Smart Contract Audit

Kleros Liquid

By,
Shebin John

3rd May 2020

Index

Note: Some threat levels or headings might be empty if there is no vulnerability/updates/suggestions found.

Introduction

The contract audited here is/are:
https://github.com/kleros/kleros/blob/c639bf9/contracts/kleros/KlerosLiquid.sol
Related Contracts:
https://github.com/kleros/kleros-interaction/blob/96dba0f/contracts/standard/rng/BlockhashRNG.sol
and was shared by Kleros for auditing purposes while working with them.

Based on the audit, we were able to find no High threats, 1 Medium threat, and no Low threat with some other changes in the optimization, readability, typos, and comments section.

High Threats

1. None

Medium Threats

1. An attacker can change values older than 256 blocks based on pre-determined values from the last 256 blocks using `saveRN` function.
   Attack Workflow [Fixed]: Calls saveRN function (as it is a public one, might have avoided this attack if it was internal). As `blockhash(_block)` will give 0x0, it will call the `getFallbackRN` function, which is implemented in BlockhashRNGFallback.sol, from which if he calculated in advance, can change the number to whichever one, based on any one of the last 256 block values.

Low Threats

1. None

Optimization & Readability

1. To increase readability, the condition in `if` can be changed in Line 857, 866, etc. Like for Line 857, instead of writing it like `!(_subcourtID < courts.length)` we can write it like `_subcourtID >= courts.length`. Similarly for Line 861, instead of writing it like '!(_stake == 0 || courts[_subcourtID].minStake <= _stake)' we can write it as '_stake != 0 || _stake < courts[_subcourtID].minStake'.
2. Using brackets in the logical expression to avoid confusion is recommended in Line 658.

Typo's & Comments

1. Line 39, a better description would be "Where parties can cast votes (for public votes) or reveal them (for private ones)."
2. Line 40, a better description would be "Where the current ruling can be appealed.". The dispute is not being appealed, rather the ruling of the dispute is.

Suggestions

1. None