October 15th 2019 — Quantstamp Verified

Substratum Token

This smart contract audit was prepared by Quantstamp, the protocol for securing smart contracts.

Executive Summary

Type	Token Contract
Auditors	Martin Derka, Senior Research Engineer Kacper Bąk, Senior Research Engineer
Timeline	2018-12-14 through 2018-12-17
Languages	Solidity, Javascript
Methods Specification	None
Source Code	Repository / Commit sub-contract / 1f5d6ff

Total Issues	1	(0 Resolved)
High-Risk Issues	0	
Medium Risk Issues	0	
Low Risk Issues	0	
Informational Risk Issues	1	(0 Resolved)
Undetermined Risk Issues	0	

1 Issue

Overall Assessment

The code follows best practices and avoids the ERC20 double-spend exploit by deviating from the ERC20 specification in the implementation of the function `approve()`.

Severity Categories	
High	The issue puts a large number of users' sensitive information at risk, or is reasonably likely to lead to catastrophic impact for client's reputation or serious financial implications for client and users.
Medium	The issue puts a subset of users' sensitive information at risk, would be detrimental for the client's reputation if exploited, or is reasonably likely to lead to moderate financial impact.
Low	The risk is relatively small and could not be exploited on a recurring basis, or is a risk that the client has indicated is low impact in view of the client's business circumstances.
Informational	The issue does not post an immediate risk, but is relevant to security best practices or Defence in Depth.
Undetermined	The impact of the issue is uncertain.

Goals

- Is there any centralization of power?
- Does the code conform to ERC20?

Changelog

- 2018-12-17 - Initial report

Quantstamp Audit Breakdown

Quantstamp's objective was to evaluate the Substratum Token repository for security-related issues, code quality, and adherence to specification and best practices.

Possible issues we looked for included (but are not limited to):

- Transaction-ordering dependence
- Timestamp dependence
- Mishandled exceptions and call stack limits
- Unsafe external calls
- Integer overflow / underflow
- Number rounding errors
- Reentrancy and cross-function vulnerabilities
- Denial of service / logical oversights
- Access control
- Centralization of power
- Business logic contradicting the specification
- Code clones, functionality duplication
- Gas usage
- Arbitrary token minting

Methodology

The Quantstamp auditing process follows a routine series of steps:

1. Code review that includes the following
   i. Review of the specifications, sources, and instructions provided to Quantstamp to make sure we understand the size, scope, and functionality of the smart contract
   ii. Manual review of code, which is the process of reading source code line-by-line in an attempt to identify potential vulnerabilities.
   iii. Comparison to specification, which is the process of checking whether the code does what the specifications, sources, and instructions provided to Quantstamp describe.
2. Testing and automated analysis that includes the following:
   i. Test coverage analysis, which is the process of determining whether the test cases are actually covering the code and how much code is exercised when we run those test cases.
   ii. Symbolic execution, which 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, clarity, maintainability, security, and control based on the established industry and academic practices, recommendations, and research.
4. Specific, itemized, and actionable recommendations to help you take steps to secure your smart contracts.

Toolset

The below notes outline the setup and steps performed in the process of this audit.

Setup

Tool Setup:

- Truffle v4.1.12
- Ganache v1.1.0
- Oyente v1.2.5
- Mythril v0.2.7
- MAIAN commit sha: ab0819cf
- Security

Steps taken to run the tools:

1. Installed Truffle: `npm install -g truffle`
2. Installed Ganache: `npm install -g ganache-cli`
3. Installed the solidity-coverage tool (within the project's root directory): `npm install --save-dev solidity-coverage`
4. Run the coverage tool from the project's root directory: `./node_modules/.bin/solidity-coverage`
5. Flattened the source code using `truffle-flatener` to accommodate the auditing tools.
6. Installed the Mythril tool from Pip3: `pip3 install mythril`
7. Ran the Mythril tool on each contract: `myth -x path/to/contract`
8. Run the Security tool: `java -Xmx6048m -jar security-0.1.jar -fs contract.sol`
9. Installed the Oyente tool from Docker: `docker pull luongnguyen/oyente`
10. Migrated files into Oyente (root directory): `docker run -v $(pwd):/tmp -it luongnguyen/oyente`
11. Ran the Oyente tool on each contract: `cd /oyente/oyente && python oyente.py /tmp/path/to/contract`
12. Cloned the MAIAN tool: `git clone --depth 1 https://github.com/MAIAN-tool/MAIAN.git maian`
13. Ran the MAIAN tool on each contract: `cd maian/tool/ && python3 maian.py -s path/to/contract contract.sol`

Assessment

Findings

No full compatibility with ERC20 standard

Severity: Informational

Contract(s) affected: `Substratum.sol`

Description: As it presently is constructed, the contract avoids the ERC20 allowance double-spend exploit by redefining the behavior of `approve()`.

Recommendation: The Substratum team should inform users about non-standard behavior of `approve()`.

Test Results

Test Suite Results

```
  Contract: Substratum
    deployed contract
      ✓ has the name Substratum (67ms)
      ✓ has the symbol SUB (45ms)
      ✓ has 18 decimal precision
      ✓ starts with a total supply of 872 million
      ✓ starts with owner balance at 872 million (71ms)
      ✓ emits an event for token creation
      ✓ should reject receiving ETH in the fallback function (49ms)
    token basic
      ✓ cannot burn more than owner has (109ms)
      ✓ can burn an amount that owner has (209ms)
    contract
      ✓ allows transfers from any account (228ms)
      ✓ allows low-level transfers, even those that the balance (51ms)
      ✓ can transfer zero tokens from any account
      ✓ can transfer approved funds in chunks (317ms)
      ✓ can not transfer funds that have not been approved (53ms)
      ✓ can not do the transfer if not enough has been approved (141ms)
      ✓ can not transfer more than owner has (53ms) (1 min)
      ✓ reverts 2nd non-zero approve calls to prevent double-spend race condition (264ms)


  27 passing (7m)
```

Code Coverage

The test coverage of the contract is excellent.

```
----------------|----------|----------|----------|----------|----------------|
File            |  % Stmts | % Branch |  % Funcs | % Lines  |Uncovered Lines |
----------------|----------|----------|----------|----------|----------------|
 contracts/     |      100 |      100 |      100 |      100 |                |
  Substratum.sol|      100 |      100 |      100 |      100 |                |
----------------|----------|----------|----------|----------|----------------|
All files       |      100 |      100 |      100 |      100 |                |
----------------|----------|----------|----------|----------|----------------|
```

Automated Analyses

Oyente

Oyente reported integer overflows in functions `transfer()` and `transferFrom()`. Both are false positives, however.

Mythril

Mythril reported assertion failure and integer overflow in the function `increaseApproval()`. The former is caused by how standard arithmetic functions are implemented in `SafeMath.sol`. The latter is a false positive.

MAIAN

MAIAN did not report any issues.

Security

Security did not report any issues.

Adherence to Specification

The token contract adheres to the specification.

Code Documentation

The code is straightforward and the documentation is adequate.

Adherence to Best Practices

The code conforms to best practices.

Appendix

File Signatures

The following are the SHA-256 hashes of the audited contracts and/or test files. A smart contract or file with a different SHA-256 hash has been modified, intentionally or otherwise, after the audit. You are cautioned that a different SHA-256 hash could be (but is not necessarily) an indication of a changed condition or potential vulnerability that was not within the scope of the audit.

Contracts	Tests
`bcb2233ba758fa287315d5f85e69195834fa1e4fd723d8cdb1c5e317bdbc35b ./contracts/Migrations.sol`	`a1585d357a9b2185fccd09b71d5acc9262b3/617b6e047945f07d22b3080746 ./test/Substratum_test.js`
`09fb293f7297741521b6d20f5815f2e4ff9d3253f5a1547a8b62f8db879 ./contracts/Substratum.sol`	`6952e7aae94e5afe51394c27f98f9353a5a9e7357322cce09b24215a5f3 ./test/helpers/shared.js`
	`8b9c51a7154d8f4b35a5f351fd9a77fd8a395a6e5f5dae8b52ed5795d14ac ./test/helpers/reverted.js`

About Quantstamp

Quantstamp is a Y Combinator-backed company that helps to secure smart contracts at scale using computer-aided reasoning tools, with a mission to help boost adoption of this exponentially growing technology.

Quantstamp's team boasts decades of combined experience in formal verification, static analysis, and software verification. Collectively, our individuals have over 500 Google scholar citations and numerous published papers. In its mission to proliferate development and adoption of blockchain applications, Quantstamp is also developing a new protocol for smart contract verification to help smart contract developers and projects worldwide to perform cost-effective smart contract security audits.

To date, Quantstamp has helped to secure hundreds of millions of dollars of transaction value in smart contracts and has assisted dozens of blockchain projects globally with its white glove security auditing services. As an evangelist of the blockchain ecosystem, Quantstamp assists core infrastructure projects and leading community initiatives such as the Ethereum Community Fund to expedite the adoption of blockchain technology.

Finally, Quantstamp's dedication to research and development in the form of collaborations with leading academic institutions such as National University of Singapore and MIT (Massachusetts Institute of Technology) reflects Quantstamp's commitment to enable world-class smart contract innovation.

Timeliness of content

The content contained in the report is current as of the date appearing on the report and is subject to change without notice, unless indicated otherwise by Quantstamp; however, Quantstamp does not guarantee or warrant the accuracy, timeliness, or completeness of any report you access using the Internet or other means, and assumes no obligation to update any information following publication.

Notice of confidentiality

This report, including the content, data, and underlying methodologies, are subject to the confidentiality and feedback provisions in your agreement with Quantstamp. These materials are not to be disclosed, extracted, copied, or distributed except to the extent expressly authorized by Quantstamp.

Links to other websites

You may, through hypertext or other computer links, gain access to web sites operated by persons other than Quantstamp, Inc. (Quantstamp). Such hyperlinks are provided for your reference and convenience only, and are the exclusive responsibility of such web sites' owners. You agree that Quantstamp are not responsible for the content or operation of such web sites, and that Quantstamp shall have no liability to you or any other person or entity for the use of third-party web sites. Except as described below, a hyperlink from this web site to another web site does not imply or mean that Quantstamp endorses the content on that web site or the operator or operations of that site. You are solely responsible for determining the extent to which you may use any content at any other web sites to which you link from the report. Quantstamp assumes no responsibility for the use of third-party software on the website and shall have no liability whatsoever to any person or entity for the accuracy or completeness of any outcome generated by such software.

Disclaimer

This report is based on the scope of materials and documentation provided for a limited review at the time provided. Results may not be complete nor inclusive of all vulnerabilities. The review and this report are provided on an as-is, where-is, and as-available basis. You agree that your access and/or use, including but not limited to any associated services, products, protocols, platforms, content, and materials, will be at your sole risk. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The Solidity language itself and other smart contract languages remain under development and are subject to unknown risks and flaws. The review does not extend to the compiler layer, or any other areas beyond Solidity or the smart contract programming language, or other programming aspects that could present security risks. You may risk loss of tokens, Ether, and/or other loss. A report is not an endorsement (or other opinion) of any particular project or team, and the report does not guarantee the security of any particular project. A report does not consider, and should not be interpreted as considering or having any bearing on, the potential economics of a token, token sale or any other product, service or other asset. No third party should rely on the reports in any way, including for the purpose of making any decisions to buy or sell any token, product, service or other asset. To the fullest extent permitted by law, we disclaim all warranties, express or implied, in connection with this report, its content, and the related services and products and your use thereof, including, without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. We do not warrant, endorse, guarantee, or assume responsibility for any product or service advertised or offered by a third party through the product, any open source or third party software, code, libraries, materials, or information linked to, called by, referenced by or accessible through the report, its content, and the related services and products, any hyperlinked website, or any website or mobile application featured in any banner or other advertising, and we will not be a party to or in any way be responsible for monitoring any transaction between you and any third-party providers of products or services. As with the purchase or use of a product or service through any medium or in any environment, you should use your best judgment and exercise caution where appropriate. You may risk loss of QSP tokens or other loss. FOR AVOIDANCE OF DOUBT, THE REPORT, ITS CONTENT, ACCESS, AND/OR USAGE THEREOF, INCLUDING ANY ASSOCIATED SERVICES OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, INVESTMENT, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.