☰ **Omniscia Bonq Audit**

Borrowing Protocol Security Audit

Audit Overview

We were tasked with performing an audit of the Bonq codebase and in particular their borrowing protocol based on the Liquity stablecoin system with support for multiple tokens instead of the single native one.

Over the course of the audit, we identified multiple vulnerabilities as well as core design flaws that may significantly impact the project's expected development timeline. The most crucial issue being the reliance on TWAP implementations that will become insecure following the upcoming PoS hard fork.

Additionally, the system appears to rely on an old version of the Liquity codebase that contains a convoluted code structure as well as lightly defined mathematical models. We advise the Bonq team to evaluate these formulas and define their own white-paper the codebase is based on so that we can properly validate the final codebase output.

We advise the Bonq team to closely evaluate all minor-and-above findings identified in the report and promptly remediate them as well as consider all optimizational exhibits identified in the report. Ultimately, we believe a pivot of some of the project's core components is required at this stage (reliance on decentralized oracles instead of TWAPs as an example).

Post-Audit Conclusion

The Bonq protocol team opted to remove the oracle implementations from the final state of the codebase after consuming the outputs of our audit report and proceeded to alleviate all exhibits identified within it that remained relevant to the codebase.

With regards to the centralization concerns, the Bonq protocol team has shared their decentralization strategy which can be found on each centralization-related exhibit that is addressed as alleviated.

Overall, all exhibits identified in the report have been adequately dealt with and those that had no action taken do not pose an active threat to the protocol.

Contracts Assessed

| Files in Scope	Repository	Commit(s)
BONQMath.sol (BON)	borrowing-protocol	7dc2b0a8e7, 58487cd1b0
BONQ-staking.sol (BOQ)	borrowing-protocol	7dc2b0a8e7, 58487cd1b0
arbitrage-pool.sol (ARB)	borrowing-protocol	7dc2b0a8e7, 58487cd1b0
constants.sol (CON)	borrowing-protocol	7dc2b0a8e7, 58487cd1b0
community-liquidation-pool.sol (COM)	borrowing-protocol	7dc2b0a8e7, 58487cd1b0
external-price-feed.sol (EXT)	borrowing-protocol	7dc2b0a8e7, 58487cd1b0
fixed-supply-token.sol (FIX)	borrowing-protocol	7dc2b0a8e7, 58487cd1b0
linked-address-list.sol (LIN)	borrowing-protocol	7dc2b0a8e7, 58487cd1b0
mintable-token.sol (MIN)	borrowing-protocol	7dc2b0a8e7, 58487cd1b0
mintable-token-owner.sol (MIT)	borrowing-protocol	7dc2b0a8e7, 58487cd1b0
price-feed.sol (PRI)	borrowing-protocol	7dc2b0a8e7, 58487cd1b0
stability-pool.sol (STA)	borrowing-protocol	7dc2b0a8e7, 58487cd1b0
trove.sol (TRO)	borrowing-protocol	7dc2b0a8e7, 58487cd1b0

Files in Scope	Repository	Commit(s)
trove-creator.sol (TRV)	**borrowing-protocol**	**7dc2b0a8e7**, **58487cd1b0**
trove-factory.sol (TRE)	**borrowing-protocol**	**7dc2b0a8e7**, **58487cd1b0**
token-to-price-feed.sol (TOK)	**borrowing-protocol**	**7dc2b0a8e7**, **58487cd1b0**

Audit Synopsis

Severity	Identified	Alleviated	Partially Alleviated	Acknowledged
⬤ Unknown	10	8	2	0
⬤ Informational	22	14	2	6
⬤ Minor	6	6	0	0
⬤ Medium	9	6	3	0
⬤ Major	8	8	0	0

During the audit, we filtered and validated a total of **13 findings utilizing static analysis** tools as well as identified a total of **42 findings during the manual review** of the codebase. We strongly recommend that any minor severity or higher findings are dealt with promptly prior to the project's launch as they introduce potential misbehaviours of the system as well as exploits.

pie title Total Issues "Unknown" : 10 "Informational" : 22 "Minor" : 6 "Medium" : 9 "Major" : 8
The list below covers each segment of the audit in depth and links to the respective chapter of the report:

- **Compilation**
- **Static Analysis**
- **Manual Review**
- **Code Style**

NEXT
Compilation