256)

```



```

75a0b6dd => reducePosition(uint256,uint256)
5fdb05f3 => modifyTp(uint256,uint256)
db3ab0ba => modifySl(uint256,uint256)
42966c68 => burn(uint256)
9add4e5f => assetOpenPositionsLength(uint256)
44d61f38 => limitOrdersLength(uint256)
a87d942c => getCount()
6a6ae606 => userTrades(address)
a550a8be => openPositionsSelection(uint256,uint256)
cf456ae7 => setMinter(address,bool)
79cc6790 => burnFrom(address,uint256)
da1919b3 => mintFor(address,uint256)
313ce567 => decimals()
d505accf => permit(address,address,uint256,uint256,uint8,bytes32,bytes32)
47e7ef24 => deposit(address,uint256)
35fd95c4 => depositWithPermit(address,uint256,uint256,bool,uint8,bytes32,bytes32)
f3fef3a3 => withdraw(address,uint256)
1fc1e25f => listToken(address)
abffc9ac => delistToken(address)
4e9ef649 => initiateMarketOrder(TradeInfo,PriceData[],bytes[],ERC20PermitData)
f12126ea => initiateCloseOrder(uint256,uint256,PriceData[],bytes[],address,address)
4ff153ea => initiateLimitOrder(TradeInfo,uint256,uint256,PriceData[],bytes[],ERC20PermitData)
a5cdc8fc => cancelLimitOrder(uint256)
f7993856 => addMargin(uint256,uint256,address,address,ERC20PermitData)
c5a22c2a => updateTpSl(bool,uint256,uint256,PriceData[],bytes[])
efa73a89 => executeLimitOrder(uint256,PriceData[],bytes[])
8d363c6e => liquidatePosition(uint256,PriceData[],bytes[])
7b217a0f => limitClose(uint256,bool,PriceData[],bytes[])
5c491e0e => _closePosition(uint256,uint256,uint256,address,address)
13a57b57 => _handleOpenFees(uint256,uint256,address,uint256,address)
2ec24287 => _handleDeposit(address,address,uint256,address,ERC20PermitData)
f8fef4ea => updateFunding(uint256,address)
a7d227f6 => _setReferral(bytes32)
78157a90 => validateTrade(uint256,address,uint256,uint256)
6ebb6574 => _checkOwner(uint256)
66b481e8 => _checkGas()
71b75be0 => _checkDelay(uint256)
fa67ae5a => setBlockDelay(uint256)
182008a4 => setLiqPercent(uint256)
895164e8 => setMaxWinPercent(uint256)
797b371e => setValidSignatureTimer(uint256)
e6793a54 => setMinNodeCount(uint256)
80a1c4f5 => setAllowedMargin(address,bool)
25f2f479 => setMinPositionSize(address,uint256)
16c38b3c => setPaused(bool)
d2fa635e => setMaxGasPrice(uint256)
6fcba377 => setFees(uint256,uint256,uint256,uint256)
41adb7b => setNode(address,bool)
058f3bc8 => setChainlinkEnabled(bool)
b747c8cc => getLiqPrice(uint256)

```



```
e691d03b => setTrustedForwarder(address,bool)
572b6c05 => isTrustedForwarder(address)
50d25bcd => latestAnswer()
360e8043 => pnl(bool,uint256,uint256,uint256,int256)
d63b3c7b => liqPrice(bool,uint256,uint256,int256,uint256)
d4af2822 =>
verifyAndCreatePrice(uint256,uint256,bool,address,PriceData[],bytes[],mapping(address)
ce62a3bf => median(uint256[])
f5a956d8 => swap(uint256[],uint256,uint256)
```

# InterFi

## Smart Contract Security Audit





# Manual Analysis

Function	Description	Available	Status
<b>Total Supply</b>	provides information about the total token supply	Yes	<b>Passed</b>
<b>Balance Of</b>	provides account balance of the owner's account	Yes	<b>Passed</b>
<b>Transfer</b>	executes transfers of a specified number of tokens to a specified address	Yes	<b>Passed</b>
<b>Approve</b>	allow a spender to withdraw a set number of tokens from a specified account	Yes	<b>Passed</b>
<b>Allowance</b>	returns a set number of tokens from a spender to the owner	Yes	<b>Passed</b>
<b>Burn</b>	executes transfers of a specified number of tokens to a burn address	Yes	<b>! Low</b>
<b>Mint</b>	executes the creation of a specified number of tokens and adds it to the total supply	Yes	<b>Passed</b>
<b>Contract Fees</b>	executes fee collection from swap events and/or transfer events	Yes	<b>! Low</b>
<b>Transfer Ownership</b>	executes transfer of contract ownership to a specified wallet	Yes	<b>Passed</b>
<b>Renounce Ownership</b>	executes transfer of contract ownership to a dead address	Yes	<b>Passed</b>



## Notable Information

- ❖ Tigris Trade's owner(s) can **authorize** certain wallets to be a minter or a protocol. When ownership is transferred, previous authorizations should be nullified.

```
function setProtocol(address _protocol) external onlyOwner {
    protocol = _protocol;
function setMinter(address _minter, bool _bool) external onlyOwner {
    _isMinter[_minter] = _bool;
```

- ❖ GovNFT.sol smart contract owner can `mintMany()`, and `mint()` NFTs. StableToken.sol smart contract minter can `mintFor()` NFTs in externally owned accounts (EOA). There's an elevated risk of out-of-gas, and potential resource exhaustion errors with multi wallet mint.

```
function mintFor(
    address account,
    uint256 amount
    public
    virtual
    onlyMinter()
function mintMany(uint _amount) external onlyOwner {
    for (uint i=0; i<_amount; i++) {
        _mint(_msgSender(), counter);
function mint() external onlyOwner {
    _mint(_msgSender(), counter);
```

- ❖ PairsContract.sol Smart contract owner can **pause asset**.

```
function pauseAsset(uint256 _asset, bool _isPaused) external onlyOwner {
    bytes memory _name = bytes(_idToAsset[_asset].name);
    require(_name.length > 0, "!Asset");
```

- ❖ Trading.sol smart contract owner can **switch trading status**; this function module may be used to stop the users from trading.

```
function setPaused(bool _paused) external onlyOwner {
    paused = _paused;
```



- ❖ StableToken.sol smart contract minter can initiate `burnFrom()`. EOA allowance requirements must be met to execute this function.
- ❖ Tigris Trade's smart contracts do not utilize **re-entrancy guard** to prevent re-entrant calls.
- ❖ Trading.sol and NativeStableVault.sol smart contracts call `receive()`, it is executed on a call to the contract with empty call data. This is the function that is executed on plain ether transfers such as `send()`, and `transfer()`. Make sure the contract can receive token through a regular transaction, and does not throw an exception.

```
receive() external payable {}
```

- ❖ Smart contract owner can **set block delay**.

```
function setBlockDelay(
    uint _blockDelay
    external
    onlyOwner
```



- ❖ Trading.sol smart contract owner can **change transaction fees**. This function module can be used to impose extraordinary fees. No arbitrary limit set.

```
function setFees(uint _daoFees, uint _burnFees, uint _referralFees, uint _botFees) external
onlyOwner {
    require(_daoFees >= _botFees+_referralFees);
    daoFees = _daoFees;
    burnFees = _burnFees;
    referralFees = _referralFees;
    botFees = _botFees;
```

- ❖ GovNFT.sol smart contract owner can **set gas**. Trading.sol smart contract owner can **set max gas price**. `setGas()` and `setMaxGasPrice()` value change must be set within set parameters.
- ❖ Smart contract has an **informational severity issue** which may or may not create any functional vulnerability.

**"severity": 4, (! Informational Severity)**

**"Irrelevant Code"**



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

"severity": 4, (! Informational Severity)

"Floating Pragma"

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

"severity": 8, (! Low Severity)

"Utilization of block.timestamp"

# InterFi

Smart Contract  
Security Audit



# SWC Attacks

SWC ID	Description	Status
SWC-101	Integer Overflow and Underflow	Passed
SWC-102	Outdated Compiler Version	! Informational
SWC-103	Floating Pragma	! Informational
SWC-104	Unchecked Call Return Value	Passed
SWC-105	Unprotected Ether Withdrawal	Passed
SWC-106	Unprotected SELF-DESTRUCT Instruction	Passed
SWC-107	Re-entrancy	Acknowledged
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	Passed

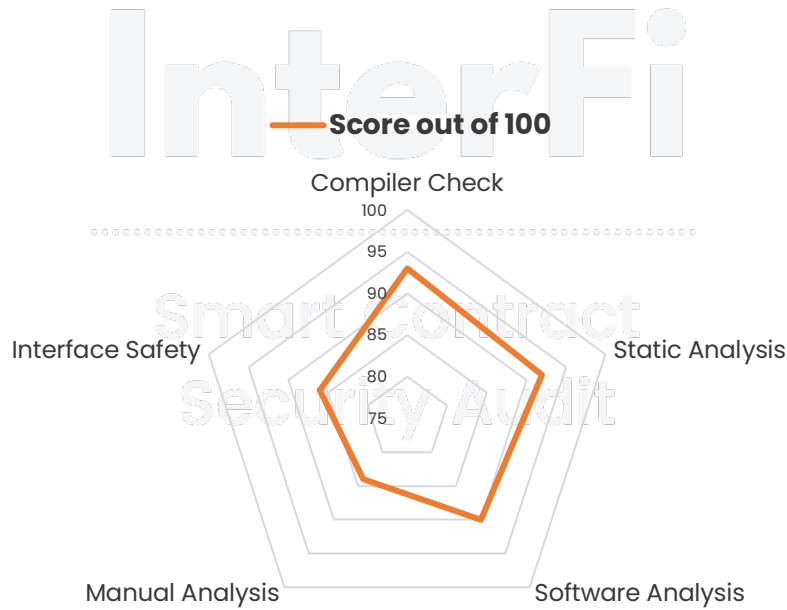


<b>SWC-119</b>	Shadowing State Variables	<b>Passed</b>
<b>SWC-120</b>	Weak Sources of Randomness from Chain Attributes	<b>Passed</b>
<b>SWC-121</b>	Missing Protection against Signature Replay Attacks	<b>Passed</b>
<b>SWC-122</b>	Lack of Proper Signature Verification	<b>Passed</b>
<b>SWC-123</b>	Requirement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



# Risk Status & Radar Chart

Risk Severity	Status
High	No high severity issues identified
Medium	No medium severity issues identified
Low	3 low severity issues identified
Informational	2 informational severity issues identified
Centralization Risk	Active contract ownership identified



## Auditor's Verdict

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

- ❖ Tigris Trade's solidity source codes have **LOW RISK SEVERITY**
- ❖ Tigris Trade's smart contracts have **ACTIVE OWNERSHIP**
- ❖ 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.





# 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>





RELENTLESSLY SECURING THE PUBLIC BLOCKCHAIN | MADE IN CANADA 