

Smart Contract Audit

Kleros Escrow

By,

Shebin John

10th June 2020

Index

1. [Introduction](#)
2. [High Threats](#)
3. [Medium Threats](#)
4. [Low Threats](#)
5. [Optimization & Readability](#)
6. [Typo's & Comments](#)
7. [Suggestions](#)

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-interaction/blob/master/contracts/standard/arbitration/MultipleArbitrableTransaction.sol>

<https://github.com/kleros/kleros-interaction/blob/master/contracts/standard/arbitration/MultipleArbitrableTokenTransaction.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, no 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. None

Low Threats

1. None



Optimization & Readability

1. Adding another function, which can only be called by the receiver to increase the `timeoutPayment` can help in a certain situation, where the receiver might need some more time to complete what he promised. This can avoid a situation to create a dispute by the sender or even cancel the complete transaction altogether by the sender and create a new one. It might be bad for Kleros in short term, as might lose out on one case, but it would be better for the UX of the users, and in the future, we might get more transactions from these, and potentially more cases.

Without this function, if a situation like this happens, two things can happen, which can result in one party at risk:

- A. The Sender says he will cancel the current transaction, and asks the receiver to not dispute it. Here the receiver is at risk, as the Sender might now use a new (less) value for the work he has done (than before), and he might not be able to do anything about it. He could also not walk away considering the time he has invested in completing this project.
- B. The receiver says to trust him and says he will complete the work in +X days, but after the `timeoutPayment` completes, he swiftly takes the money using the Smart Contract and scams.

Typo's & Comments

1. None

Suggestions

1. None

