Bastion Lockdrop Security Review

This security review was prepared by Quantstamp (https://www.quantstamp.com/), the leader in blockchain security.

Executive Summary

Category	Description
Type	Lockdrop contract
Reviewer(s)	
Timeline	2022-03-09 through 2022-03-09
EVM	London
Language(s)	Solidity
Method(s)	Architecture Review, Unit Testing, Functional Testing, Computer-Aided Verification, Manual Review
Specification(s)	None
Documentation Quality	Undetermined
Test Quality	High
Source code	Repository: testnet-deploy (https://github.com/Near-Lending-Protocol/testnet-deploy/tree/lockdrop-ctokendeposit) Commit: 773f63
Total Issues	0
High Risk Issues	0
Medium Risk Issues	0
Low Risk Issues	0
Informational Risk Issues	0
Undetermined Risk Issues	0

Severity Level	Explanation
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 pose an immediate threat to continued operation or usage, but is relevant for security best practices, software engineering best practices, or defensive redundancy.
Undetermined	The impact of the issue is uncertain.

Overall Assessment

The engagement has iterated over the lockdrop contract for several times where Quantstamp have provided inputs on its design. This report only comments on the contract that was provided to Quantstamp in the last iteration. There is no issue found in the lockdrop contract on commit `773f63`.

Quantstamp Review Breakdown

Quantstamp's objective was to evaluate the 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 reviewing process follows a routine series of steps:

1. Code review that includes the following
    1. Review of the specifications, sources, and instructions provided to Quantstamp to make sure we understand the size, scope, and functionality of the smart contract.
    2. Manual review of code, which is the process of reading source code line-by-line in an attempt to identify potential vulnerabilities.
    3. 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:
    1. 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.
    2. 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, clarify, 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.

Findings

Test Results

Test Suite Results

```
 Lockdrop testing
The Hardhat Network tracing engine could not be initialized. Run Hardhat with --verb
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
BigNumber { _hex: '0x3a35294400', _isBigNumber: true }
    ✓ CToken Transfer
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
    ✓ CToken Transfer Then Attempt Borrow
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
    ✓ Lockdrop initialization claim unlock date in the past
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
    ✓ Deposit
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
```

    ✓ Deposit then claim when unlocked
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
250000000000
    ✓ Deposit twice then claim when unlocked
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
    ✓ User cannot claim twice
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
    ✓ User cannot claim before claim unlock time
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
    ✓ User with no deposit cannot claim
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
    ✓ User cannot deposit while deposits are locked
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
    ✓ Only owner can set lock
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
    ✓ Only owner can set owner
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres

```
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
    ✓ Owner cannot be set to 0
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
    ✓ Owner cannot be set to vault address
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
    ✓ Deposit Event
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
    ✓ Claim Event
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
Duplicate definition of ActionPaused (ActionPaused(string,bool), ActionPaused(addres
    ✓ Deposit Nothing Fails
```

Code Coverage

```
----------------------------------|----------|----------|----------|----------|-----
File                              |  % Stmts | % Branch |  % Funcs |  % Lines |Uncov
----------------------------------|----------|----------|----------|----------|-----
  LockdropVaultV2.sol             |      100 |       90 |      100 |      100 |
----------------------------------|----------|----------|----------|----------|-----
```

Changelog

- 2022-03-18 - Final report

Appendix

About Quantstamp

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

With over 1000 Google scholar citations and numerous published papers, Quantstamp's team has decades of combined experience in formal verification, static analysis, and software verification. Quantstamp has also developed a protocol to help smart contract developers and projects worldwide to perform cost-effective smart contract security scans.

To date, Quantstamp has protected $5B in digital asset risk from hackers and assisted dozens of blockchain projects globally through its white glove security assessment 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.

Quantstamp's collaborations with leading academic institutions such as the National University of Singapore and MIT (Massachusetts Institute of Technology) reflect our commitment to research, development, and enabling world-class blockchain security.

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.
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 arenot 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.

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. Blockchain technology remains under development and is subject to unknown risks and flaws. The review does not extend to the compiler layer, or any other areas beyond the programming language, or other programming aspects that could present security risks. A report does not indicate the endorsement of any particular project or team, nor guarantee its security. No third party should rely on the reports in any way, including for the purpose of making any decisions to buy or sell a product, service or any other asset. To the fullest extent permitted by law, we disclaim all warranties, expressed 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 websites, any websites or mobile applications appearing on any 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. 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.