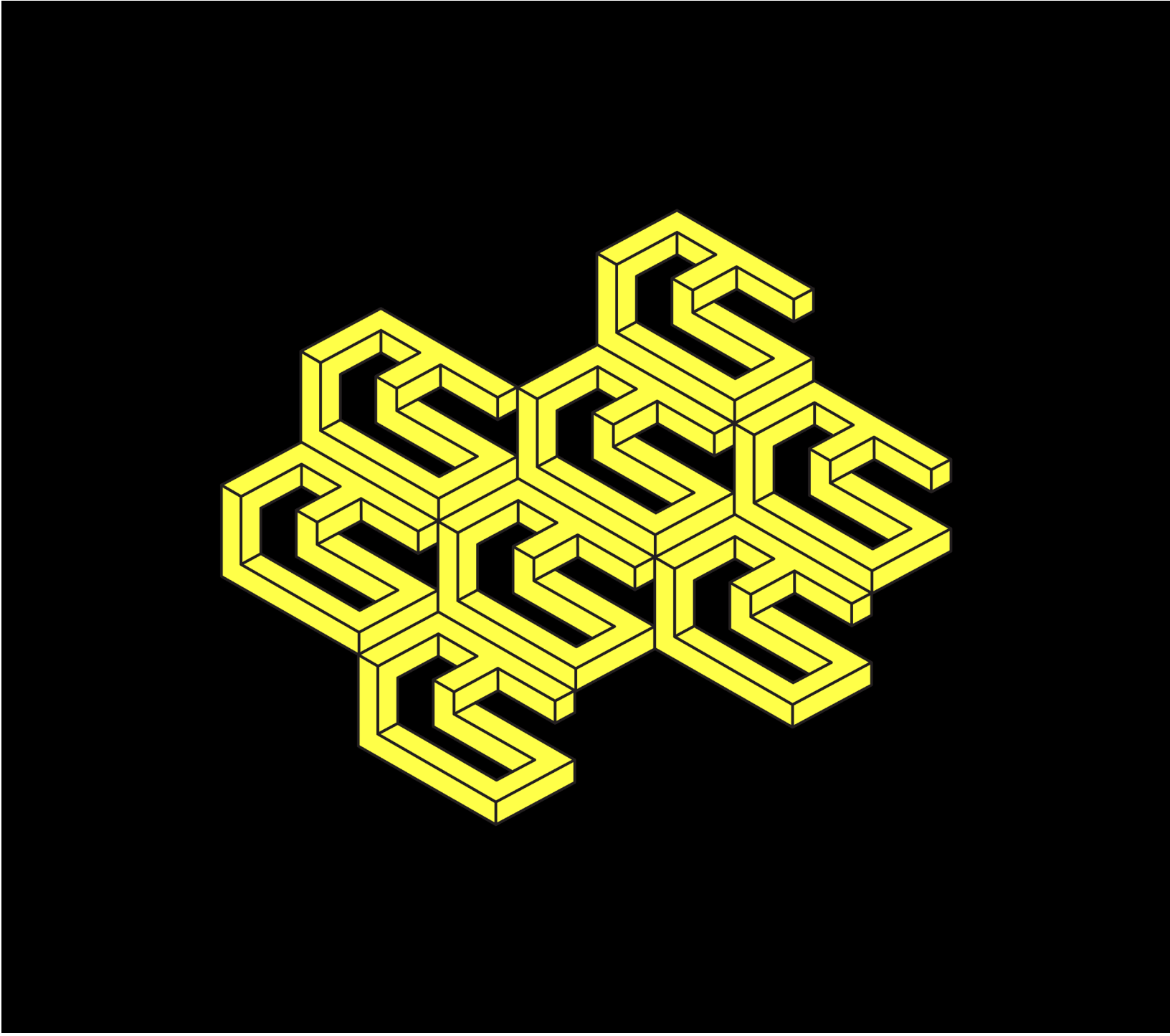

The Graph Vector Withdraw Helper Review

By ChainSafe Systems

April 2021

ChainSafe

The Graph Vector Withdraw Helper Review

Auditors: Tanya Bushenyova, Oleksii Matiiasevych

Warranty

Executive Summary

All the initially identified issues were promptly fixed and are not present in the final version of the contract. There are no known compiler bugs, for the specified compiler version (0.7.3), that might affect the contracts’ logic. During this review we collaborated with both The Graph and Connext Vector team, which proved to be very effective.

1. Introduction

The Graph requested ChainSafe Systems to perform a review of the **GRTWithdrawHelper** smart contract. The contract in question can be identified by the following git commit hash:

`41ceb7978f4660e5b569b1dd6a7338d2082129f6`

There is 1 contract in scope.

After the initial review, The Graph team applied a number of updates which can be identified by the following git commit hash:

`7170fc04a210c9158712edd81b797702f82fcff6`

Additional verification was performed after that.

2. Disclaimer

The review makes no statements or warranties about utility of the code, safety of the code, suitability of the business model, regulatory regime for the business model, or any other statements about fitness of the contracts for any specific purpose, or their bug free status.

Since this is a partial review, our report does not guarantee a lack of vulnerabilities in the remainder of The Graph codebase.

3. Executive Summary

All the initially identified issues were promptly fixed and are not present in the final version of the contract. There are **no** known compiler bugs, for the specified compiler version (0.7.3), that might affect the contracts' logic. During this review we collaborated with both The Graph and Connext Vector team, which proved to be very effective.

GRTWithdrawHelper is designed to withdraw funds from the Vector Channel and transfer them to the Staking contract in a single transaction. This review is made on an **assumption** that Vector Channel platform and Staking contract are secure and safe to use. If that assumption is wrong, then withdrawal could be impossible or the funds transferred to the Staking contract could be lost.

In the initial version, we identified 1 critical and 1 informational/optimizational issue. Those findings are described below for historical purposes:

A. The **critical issue** that was found during the review could lead to losing funds by some users and gaining of these funds by other users. The flow of the withdrawal was as follows: funds were

withdrawn from the Vector Channel, transferred to the receiver (GRTWithdrawHelper contract), and the `execute` function of the GRTWithdrawHelper contract was called afterwards. In this function, the withdrawn tokens were transferred to the Staking contract by calling the `collect()` function of the Staking contract.

If the call to the Staking contract failed, the funds were transferred back to the Vector Channel. In this case, the tokens would end up on the address of the Vector Channel. The future of these tokens would depend on the role of the initiator of the withdrawal in the Vector Channel. In the best case scenario, the tokens would be added to the balance of the initiator of the withdrawal. In the worst case scenario, the tokens would be added to the balance of the opposite user. To eliminate this possibility, we suggested transferring the tokens to some fallback address instead of returning them to the Vector Channel in case of failed transfer. Reverting the transaction would lead to funds being technically lost and as such was not recommended by the Vector team.

B. The **optimizational issue** was related to the storage variable `tokenAddress` that was set in the constructor and never changed afterwards and could be made immutable to save gas when reading it.

After the initial review, The Graph team updated the contract and all discovered issues were fixed. No new issues were discovered.

4. Critical Bugs and Vulnerabilities

One critical issue was identified during the initial review. It could've led to losing funds by some users that attempt a withdrawal. It was addressed by The Graph team and was not present in the final version of the contract.

Tanya Bushenyova Oleksii Matiiasevych