



# SMART CONTRACT SECURITY AUDIT OF



# YEARNNFT

SMART CONTRACT AUDIT | TEAM KYC | PROJECT EVALUATION

RELENTLESSLY SECURING THE PUBLIC BLOCKCHAIN | MADE IN CANADA 

# Summary

<b>Auditing Firm</b>	InterFi Network
<b>Architecture</b>	InterFi "Echelon" Auditing Standard
<b>Smart Contract Audit Approved By</b>	Chris   Blockchain Specialist at InterFi Network
<b>Project Overview Approved By</b>	Albert   Marketing Specialist at InterFi Network
<b>Platform</b>	Solidity
<b>Mandatory Audit Check</b>	Static, Software, Auto Intelligent & Manual Analysis
<b>Consultation Request Date</b>	November 22, 2021
<b>Report Date</b>	November 24, 2021

InterFi

## 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:

- ❖ **YearnNFT Finance's smart contract source code has MEDIUM RISK SEVERITY.**
- ❖ **YearnNFT Finance has **PASSED** the smart contract audit.**
- ❖ **Smart contract owner **CAN MINT** tokens after initial contract creation/deployment.**

🔴 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/interfinetwork>



# Table Of Contents

## **Project Information**

Overview .....	4
----------------	---

## **InterFi “Echelon” Audit Standard**

Audit Scope & Methodology .....	6
InterFi’s Risk Classification.....	8

## **Smart Contract Risk Assessment**

Static Analysis.....	9
Software Analysis .....	11
Manual Analysis.....	13
SWC Attacks.....	17
Risk Status & Radar Chart.....	19

## **Report Summary**

Auditor’s Verdict .....	20
-------------------------	----

## **Legal Advisory**

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



# Project Overview

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

## About YearnNFT Finance

YearnNFT Finance is a BSC based NFT marketplace to trade digital collections. Powered by the native asset YFNT token, the low supply NFT token. We are building an ecosystem of nft creators and traders with simplified and reliable NFT trading experience.

<b>Project</b>	YearnNFT Finance
<b>Blockchain</b>	Binance Smart Chain
<b>Language</b>	Solidity
<b>Contract</b>	0x151F7cA9Cb58D1Fe11D0a84ebc0e01516f292EF9
<b>Website</b>	<a href="https://yearnft.finance/">https://yearnft.finance/</a>
<b>Telegram</b>	<a href="https://t.me/YearnNFT">https://t.me/YearnNFT</a>
<b>Twitter</b>	<a href="https://twitter.com/YearnNft">https://twitter.com/YearnNft</a>
<b>Reddit</b>	<a href="http://www.reddit.com/user/YearnNFT/">http://www.reddit.com/user/YearnNFT/</a>
<b>Medium</b>	<a href="https://medium.com/@yearnft">https://medium.com/@yearnft</a>



## Public logo



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

<https://bscscan.com/address/0x151f7ca9cb58d1fe11d0a84ebc0e01516f292ef9#code>

Contract Name: YearnNFT Finance

Compiler Version: v0.5.16

Optimization Enabled: Yes with 200 runs

## Solidity Source Code On InterFi GitHub

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

## SHA-1 Hash

Solidity source code is audited at hash #f6f359c6c50bfe274f062b4a3c46794c031dd9c6



# Audit Scope & Methodology

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

## Category

---

### Smart Contract Vulnerabilities

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

### Requirement Violation

- ❖ Ownership Takeover
- ❖ Gas Limit and Loops

### Source Code Review

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

### Functional Assessment

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



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

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

1. Solidity smart contract source code reviewal:
  - ❖ Review of the specifications, sources, and instructions provided to InterFi to make sure we understand the size, scope, and functionality of the smart contract.
  - ❖ Manual review of code, which is the process of reading source code line-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 Code Analyzer
- ❖ 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

```

**IBEP20** | Interface | |||
| L | totalSupply | External ! | |NO ! |
| L | decimals | External ! | |NO ! |
| L | symbol | External ! | |NO ! |
| L | name | External ! | |NO ! |
| L | getOwner | External ! | |NO ! |
| L | balanceOf | External ! | |NO ! |
| L | transfer | External ! |  |NO ! |
| L | allowance | External ! | |NO ! |
| L | approve | External ! |  |NO ! |
| L | transferFrom | External ! |  |NO ! |
|||||
**Context** | Implementation | |||
| L | <Constructor> | Internal   | |
| L | _msgSender | Internal  |
| L | _msgData | Internal  |
|||||
**SafeMath** | Library | |||
| L | add | Internal  | |
| L | sub | Internal  |
| L | sub | Internal  |
| L | mul | Internal  |
| L | div | Internal  |
| L | div | Internal  |
| L | mod | Internal  |
| L | mod | Internal  |
|||||
**Ownable** | Implementation | Context |||
| L | <Constructor> | Internal   | | |
| L | owner | Public ! | |NO ! |
| L | renounceOwnership | Public ! |  | onlyOwner |

```



```

| L | transferOwnership | Public ! | 🔴 | onlyOwner |
| L | _transferOwnership | Internal 🔒 | 🔴 | |
|||||
| **YEARNFT** | Implementation | Context, IBEP20, Ownable |||
| L | <Constructor> | Public ! | 🔴 | NO ! |
| L | getOwner | External ! | | NO ! |
| L | decimals | External ! | | NO ! |
| L | symbol | External ! | | NO ! |
| L | name | External ! | | NO ! |
| L | totalSupply | External ! | | NO ! |
| L | balanceOf | External ! | | NO ! |
| L | transfer | External ! | 🔴 | NO ! |
| L | allowance | External ! | | NO ! |
| L | approve | External ! | 🔴 | NO ! |
| L | transferFrom | External ! | 🔴 | NO ! |
| L | increaseAllowance | Public ! | 🔴 | NO ! |
| L | decreaseAllowance | Public ! | 🔴 | NO ! |
| L | mint | Public ! | 🔴 | onlyOwner |
| L | _transfer | Internal 🔒 | 🔴 | |
| L | _mint | Internal 🔒 | 🔴 | |
| L | _burn | Internal 🔒 | 🔴 | |
| L | _approve | Internal 🔒 | 🔴 | |
| L | _burnFrom | Internal 🔒 | 🔴 | |

```

## Smart Contract Security Audit



# Smart Contract – Software Analysis

## Function Signatures

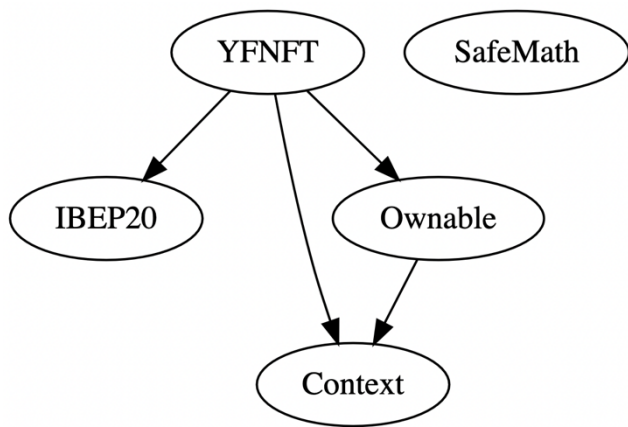
```

39509351 => increaseAllowance(address,uint256)
18160ddd => totalSupply()
313ce567 => decimals()
95d89b41 => symbol()
06fdde03 => name()
893d20e8 => getOwner()
70a08231 => balanceOf(address)
a9059cbb => transfer(address,uint256)
dd62ed3e => allowance(address,address)
095ea7b3 => approve(address,uint256)
23b872dd => transferFrom(address,address,uint256)
119df25f => _msgSender()
8b49d47e => _msgData()
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)
8da5cb5b => owner()
715018a6 => renounceOwnership()
f2fde38b => transferOwnership(address)
d29d44ee => _transferOwnership(address)
a457c2d7 => decreaseAllowance(address,uint256)
a0712d68 => mint(uint256)
30e0789e => _transfer(address,address,uint256)
4e6ec247 => _mint(address,uint256)
6161eb18 => _burn(address,uint256)
104e81ff => _approve(address,address,uint256)
a22b35ce => _burnFrom(address,uint256)

```



## Inheritance Graph



# InterFi

Smart Contract  
Security Audit



# Smart Contract – Manual Analysis

Function	Description	Tested	Verdict
<b>Total Supply</b>	provides information about the total token supply	Yes	Passed
<b>Balance Of</b>	provides account balance of the owner's account	Yes	Passed
<b>Transfer</b>	executes transfers of a specified number of tokens to a specified address	Yes	Passed
<b>Approve</b>	allow a spender to withdraw a set number of tokens from a specified account	Yes	Passed
<b>Allowance</b>	returns a set number of tokens from a spender to the owner	Yes	Passed
<b>Buy Back</b>	is an action in which the project buys back its tokens from the existing holders usually at a market price	NA	NA
<b>Burn</b>	executes transfers of a specified number of tokens to a burn address	NA	NA
<b>Mint</b>	executes creation of a specified number of tokens and adds it to the total supply	Yes	Passed
<b>Rebase</b>	circulating token supply adjusts (increases or decreases) automatically according to a token's price fluctuations	NA	NA
<b>Blacklist</b>	stops specified wallets from interacting with the smart contract function modules	NA	NA
<b>Lock</b>	stops or locks all function modules of the smart contract	NA	NA



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



## Best Practices

- ❖ Owner cannot stop or pause the smart contract.
- ❖ Owner cannot lock or burn the user assets.
- ❖ The smart contract utilizes "SafeMath" function to avoid common smart contract vulnerabilities.

```
string private _name = "YearnNFT Finance";

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");
```

## Security Audit

## Warning

- ❖ Active smart contract owner: 0x6e838299116e428d73e5070d47a8782708fb7414
- ❖ ***Be aware that active smart contract owner privileges constitute an elevated impact to smart contract's safety and security.***
- ❖ Owner ***can mint*** tokens after initial contract creation/deployment.



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

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

InterFi

Smart Contract  
Security Audit





# Smart Contract – SWC Attacks

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

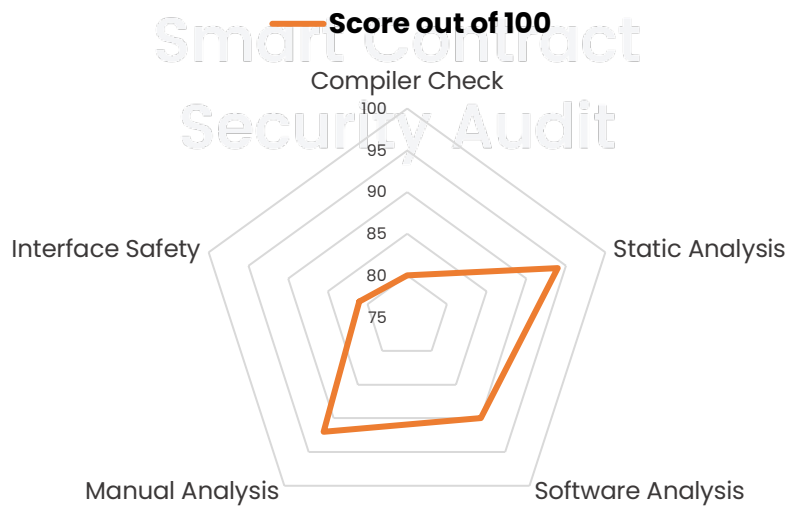


<b>SWC-119</b>	Shadowing State Variables	<b>Passed</b>
<b>SWC-120</b>	Weak Sources of Randomness from Chain Attributes	<b>Passed</b>
<b>SWC-121</b>	Missing Protection against Signature Replay Attacks	<b>Passed</b>
<b>SWC-122</b>	Lack of Proper Signature Verification	<b>Passed</b>
<b>SWC-123</b>	Requirement 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 hardcoded gas amount	<b>Passed</b>
<b>SWC-135</b>	Code With No Effects (Irrelevant/Dead Code)	<b>Passed</b>
<b>SWC-136</b>	Unencrypted Private Data On-Chain	<b>Passed</b>



# Smart Contract - Risk Status & Radar Chart

Risk Severity	Status
<b>! Critical</b>	None critical severity issues identified
<b>! High</b>	None high severity issues identified
<b>! Medium</b>	2 medium severity issues identified
<b>! Low</b>	1 low severity issue identified
<b>Verified</b>	54 functions and instances verified and checked
<b>Safety Score</b>	81 out of 100



## 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.

**YearnNFT Finance's smart contract source code has MEDIUM RISK SEVERITY.**

**YearnNFT Finance has **PASSED** the smart contract audit.**

**Smart contract owner **CAN MINT** tokens after initial contract creation/deployment.**

# InterFi

.....

## Smart Contract Security Audit

### 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/interfinetwork>.....

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





**@INTERFINETWORK**

**RELENTLESSLY SECURING THE PUBLIC BLOCKCHAIN | MADE IN CANADA **