Bridgeworld Harvesters contract review #69

Open **fulldecent** opened this issue on Jul 11, 2022 · 2 comments

fulldecent commented on Jul 11, 2022 Contributor

Bridgeworld Harvesters contract review

Bridgeworld Harvesters contract review
William Entriken
Delivered 2022-07-10

Thank you for the opportunity to participate in this review!

Review scope

This is a review of Bridgeworld Harvesters, pre-release version. Code was published at `c0840a4` with SHA-1 hash `c0840a42dc2c68111ed47f79b8da3f7ce153d6cf`. Only code in the "harvesters" folder are included in this review, but findings may be included on other topics it they may be helpful.

The scope of review included code-level review (human reading source code), automated code review, (computer reading source code) and unit testing (computer running small-scope tests). Due to limitations of the engagement, the review does not include functional testing (human using compiled program).

The review was performed for the purpose of comparing Bridgeworld Harvesters against the provided "Bridgeworld Harvesters" documentation (accessed 2022-07-08 saved as PDF with SHA-256 hash `5e4a1ce1274154d1d6bdd31aabee215a66c0dcf27375ca4bc71f4c8db6c8101f`), the plain English meaning of comments and function names, and a general understanding of NFT games. Any deviation from this standard, or deficiency against relevant best programming practices would be an in-scope review finding.

Sensitivity was set as "anything we should fix or wouldn't want a million people to read".

Review exclusions

Open Zeppelin Contacts were specifically excluded from the scope. Although certain notes about the contracts used are provided below.

MasterOfCoin.sol is explicitly excluded from this review. It appears that TreasuryMine and TreasuryStake are not related to the other files in the project. They are not mentioned in the documentation and they are not connected in any other way to Harvesters and are also excluded.

Quality and correctness of automated testing approaches and deployment strategy is excluded from the scope.

This review does not consider the applicability of this project to any specific jurisdiction's laws or regulations. Although certain of these concepts are discussed below where there is a risk of customer confusion or harm.

Findings

Each finding is listed and is organized by topic. Critical findings that are not resolved are marked with the bomb symbol (💣) and other unresolved material findings are marked with the warning symbol (⚠️). Resolved and less-than-material findings have no emoji marking.

Word choice

Unnecessary use of regulated finance words #30

Typos #31

Unnecessary use of gendered word for primary controller #32

"Boost" word is used inconsistently #33

Legion "class" and "rarity" are used without consistent meaning #34

_vestedPrincipal function has unexpected functionality #35

getHarvesterEmissionsShare function does not return emissions share #36

Function isMaxUserGlobalDeposit does not calculate if it is the max #37

Dependencies

⚠️ Solidity version is unsupported #38

⚠️ OpenZeppelin Contracts version is unsupported #39

Code sniffs and general best practices

⚠️ NatSpec documentation is missing #40

Revert strings are disguised as revert errors #41

HarvestFactory grants all permissions to a single account #42

Inconsistent use of option `override` keyword for implementation of interface #43

Design specifications

Conflicting requirements on MAGIC staking utilization multiplier #44

Corruption modifier specification is not specific enough #45

Legion boost average rank is vulnerable to griefing attack #46

Conflicting requirements on timelock periodicity #47

Major administrative functions with dire consequences are not listed as "emergency" functions #48

Design does not differentiate between fixed and configurable parameters #49

Legions boost is missing boost factor #50

Design does not specify what happens to disabled harvesters' emissions share #51

Specification violations

💣 Legion ranks matrix incorrect #52

💣 Legion weights matrix incorrect #53

💣 Treasure boosts incorrect #54

💣 Player stakes cannot be removed if harvester disabled #55

💣 Extractor boosts are not effective for their full lifetime #56

Player can use disallowed locking periods #57

AtlasMine does not implement interface detection for super classes #58

Rewards duration restriction is not checked #59

Implementation issues

💣 The liquidity pool can leak liquidity leading to a run on the bank #60

💣 1/1 legions can get stuck after setInitialMetadataForLegion #61

💣 Any NFT can get stuck after _setNftConfig #62

💣 A configuration error may allow anybody to burn other's NFTs #63

Divide-by-zero if admin performs multiple operations at once #64

`canStake` and `canUnstake` functions are more dangerous than their names imply #65

getRatePerSecond produces incorrect result on start of stream #66

Testing

Several test cases are not implemented #67

Please create test case for Harvester.withdrawPosition with unstaking NFTs in the same transaction #68

☺ 🚀 1

fulldecent commented on Jul 11, 2022 Contributor Author

When doing audits I go into "hate everything and find what could go wrong" mode. That's all you're reading in these issues.

But stepping out of that I just want to say this is a nice game design, with care chosen on the setup (21 kg... which isn't a clean divisor of 200 kg... love it!). And I can see a truckload of work went into this, and I can appreciate the compromises that were implemented to make these things work... like using proxies, beacons, configurable options in a lot of places.

As always I appreciate that the Treasure team doesn't commit publicly on ridiculous time lines and really puts a lot of heart into these releases, so keep it up!

I'd love to see this gameplay on a livestream or video sharing websites—will really help fill in the picture for me.

☺ 🚀 1

ghoul-sol commented on Aug 8, 2022 Owner

Thank you for all the issues you reported. It's your 2nd audit I'm working on and I really enjoy your feedback. I can say that it's much more on point and calibrated to be practical than some of the biggest auditors I worked with in another metaverse :)

We will fix a lot of stuff, some will be mitigated and some will be ignored as we have limited resources, unfortunately.

☺ 👍 1

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants