Yearn Gold Finance

Token

Smart Contract Audit Report

IMMUNE BYTES

Audits

October 29, 2020

Introduction

1. About Yearn Gold Finance

Yearn Gold Finance (YGF) is a protocol that unifies leading DeFi protocols and blockchain infrastructure by standardizing communication between them to create and execute complex financial transactions while championing Privacy, Anonymity, and Sovereignty. It's a community project where only a small portion is allocated to Dev & the YGF team members.

YGF protocol will combine some of the best features of a decentralized finance market protocol, maximize its unique features, enabling users to enjoy the promise of a decentralized finance marketplace.

https://yearngoldfinance.com/

2. About ImmuneBytes

ImmuneBytes is a security start-up to provide professional services in the blockchain space. The team has hands-on experience in conducting smart contract audits, penetration testing, and security consulting. ImmuneBytes's security auditors have worked on various A-league projects and have a great understanding of DeFi projects like AAVE, Compound, 0x Protocol, Uniswap, dydx.

The team has been able to secure 15+ blockchain projects by providing security services on different frameworks. ImmuneBytes team helps start-up with a detailed analysis of the system ensuring security and managing the overall project.

Visit http://immunebytes.com/ to know more about the services.

Documentation Details

Yearn Gold Finance team has provided documentation for the purpose of conducting the audit. The documents are:

1. Short Description on Telegram
2. Medium Link
   https://info-ygf.medium.com/

Audit Process & Methodology

ImmueBytes team has performed thorough testing of the project starting with analyzing the code design patterns in which we reviewed the smart contract architecture to ensure it is structured and safe use of third-party smart contracts and libraries.

Our team then performed a formal line by line inspection of the Smart Contract in order to find any potential issues like Signature Replay Attacks, Unchecked External Calls, External Contract Referencing, Variable Shadowing, Race conditions, Transaction-ordering dependence, timestamp dependence, DoS attacks, and others.

In the Unit testing phase, we run unit tests written by the developer in order to verify the functions work as intended. In Automated Testing, we tested the Smart Contract with our in-house developed tools to identify vulnerabilities and security flaws.

The code was audited by a team of independent auditors which includes -

1. Testing the functionality of the Smart Contract to determine proper logic has been followed throughout.
2. Analyzing the complexity of the code by thorough, manual review of the code, line-by-line.
3. Deploying the code on testnet using multiple clients to run live tests.
4. Analyzing failure preparations to check how the Smart Contract performs in case of bugs and vulnerabilities.
5. Checking whether all the libraries used in the code are on the latest version.
6. Analyzing the security of the on-chain data.

Audit Details

- Project Name: Yearn Gold Finance
- Languages: Solidity(Smart contract), Javascript(Unit Testing)
- Etherscan Link for the audit: https://etherscan.io/address/0x5A08c1A3455E37Ac6bE0EaE40f2a451D10529824#code

Audit Goals

The focus of the audit was to verify that the smart contract system is secure, resilient, and working according to its specifications. The audit activities can be grouped into the following three categories:

1. Security: Identifying security related issues within each contract and within the system of contracts.
2. Sound Architecture: Evaluation of the architecture of this system through the lens of established smart contract best practices and general software best practices.
3. Code Correctness and Quality: A full review of the contract source code. The primary areas of focus include:
    a. Correctness
    b. Readability
    c. Sections of code with high complexity
    d. Quantity and quality of test coverage

Security Level References

Every issue in this report was assigned a severity level from the following:

High severity issues will bring problems and should be fixed.

Medium severity issues could potentially bring problems and should eventually be fixed.

Low severity issues are minor details and warnings that can remain unfixed but would be better fixed at some point in the future.

Issues	High	Medium	Low
Open	-	-	1
Closed	-	-	-

High severity issues

No High Severity Issues Found

Medium severity issues

No High Severity Issues Found

Low severity issues

1. **Validation in _supportCM() can be improved.**
   The **_supportCM**() function in **CM** smart contract has a **require** statement which checks that the **msg.value** should be **greater than 0.045 Ether** and then transfers only **0.045 Ether** to a predefined address, which is not completely correct. This function is called when the **CMErc20BurnSnap** token contract is deployed. The deployer has to supply an amount a bit higher than **0.045 Ether (+1 wei)** and any amount above **0.045 Ether** gets locked inside the deployed token contract.

   Recommendation:
   Consider modifying the **require** statement to check for **equality** instead of **greater than** or transfer the entire **msg.value** to the predefined address.

Since the smart contract of **YGF Token** inherits and uses the open sourced and well audited smart contract of **OpenZeppelin** like **ERC20**, **ERC20Burnable** and **ERC20Snapshot**, no high and medium severity issues were found. However **one** low severity issue was found which is mentioned above.

The contracts are well written and well documented as well. However there are some Notes regarding the token contract which are mentioned below.

Notes

1. **Yearn Gold Finance token is a Burnable ERC20 token.**

Yearn Gold Finance token is a **Burnable** token inherited from **OpenZeppelin's Burnable** and **ERC20Snapshot** smart contract. Total supply of the token can be burnt/reduced by token holders at their will by burning the tokens they own.

2. **Capped Total Supply - 50,000 YGF.**

YGF Token has a total supply of **50,000 (50 thousand)** tokens which was initially minted to the deployer of the token contract. This means that while the tokens can be burned, no new tokens can be minted.

Unit Test

No Test Cases have been written by the developers for Yearn Gold Finance.

Recommendation:
Our team suggests that the developer should write extensive test cases.

Concluding Remarks

While conducting the audits of Yearn Gold Finance smart contract, it was observed that the contracts only contain 1 Low severity issues, along with some areas of recommendations.

Our auditors suggest that issues should be resolved by Yearn Gold Finance's developers. Resolving the areas of recommendations are up to Yearn Gold Finance's discretion. The recommendations given will improve the operations of the smart contract.

Disclaimer

ImmuneBytes's audit does not provide a security or correctness guarantee of the audited smart contract. Securing smart contracts is a multistep process, therefore running a bug bounty program as a complement to this audit is strongly recommended.

Our team does not endorse the Yearn Gold Finance platform or its product neither this audit is investment advice.
Notes:

- Please make sure contracts deployed on the mainnet are the one audited.
- Check for the code refactor by the team on critical issues.

ImmuneBytes Pvt Ltd.