# Code Security Assessment

# Numbers Protocol-Audit

Jan 12th, 2022

# Table of Contents

# Summary

This report has been prepared for Numbers Protocol-Audit to discover issues and vulnerabilities in the source code of the Numbers Protocol-Audit 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.

We are not sure the token contracts will be used in which scenarios. The issues caused by the external design logic are not included in the audit scope.

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** | Numbers Protocol-Audit |
| **Platform** | ethereum |
| **Language** | Solidity |
| **Codebase** | https://github.com/numbersprotocol/thunder_bridge/tree/feature-certik-auditing/contracts/flats |
| **Commit** | 3b6165f243e40e0ebf4da62e63141b730ed7cea1 |

## Audit Summary

| | |
|---|---|
| **Delivery Date** | Jan 12, 2022 |
| **Audit Methodology** | Static Analysis, Manual Review |

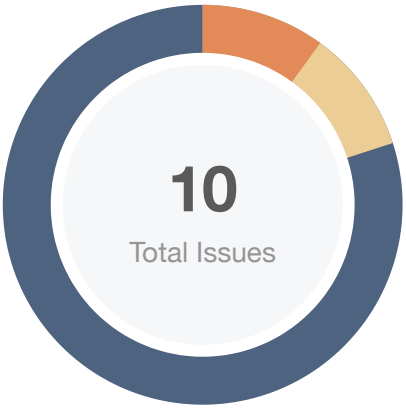
## Vulnerability Summary

| Vulnerability Level | Total | Pending | Declined | Acknowledged | Partially Resolved | Resolved |
|---|---|---|---|---|---|---|
| Critical | 0 | 0 | 0 | 0 | 0 | 0 |
| Major | 1 | 0 | 0 | 1 | 0 | 0 |
| Medium | 0 | 0 | 0 | 0 | 0 | 0 |
| Minor | 1 | 0 | 0 | 1 | 0 | 0 |
| Informational | 8 | 0 | 0 | 8 | 0 | 0 |
| Discussion | 0 | 0 | 0 | 0 | 0 | 0 |

# Audit Scope

| ID | File | SHA256 Checksum |
| --- | --- | --- |
| ERC | flats/ERC677InitializableToken.sol | ae635bcb4c42e4438fdea9e96908c26fa7ae024d387887abeeaf0994d72ad680 |
| ERM | flats/ERC677MultiBridgeToken.sol | 10a881ec3a19624d1cbe26ecb92fef8fe71987629f15526100f31a0a5d5d6042 |
| TPN | flats/TokenProxy.sol | 54fa34b2dcb5cb822ff95f1bbf0543cc63eee58dedbc5338137506493a094e9b |

# Findings




| | |
|---|---|
| **Critical** | **0** (0.00%) |
| **Major** | **1** (10.00%) |
| **Medium** | **0** (0.00%) |
| **Minor** | **1** (10.00%) |
| **Informational** | **8** (80.00%) |
| **Discussion** | **0** (0.00%) |

| ID | Title | Category | Severity | Status |
|---|---|---|---|---|
| GLOBAL-01 | Missing Error Messages | Coding Style | Informational | Acknowledged |
| **GLOBAL-02** | Centralization Related Risks | **Centralization / Privilege** | **Major** | Acknowledged |
| ERC-01 | Redundant Statements | Volatile Code | Informational | Acknowledged |
| ERC-02 | Code Optimization | Logical Issue | Informational | Acknowledged |
| ERM-01 | Missing BridgeContract Removing Function | Logical Issue | Informational | Acknowledged |
| NPC-01 | Unclear Purpose Of `fundReceiver()` | Logical Issue | Informational | Acknowledged |
| NPC-02 | Unlocked Compiler Version | Language Specific | Informational | Acknowledged |
| NPC-03 | Meaningless Function | Logical Issue | Informational | Acknowledged |
| NPC-04 | Mixed Complier Version | Compiler Error | Informational | Acknowledged |
| NPC-05 | Missing Input Validation | Volatile Code | Minor | Acknowledged |

# GLOBAL-01 | Missing Error Messages

| Category | Severity | Location | Status |
| --- | --- | --- | --- |
| Coding Style | Informational | Global | Acknowledged |

## Description

The **require** can be used to check for conditions and throw an exception if the condition is not met. It is better to provide a string message containing details about the error that will be passed back to the caller.

## Recommendation

We advise refactoring the linked codes as below:

For example:

```
function add(uint256 a, uint256 b) internal pure returns (uint256 c) {
    c = a + b;
    require(c >= a, ""SafeMath: addition overflow"");
}
```

## Alleviation

No alleviation.

# GLOBAL-02 | Centralization Related Risks

| Category | Severity | Location | Status |
| --- | --- | --- | --- |
| Centralization / Privilege | Major | Global | Acknowledged |

## Description

The role `owner` has the authority over the listed functions:

`ERC677MultiBridgeToken.sol:`

- `setFundingRules()`
- `setBridgeContract()`
- `renounceOwnership()`
- `claimTokens()`
- `transferOwnership()`
- `finishMinting()`
- `addBridgeContract()`

`ERC677InitializableToken.sol:`

- `setFundingRules()`
- `setBridgeContract()`
- `renounceOwnership()`
- `claimTokens()`
- `transferOwnership()`
- `mint()`

`TokenProxy.sol:`

- `changeAdmin()`
- `upgradeTo()`
- `upgradeToAndCall()`

Any compromise to the key role account may allow a potential hacker to take advantage of this and execute malicious acts.

## Recommendation

The risk describes the current project design and potentially makes iterations to improve in the security operation and level of decentralization, which in most cases cannot be resolved entirely at the present stage. 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 be improved via a decentralized mechanism or smart-contract-based accounts with enhanced security practices, e.g., multi-signature wallets.

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

## Short Term:

Timelock and Multi sign (⅔, ⅗) combination *mitigate* by delaying the sensitive operation and avoiding a single point of key management failure.

- Time-lock with reasonable latency, e.g., 48 hours, for awareness on privileged operations;
  AND
- Assignment of privileged roles to multi-signature wallets to prevent a single point of failure due to the private key compromised;
  AND
- A medium/blog link for sharing the timelock contract and multi-signers addresses information with the public audience.

## Long Term:

Timelock and DAO, the combination, *mitigate* by applying decentralization and transparency.

- Time-lock with reasonable latency, e.g., 48 hours, for awareness on privileged operations;
  AND
- Introduction of a DAO/governance/voting module to increase transparency and user involvement.
  AND
- A medium/blog link for sharing the timelock contract, multi-signers addresses, and DAO information with the public audience.

## Permanent:

Renouncing the ownership or removing the function can be considered *fully resolved*.

- Renounce the ownership and never claim back the privileged roles. OR
- Remove the risky functionality.

## Alleviation

No alleviation.

# ERC-01 | Redundant Statements

| Category | Severity | Location | Status |
| --- | --- | --- | --- |
| Volatile Code | Informational | flats/ERC677InitializableToken.sol: 606~609 | Acknowledged |

## Description

The linked statements do not affect the functionality of the codebase and appear to be either leftovers from test code or older functionality.

## Recommendation

We advise that they are removed to better prepare the code for production environments.

## Alleviation

No alleviation.

# ERC-02 | Code Optimization

| Category | Severity | Location | Status |
| --- | --- | --- | --- |
| Logical Issue | Informational | flats/ERC677InitializableToken.sol: 33~43, 645~648 | Acknowledged |

## Description

In the higher version Openzeppelin, the linked `initializer` modifier code is improved to be better suited to the following case:

- In the contract, the initialization function, which is modified by the liked `initializer` modifier, called its super contract initialization function also modified by the same `initializer` modifier.

## Recommendation

We advise refactoring the linked statements as below:

```
33  modifier initializer() {
34    require(initializing || isConstructor() || !initialized, "Contract instance has
already been initialized");
35
36    bool isTopLevelCall = !initializing;
37    if (isTopLevelCall) {
38      initializing = true;
39      initialized = true;
40    }
41
42    _;
43
44    if (isTopLevelCall) {
45      initializing = false;
46    }
47  }
```

## Alleviation

No alleviation.

# ERM-01 | Missing BridgeContract Removing Function

| Category | Severity | Location | Status |
| --- | --- | --- | --- |
| Logical Issue | Informational | flats/ERC677MultiBridgeToken.sol: 678~681 | Acknowledged |

## Description

The linked function only takes charge of adding bridge contract. However, in the codebase, there is no function for removing the added bridge contract. Does it meet the original design logic?

## Recommendation

Please provide us more information about the design logic.

## Alleviation

No alleviation.

## NPC-01 | Unclear Purpose Of `fundReceiver()`

| Category | Severity | Location | Status |
| --- | --- | --- | --- |
| Logical Issue | Informational | flats/ERC677InitializableToken.sol: 694~695, 667<br>flats/ERC677MultiBridgeToken.sol: 599~600, 599~600, 551 | Acknowledged |

### Description

Along with the `ERC677` token is transferred to the `_to` address, the `fundingRules.amount` of native tokens are transferred into the `_to` address. There is no fixed value rate between the transferred `ERC677` token and the transferred native token, so what's the purpose of the `fundReceiver()` function?

### Recommendation

Please provide us with more information about the design logic.

### Alleviation

The client gave the following response:

`The purpose of the` fundReceiver() `function is used for transferring a number of native tokens to the cross-bridge transfer recipient and helping the above recipient to pay the gas fee of other transactions.`

## NPC-02 | Unlocked Compiler Version

| Category | Severity | Location | Status |
| --- | --- | --- | --- |
| Language Specific | Informational | flats/ERC677InitializableToken.sol: 3<br>flats/ERC677MultiBridgeToken.sol: 3<br>flats/TokenProxy.sol: 3 | Acknowledged |

### Description

The contract has unlocked compiler version. An unlocked compiler version in the source code of the contract permits the user to compile it at or above a particular version. This, in turn, leads to differences in the generated bytecode between compilations due to differing compiler version numbers. This can lead to an ambiguity when debugging as compiler specific bugs may occur in the codebase that would be hard to identify over a span of multiple compiler versions rather than a specific one.

### Recommendation

We advise that the compiler version is instead locked at the lowest version possible that the contract can be compiled at. For example, for version `v0.6.2` the contract should contain the following line:

```
pragma solidity 0.6.2;
```

### Alleviation

No alleviation.

# NPC-03 | Meaningless Function

| Category | Severity | Location | Status |
| --- | --- | --- | --- |
| Logical Issue | Informational | flats/ERC677InitializableToken.sol: 756~762<br>flats/ERC677MultiBridgeToken.sol: 641~648 | Acknowledged |

## Description

The behavior of the linked functions is unchangeable no matter what the value of parameters.

## Recommendation

We advise removing the linked function.

## Alleviation

No alleviation.

# NPC-04 | Mixed Complier Version

| Category | Severity | Location | Status |
| --- | --- | --- | --- |
| Compiler Error | Informational | flats/ERC677InitializableToken.sol: 63, 3, 101, 170, 387, 420, 503, 547, 595, 604<br>flats/ERC677MultiBridgeToken.sol: 20, 75, 126, 160, 185, 311, 378, 440, 464, 477, 490, 499, 666<br>flats/TokenProxy.sol: 73, 186, 321, 109 | Acknowledged |

## Description

The using compiler version should satisfy each `pragma solidity VersionNum` declaration at the same time when multiple different compiler version declarations appear in a single `sol` file.

## Recommendation

We advise fixing the compiler version and removing the duplicated declarations.

## Alleviation

No alleviation.

# NPC-05 | Missing Input Validation

| Category | Severity | Location | Status |
| --- | --- | --- | --- |
| Volatile Code | Minor | flats/ERC677InitializableToken.sol: 645~648<br>flats/TokenProxy.sol: 234~238 | Acknowledged |

## Description

The given input is missing the check for the non-zero address.

## Recommendation

We advise adding the check for the passed-in values to prevent unexpected errors as below:

```
645  function initialize(string _name, string _symbol, uint8 _decimals, address _owner)
external initializer {
646      require(address(0) != _owner, "set owner to the zero address");
647      ERC20Mintable.initialize(_owner);
648      ERC20Detailed.initialize(_name, _symbol, _decimals);
649  }
```

```
234  constructor(address _implementation, address _admin, bytes _data)
UpgradeabilityProxy(_implementation, _data) public payable {
235    require(address(0) != _admin, "set admin to the zero address");
236    assert(ADMIN_SLOT == keccak256("org.zeppelinos.proxy.admin"));
237
238    _setAdmin(_admin);
239  }
```

## Alleviation

No alleviation.

# 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.

### Volatile Code

Volatile Code findings refer to segments of code that behave unexpectedly on certain edge cases that may result in a vulnerability.

### Language Specific

Language Specific findings are issues that would only arise within Solidity, i.e. incorrect usage of private or delete.

### 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.

### Compiler Error

Compiler Error findings refer to an error in the structure of the code that renders it impossible to compile using the specified version of the project.

## 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.