



Code Security Assessment

Hololoot

Jan 18th, 2022



Table of Contents

Summary

Overview

[Project Summary](#)

[Audit Summary](#)

[Vulnerability Summary](#)

[Audit Scope](#)

Findings

[GLOBAL-01 : Centralization Risk](#)

[TTH-01 : Missing Emit Events](#)

[TTH-02 : Missing Sanity Check](#)

Appendix

Disclaimer

About

Summary

This report has been prepared for Hololoot to discover issues and vulnerabilities in the source code of the Hololoot project as well as any contract dependencies that were not part of an officially recognized library. A comprehensive examination has been performed, utilizing Static Analysis and Manual Review techniques.

The auditing process pays special attention to the following considerations:

- Testing the smart contracts against both common and uncommon attack vectors.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

The security assessment resulted in findings that ranged from critical to informational. We recommend addressing these findings to ensure a high level of security standards and industry practices. We suggest recommendations that could better serve the project from the security perspective:

- Enhance general coding practices for better structures of source codes;
- Add enough unit tests to cover the possible use cases;
- Provide more comments per each function for readability, especially contracts that are verified in public;
- Provide more transparency on privileged activities once the protocol is live.

Overview

Project Summary

Project Name	Hololoot
Platform	Custom
Language	Solidity
Codebase	https://github.com/Holohome-DevTeam/hololoot-contracts
Commit	81686e74a3296104cf3f294380dca978693a7af6 88c14957bec69e17adfbe11e9c8c0ee9c8d3ade0 a1b44aed6f3391a928e46604d9abb246c43fc09a

Audit Summary

Delivery Date	Jan 18, 2022
Audit Methodology	Static Analysis, Manual Review

Vulnerability Summary

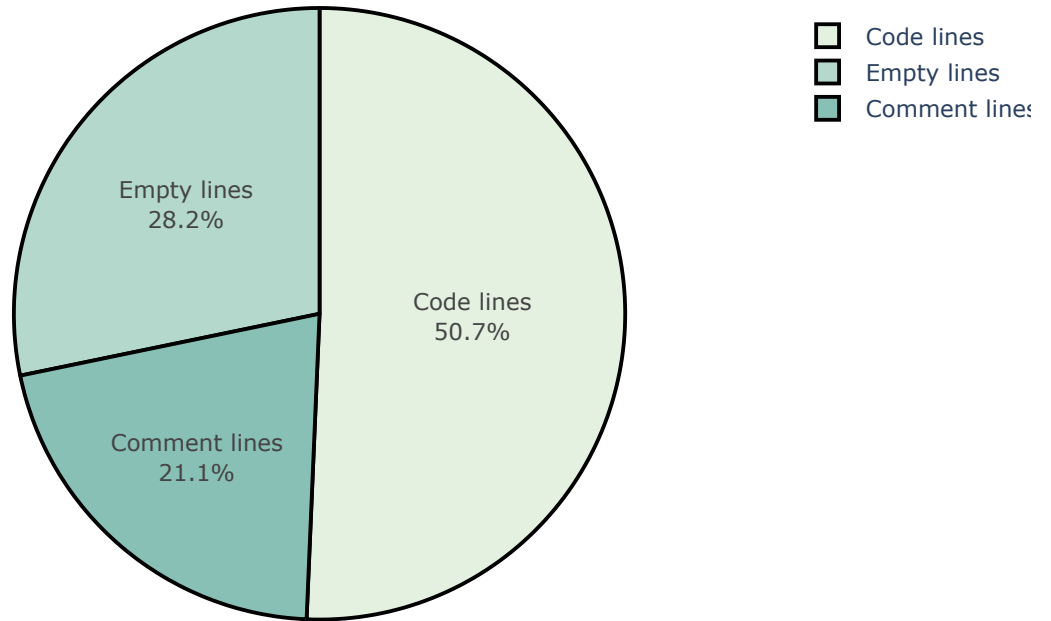
Vulnerability Level	Total	⚠ Pending	⊗ Declined	ℹ Acknowledged	🔄 Partially Resolved	✅ Resolved
● Critical	0	0	0	0	0	0
● Major	1	0	0	0	0	1
● Medium	0	0	0	0	0	0
● Minor	0	0	0	0	0	0
● Informational	2	0	0	0	0	2
● Discussion	0	0	0	0	0	0

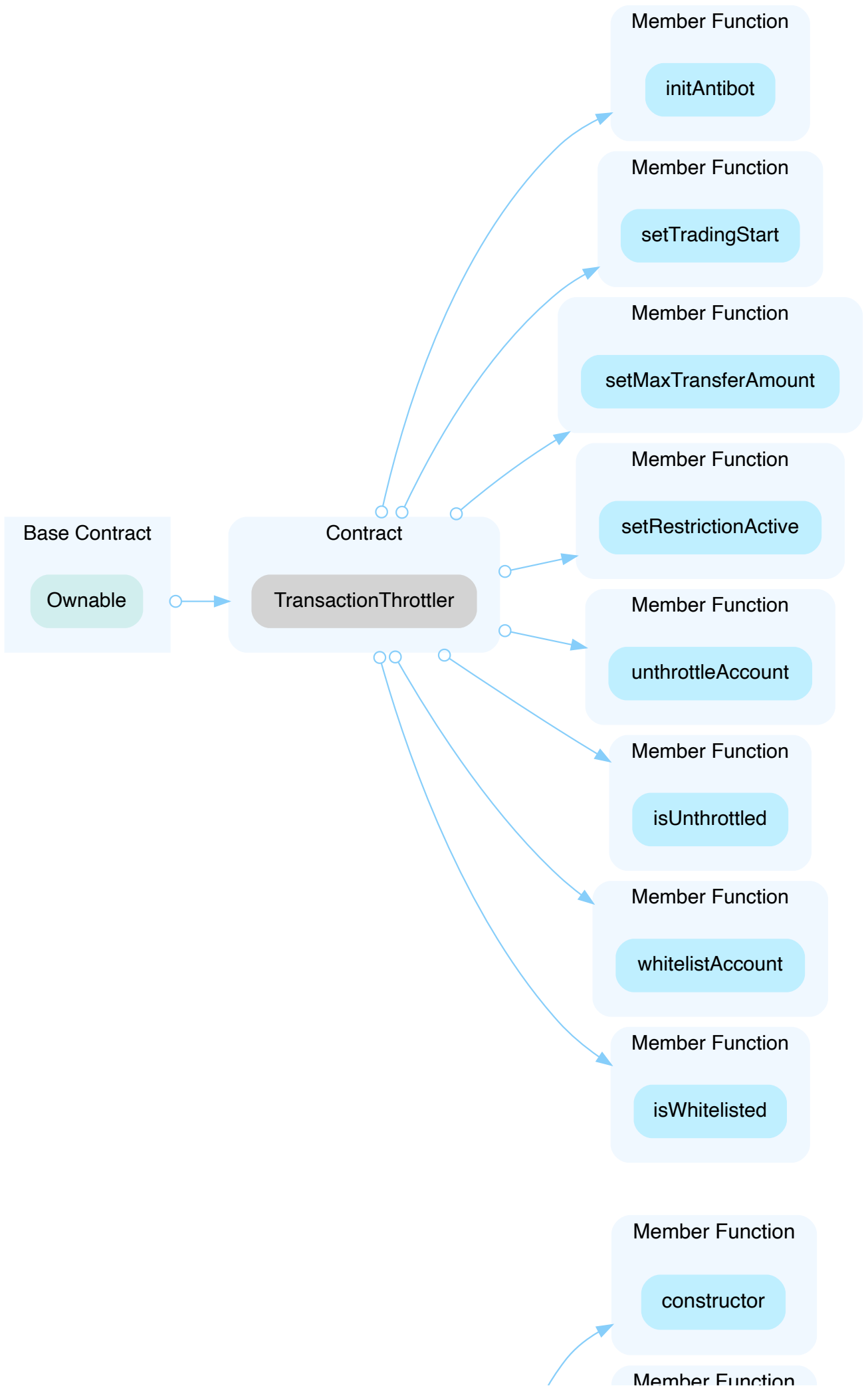
Audit Scope

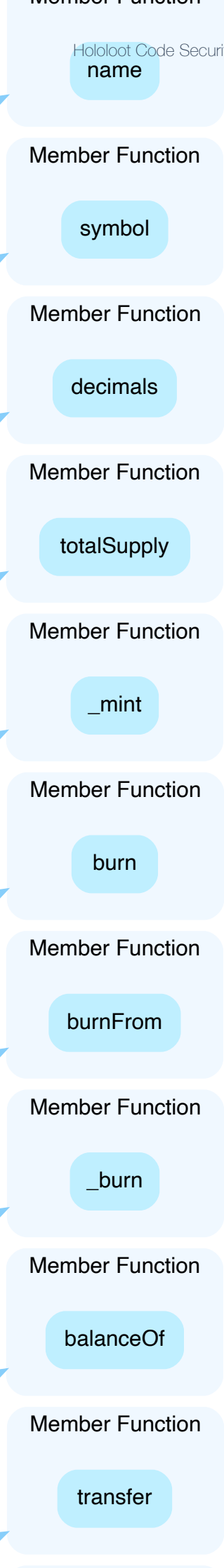
ID	File	SHA256 Checksum
FMH	contracts/abstract/FeeManager.sol	a2444f98818ce553b1392b75c7b2af5c7b24c65a60d22e8742c16eb953716435
ECD	contracts/external/openzeppelin/ECDSA.sol	5738c76bb6a1ea368a2e997981566215259f9abd34e94025e599edfec5fe6d92
EIP	contracts/external/openzeppelin/draft-EIP712.sol	1b06905c0a7c141a51b12ac967fc85ef0cd06cb859a6b42efa1fa2bd3f809c28
OHC	contracts/helpers/Ownable.sol	f3a652aa4e22f41d1f1f8a1dc72a23357558bf87c02ade01adbce33c9d472faf
TTH	contracts/helpers/TransactionThrottler.sol	e826e302a6290eff44bf281657ea411b5e5433f8eec76448dff74dec1c64ab64
IER	contracts/interfaces/IERC20.sol	2e3c98277f33afa9cee596ab89c4392f09da72b2b987a739dd35c48697fa2920
CHC	contracts/libraries/Constants.sol	80462f6dbb1d51271f0f479a6bd2c9a626dbd6bcaeff3a8103f327ff169dba5d
HHC	contracts/Hololoot.sol	ecc1b8ce082f71ef50f7896bea167c4033f7e46b282388979f9547d776b2a928

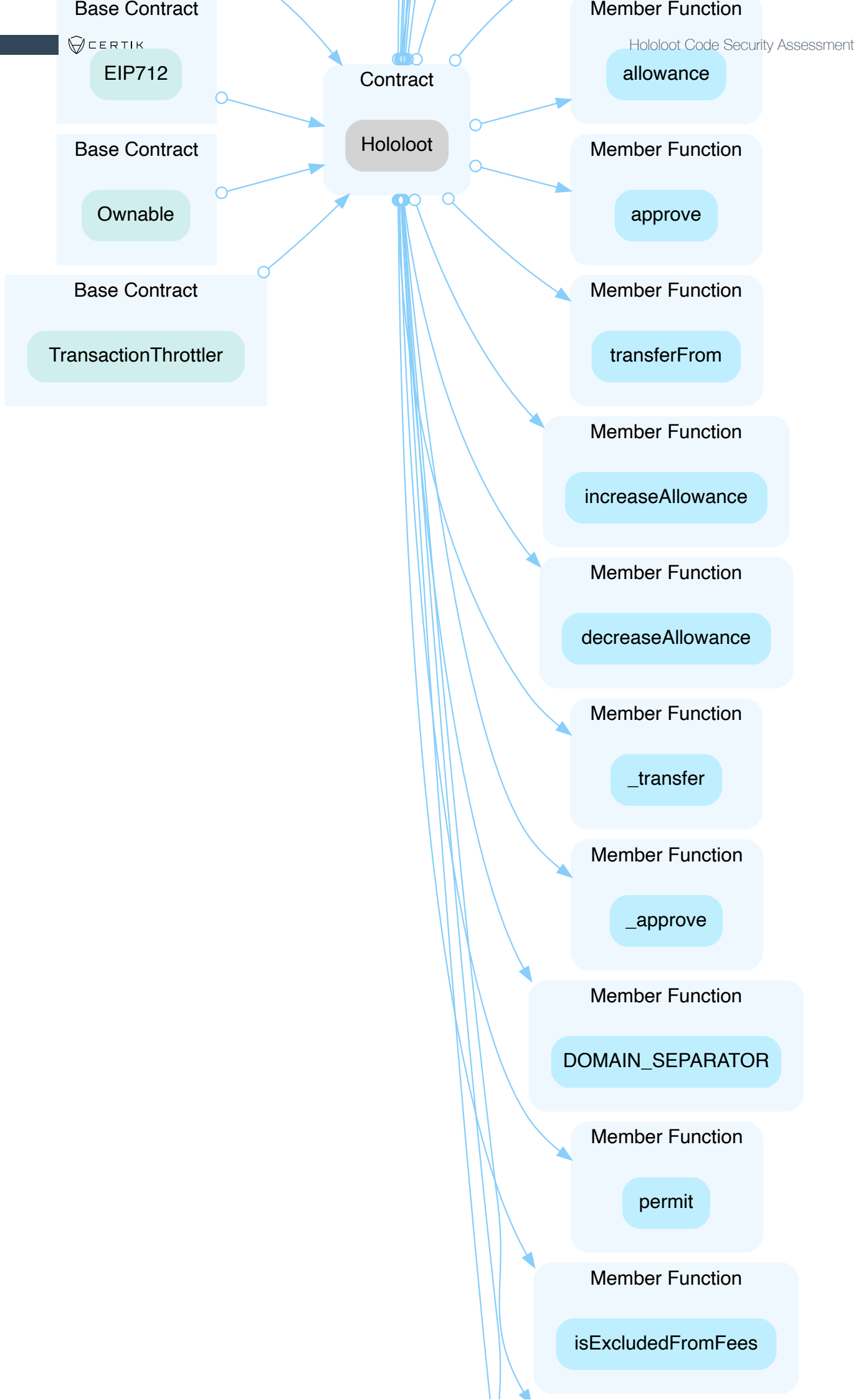
Diagrams

Source Line Chart









Member Function

Holoboot Code Security Assessment

setExcludedFromFees

Member Function

setTransferFeeBPS

Member Function

changeFeeContract

Findings



■ Critical	0 (0.00%)
■ Major	1 (33.33%)
■ Medium	0 (0.00%)
■ Minor	0 (0.00%)
■ Informational	2 (66.67%)
■ Discussion	0 (0.00%)

ID	Title	Category	Severity	Status
GLOBAL-01	Centralization Risk	Centralization / Privilege	● Major	☑ Resolved
TTH-01	Missing Emit Events	Coding Style	● Informational	☑ Resolved
TTH-02	Missing Sanity Check	Logical Issue	● Informational	☑ Resolved

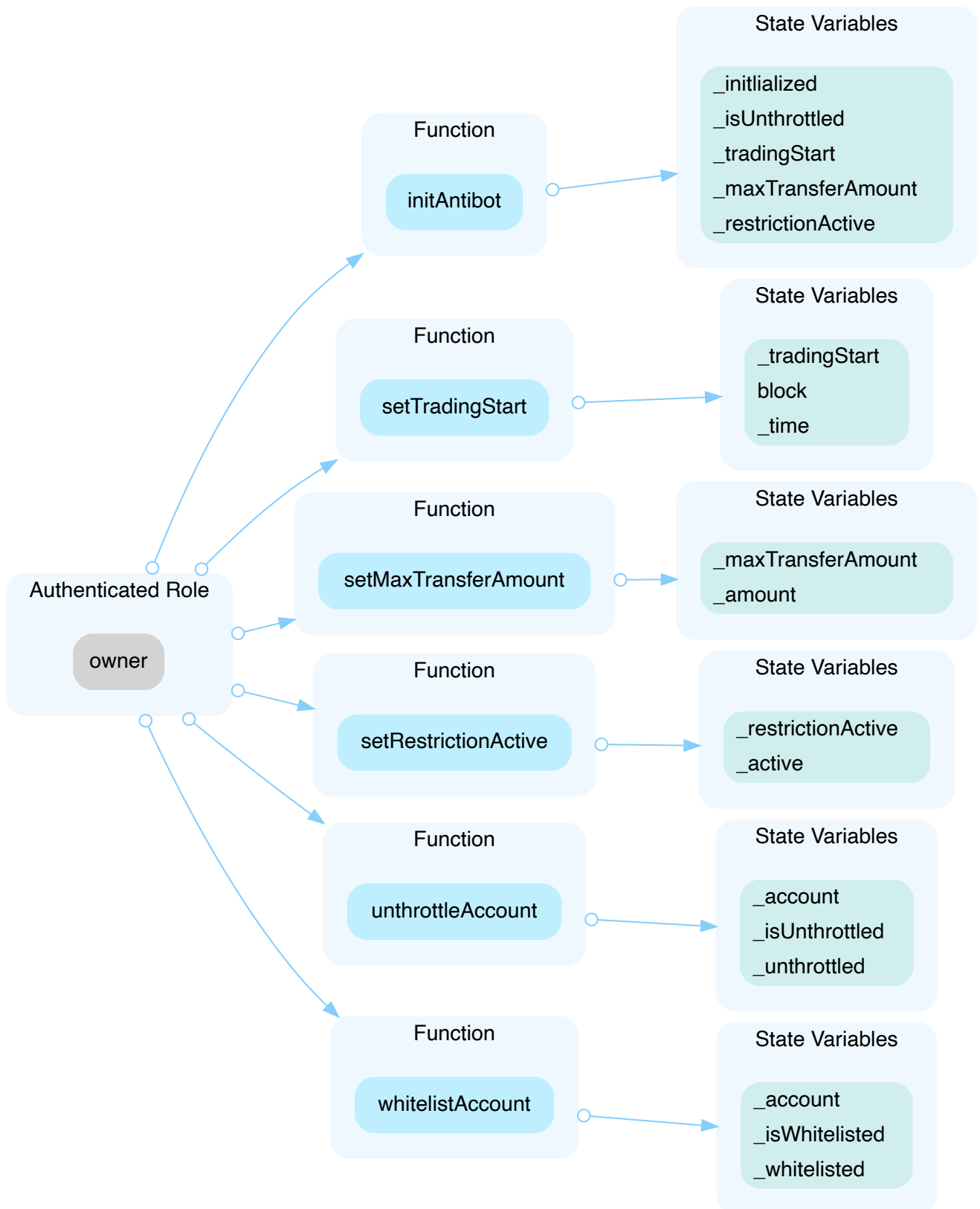
GLOBAL-01 | Centralization Risk

Category	Severity	Location	Status
Centralization / Privilege	● Major	Global	✓ Resolved

Description

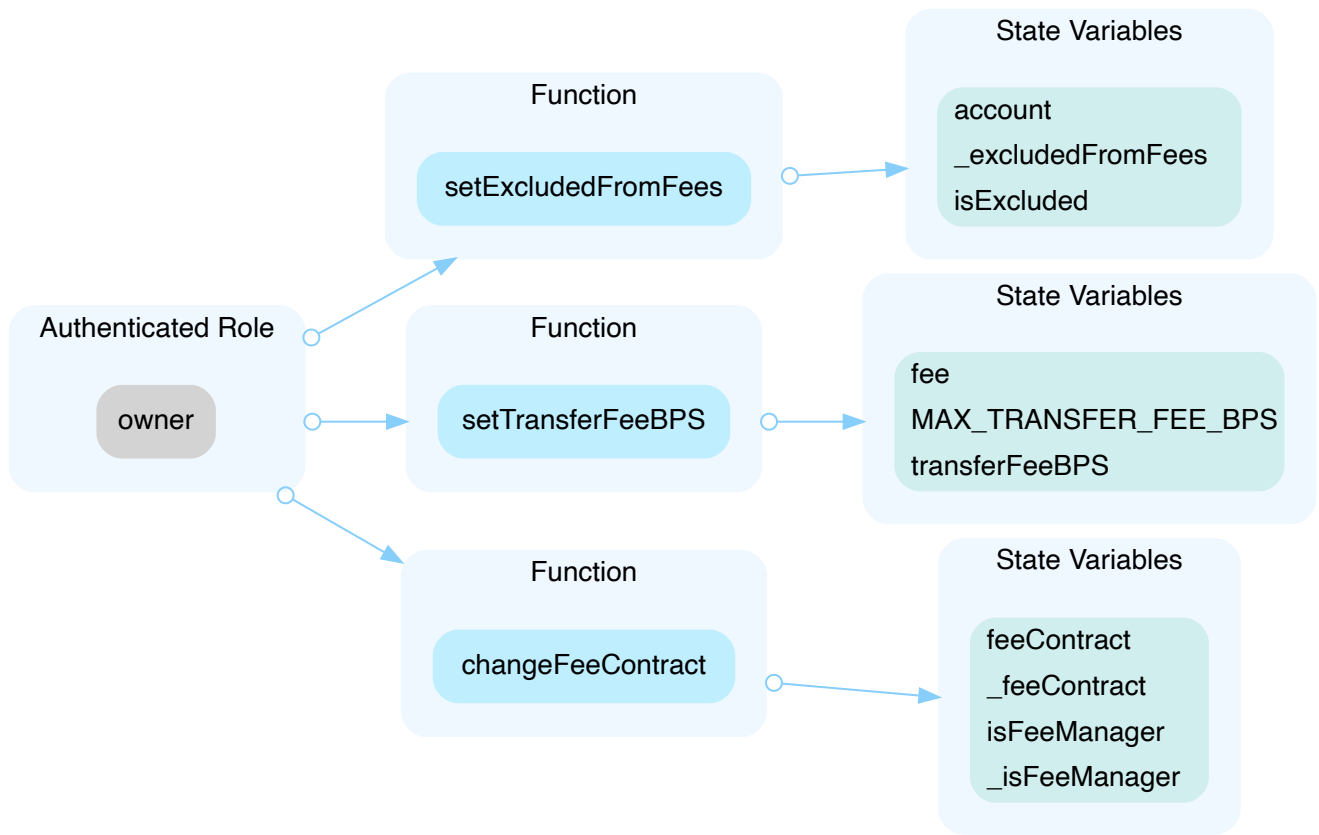
In the contract, `TransactionThrottler`, the role, `owner`, has the authority over the functions shown in the diagram below.

Any compromise to the privileged account which has access to `owner` may allow the hacker to take advantage of this.



In the contract, `Hololoot`, the role, `owner`, has the authority over the functions shown in the diagram below.

Any compromise to the privileged account which has access to `owner` may allow the hacker to take advantage of this.



Recommendation

We advise the client to carefully manage the privileged account's private key to avoid any potential risks of being hacked.

In general, we strongly recommend centralized privileges or roles in the protocol to be improved via a decentralized mechanism or smart-contract-based accounts with enhanced security practices, e.g., Multisignature wallets.

Indicatively, here is some feasible suggestions that would also mitigate the potential risk at the different level in term of short-term and long-term:

- Time-lock with reasonable latency, e.g., 48 hours, for awareness on privileged operations;
- Assignment of privileged roles to multi-signature wallets to prevent a single point of failure due to the private key;
- Introduction of a DAO/governance/voting module to increase transparency and user involvement.

Alleviation

[Hololoot]: We are acknowledging the issue raised by Certik about the Owner role in the Hololoot token contract. To prevent a single point of failure the Owner account will be assigned to the Gnosis-safe multi-sig wallet after TGE

[Hololoot]: Recommendation to move owner role to the multi-signature wallet was fulfilled. Owner role is set to: [0x2Bcf6f37c563Aadc4acB6FDD7943De3a568E3C68](https://bscscan.com/address/0x2Bcf6f37c563Aadc4acB6FDD7943De3a568E3C68)

<https://bscscan.com/address/0xa797fa4bda7c5a4b3afe73573b9d2ab942365c6f#readContract>

The [0x2Bcf6f37c563Aadc4acB6FDD7943De3a568E3C68](https://bscscan.com/address/0x2Bcf6f37c563Aadc4acB6FDD7943De3a568E3C68) is a Gnosis Safe: <https://gnosis-safe.io/app/bnb:0x2Bcf6f37c563Aadc4acB6FDD7943De3a568E3C68/settings/policies>

[Certik]: The Hololoot team heeded the advice and adopted the Gnosis Safe([0x2Bcf6f37c563Aadc4acB6FDD7943De3a568E3C68](https://bscscan.com/address/0x2Bcf6f37c563Aadc4acB6FDD7943De3a568E3C68)) to the Hololoot deployment([0xa797fa4bda7c5a4b3afe73573b9d2ab942365c6f](https://bscscan.com/address/0xa797fa4bda7c5a4b3afe73573b9d2ab942365c6f)). The `owner` has been transferred to the Gnosis Safe deployment.

There are 4 co-signers of the Gnosis Safedeployment and any transaction requires the confirmation of 2 out of 4 co-signers. The brief information of the co-signers can found as following:

- [0x1AEb024d15508F39812d8A53744224A781262D8c](https://bscscan.com/address/0x1AEb024d15508F39812d8A53744224A781262D8c)
- [0x2A467Dd0732Ac2B1eCbcDb03abFAaec5E0c333A5](https://bscscan.com/address/0x2A467Dd0732Ac2B1eCbcDb03abFAaec5E0c333A5)
- [0x8F87884689a86e39bAccc884944D38EFA961E116](https://bscscan.com/address/0x8F87884689a86e39bAccc884944D38EFA961E116)
- [0xf1221c5aA63C3f40E5a81f2aec8432D8ba8B99bd](https://bscscan.com/address/0xf1221c5aA63C3f40E5a81f2aec8432D8ba8B99bd)

The details of Gnosis Safe deployment can be found in <https://hololoot.medium.com/hololoot-code-under-the-knife-eaacf9ee9cf>

TTH-01 | Missing Emit Events

Category	Severity	Location	Status
Coding Style	● Informational	contracts/helpers/TransactionThrottler.sol: 23~30	✓ Resolved

Description

There should always be events emitted in the sensitive functions that are controlled by centralization roles.

Recommendation

It is recommended emitting events for the sensitive functions that are controlled by centralization roles.

Alleviation

[Holoboot]: Recommendation applied. Emitting events added to initAntibot function.

[Certik]: The client heeded the advice and added the events in the function in the commit [88c14957bec69e17adfbe11e9c8c0ee9c8d3ade0](#)

TTH-02 | Missing Sanity Check

Category	Severity	Location	Status
Logical Issue	● Informational	contracts/helpers/TransactionThrottler.sol: 68	🕒 Resolved

Description

The modifier `transactionThrottler()` is designed to perform a series of sanity checks for ERC20 balance transfer functionality. It will take `sender` and `recipient` parameters. As the transfer from one account to itself is meaningless, a sanity check could help to reduce the gas cost in this case.

Recommendation

We advise the client to consider adding a check to validate if `sender` is not equal to `recipient`.

```
require( sender != recipient, "sender is recipient");
```

Alleviation

[Hololoot]: The client heeded the advice and updated the codebase in the commit [a1b44aed6f3391a928e46604d9abb246c43fc09a](#)

Appendix

Finding Categories

Centralization / Privilege

Centralization / Privilege findings refer to either feature logic or implementation of components that act against the nature of decentralization, such as explicit ownership or specialized access roles in combination with a mechanism to relocate funds.

Logical Issue

Logical Issue findings detail a fault in the logic of the linked code, such as an incorrect notion on how `block.timestamp` works.

Coding Style

Coding Style findings usually do not affect the generated byte-code but rather comment on how to make the codebase more legible and, as a result, easily maintainable.

Checksum Calculation Method

The "Checksum" field in the "Audit Scope" section is calculated as the SHA-256 (Secure Hash Algorithm 2 with digest size of 256 bits) digest of the content of each file hosted in the listed source repository under the specified commit.

The result is hexadecimal encoded and is the same as the output of the Linux "sha256sum" command against the target file.

Disclaimer

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability) set forth in the Services Agreement, or the scope of services, and terms and conditions provided to you (“Customer” or the “Company”) in connection with the Agreement. This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes, nor may copies be delivered to any other person other than the Company, without CertiK’s prior written consent in each instance.

This report is not, nor should be considered, an “endorsement” or “disapproval” of any particular project or team. This report is not, nor should be considered, an indication of the economics or value of any “product” or “asset” created by any team or project that contracts CertiK to perform a security assessment. This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model or legal compliance.

This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk. CertiK’s position is that each company and individual are responsible for their own due diligence and continuous security. CertiK’s goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies, and in no way claims any guarantee of security or functionality of the technology we agree to analyze.

The assessment services provided by CertiK is subject to dependencies and under continuing development. 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. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives, and other unpredictable results. The services may access, and depend upon, multiple layers of third-parties.

ALL SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR 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, CERTIK HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS. WITHOUT LIMITING THE FOREGOING, CERTIK SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM COURSE OF DEALING, USAGE, OR TRADE PRACTICE. WITHOUT LIMITING THE FOREGOING, CERTIK MAKES NO WARRANTY OF ANY KIND THAT THE SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF, WILL MEET CUSTOMER’S OR ANY OTHER PERSON’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. WITHOUT LIMITATION TO THE FOREGOING, CERTIK PROVIDES NO WARRANTY OR UNDERTAKING, AND MAKES NO REPRESENTATION OF ANY KIND THAT THE SERVICE WILL MEET CUSTOMER’S REQUIREMENTS, ACHIEVE ANY INTENDED RESULTS, BE COMPATIBLE OR WORK WITH ANY OTHER SOFTWARE, APPLICATIONS, SYSTEMS OR SERVICES, OPERATE WITHOUT INTERRUPTION, MEET ANY PERFORMANCE OR RELIABILITY STANDARDS OR BE ERROR FREE OR THAT ANY ERRORS OR DEFECTS CAN OR WILL BE CORRECTED.

WITHOUT LIMITING THE FOREGOING, NEITHER CERTIK NOR ANY OF CERTIK’S AGENTS MAKES ANY REPRESENTATION OR WARRANTY OF ANY KIND, EXPRESS OR IMPLIED AS TO THE ACCURACY, RELIABILITY, OR CURRENCY OF ANY INFORMATION OR CONTENT PROVIDED THROUGH THE SERVICE. CERTIK WILL ASSUME NO LIABILITY OR RESPONSIBILITY FOR (I) ANY ERRORS, MISTAKES, OR INACCURACIES OF CONTENT AND MATERIALS OR FOR ANY LOSS OR DAMAGE OF ANY KIND INCURRED AS A RESULT OF THE USE OF ANY CONTENT, OR (II) ANY PERSONAL INJURY OR PROPERTY DAMAGE, OF ANY NATURE WHATSOEVER, RESULTING FROM CUSTOMER’S ACCESS TO OR USE OF THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS.

ALL THIRD-PARTY MATERIALS ARE PROVIDED “AS IS” AND ANY REPRESENTATION OR WARRANTY OF OR CONCERNING ANY THIRD-PARTY MATERIALS IS STRICTLY BETWEEN CUSTOMER AND THE THIRD-PARTY OWNER OR DISTRIBUTOR OF THE THIRD-PARTY MATERIALS.

THE SERVICES, ASSESSMENT REPORT, AND ANY OTHER MATERIALS HEREUNDER ARE SOLELY PROVIDED TO CUSTOMER AND MAY NOT BE RELIED ON BY ANY OTHER PERSON OR FOR ANY PURPOSE NOT SPECIFICALLY IDENTIFIED IN THIS AGREEMENT, NOR MAY COPIES BE DELIVERED TO, ANY OTHER PERSON WITHOUT CERTIK’S PRIOR WRITTEN CONSENT IN EACH INSTANCE.

NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING

MATERIALS AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST CERTIK WITH RESPECT TO SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING MATERIALS.

THE REPRESENTATIONS AND WARRANTIES OF CERTIK CONTAINED IN THIS AGREEMENT ARE SOLELY FOR THE BENEFIT OF CUSTOMER. ACCORDINGLY, NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH REPRESENTATIONS AND WARRANTIES AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST CERTIK WITH RESPECT TO SUCH REPRESENTATIONS OR WARRANTIES OR ANY MATTER SUBJECT TO OR RESULTING IN INDEMNIFICATION UNDER THIS AGREEMENT OR OTHERWISE.

FOR AVOIDANCE OF DOUBT, THE SERVICES, INCLUDING ANY ASSOCIATED ASSESSMENT REPORTS OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.

About

Founded in 2017 by leading academics in the field of Computer Science from both Yale and Columbia University, CertiK is a leading blockchain security company that serves to verify the security and correctness of smart contracts and blockchain-based protocols. Through the utilization of our world-class technical expertise, alongside our proprietary, innovative tech, we're able to support the success of our clients with best-in-class security, all whilst realizing our overarching vision; provable trust for all throughout all facets of blockchain.

