CRYPTONIUM FINTECH
Technology for Innovators.

Elite Cash (ELC)

Smart Contract Security Audit

September 11th, 2021

Disclaimer

This is a limited report on our findings based on our analysis, in accordance with good industry practice as of the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the details of which are set out in this report. In order to get a full view of our analysis, you must read the full report. While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us based on what it says or doesn't say or how we produced it. It is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER: By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis and does not constitute investment advice. No one shall have any right to rely on the report or its contents, and Cryptonium Fintech and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (Cryptonium Fintech) owe no duty of care towards you or any other person, nor does Cryptonium Fintech make any warranty or representation to any person on the accuracy or completeness of the report. The report is provided "as is," without any conditions, warranties or other terms of any kind except as set out in this disclaimer. Cryptonium Fintech hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, Cryptonium Fintech hereby excludes all liability and responsibility. Neither you nor any other person shall have any claim against Cryptonium Fintech for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of the use of this report, and any reliance on this report.

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.

Background

Cryptonium Fintech was commissioned by Token Revolution to perform an audit of smart contracts:

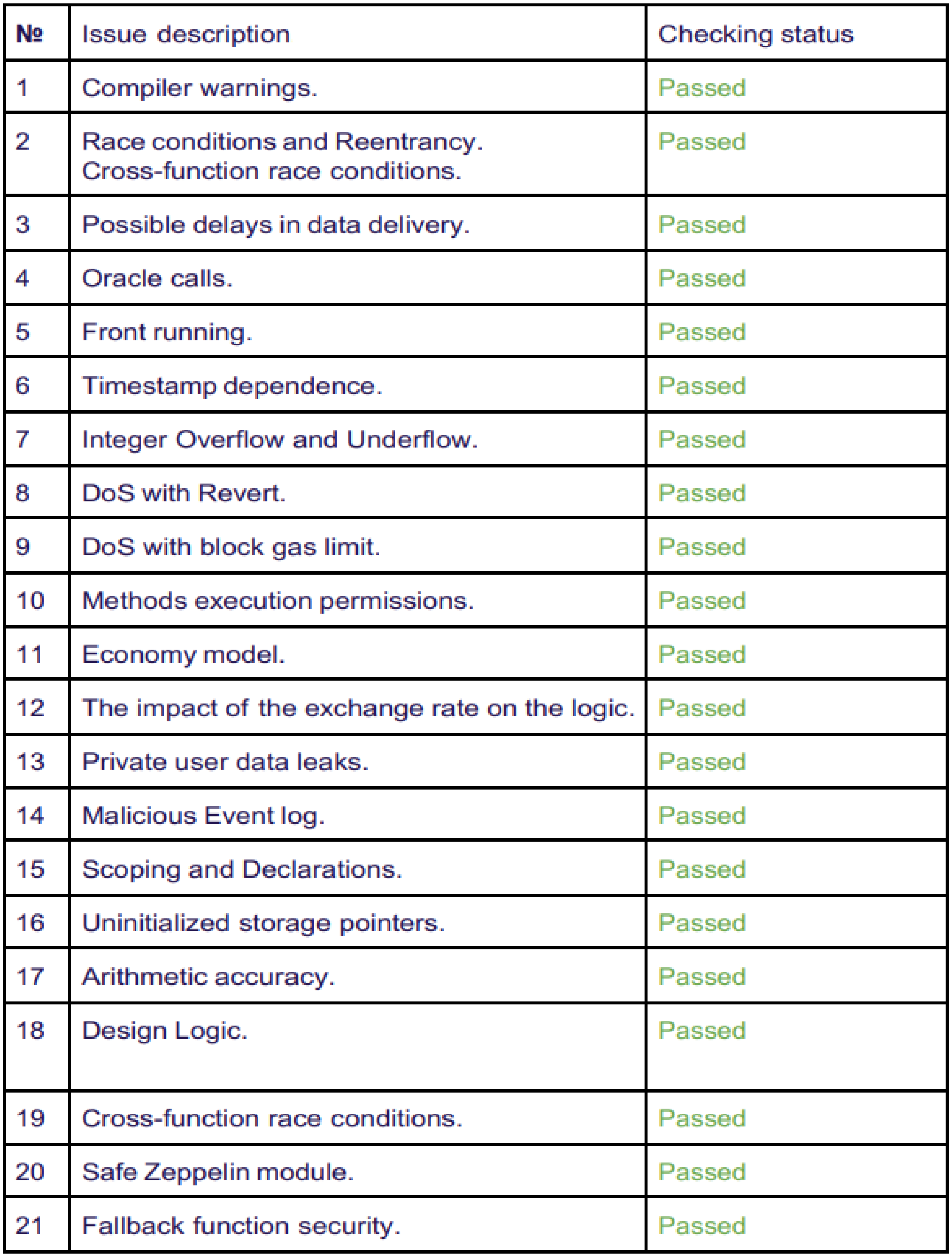
https://explorer.etherlite.org/tokens/0x65D316e69c6798463E0fae19b1dA6aa9d77d3415/token-transfers

The purpose of the audit was to achieve the following:

- Ensure that the smart contract functions as intended.
- Identify potential security issues with the smart contract.

The information in this report should be used to understand the risk exposure of the smart contract and as a guide to improving the security posture of the smart contract by remediating the issues that were identified.

Issues Checking Status



№	Issue description	Checking status
1	Compiler warnings.	Passed
2	Race conditions and Reentrancy. Cross-function race conditions.	Passed
3	Possible delays in data delivery.	Passed
4	Oracle calls.	Passed
5	Front running.	Passed
6	Timestamp dependence.	Passed
7	Integer Overflow and Underflow.	Passed
8	DoS with Revert.	Passed
9	DoS with block gas limit.	Passed
10	Methods execution permissions.	Passed
11	Economy model.	Passed
12	The impact of the exchange rate on the logic.	Passed
13	Private user data leaks.	Passed
14	Malicious Event log.	Passed
15	Scoping and Declarations.	Passed
16	Uninitialized storage pointers.	Passed
17	Arithmetic accuracy.	Passed
18	Design Logic.	Passed
19	Cross-function race conditions.	Passed
20	Safe Zeppelin module.	Passed
21	Fallback function security.	Passed

Security Issues

High Severity Issues

No high severity issues were found.

Medium Severity Issues

No medium severity issues were found.

Low Severity Issues

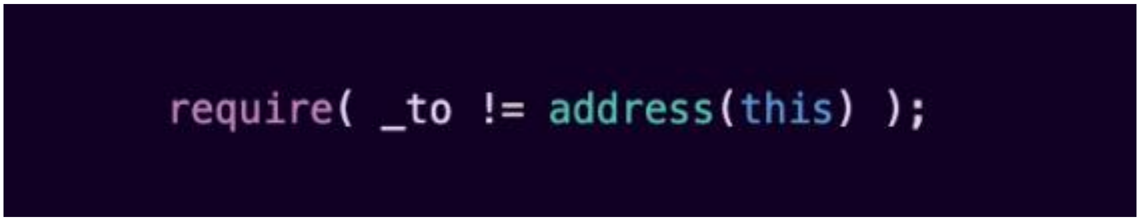
1 - Known vulnerabilities of ETL-20 token

Issue:

Lack of transaction handling mechanism issue. WARNING! This is a very common issue, and it has already caused millions of dollars losses for lots of token users.

Recommendation:

Add the following code to the **_transfer(address sender, ...)** function.



```
require( _to != address(this) );
```

Owner Privileges

The owner can mint any number of tokens without restrictions.

Conclusion

Smart contracts contain low severity issues and owner privileges.

Cryptonium Fintech note:
Please check the disclaimer above and note that the audit makes no statements or warranties on the business model, investment attractiveness, or code sustainability. The report is provided for the only contract mentioned in the report and does not include any other potential contracts deployed by the owner.