MixBytes()

THE PAY CASH

LOCKDROP & TOKEN

AUDIT REPORT

APRIL 21
2020

FOREWORD
TO REPORT

A small bug can cost you millions. **MixBytes** is a team of experienced blockchain engineers that reviews your codebase and helps you avoid potential heavy losses. More than 10 years of expertise in information security and high-load services and 18 000+ lines of audited code speak for themselves. This document outlines our methodology, scope of work, and results. We would like to thank **The Pay Cash** for their trust and opportunity to audit their smart contracts.

CONTENT
DISCLAIMER

This report is public upon the consent of **The Pay Cash**. **MixBytes** is not to be held responsible for any damage arising from or connected with the report. Smart contract security audit does not guarantee an inclusive analysis disclosing all possible errors and vulnerabilities but covers the majority of issues that represent threat to smart contract operation, have been overlooked or should be fixed.

TABLE OF CONTENTS

01 INTRODUCTION TO THE AUDIT

GENERAL PROVISIONS

The Pay Cash is a network built for free and fast stablecoin payments. It also provides a Layer 2 solution for blockchain scalability issues.

With this in mind, **MixBytes** team was willing to contribute to **The Pay Cash** project development by providing security assessment of its smart contracts.

SCOPE OF THE AUDIT

Smart contracts located in the following **repository** were reviewed

02 | SECURITY ASSESSMENT PRINCIPLES

CLASSIFICATION OF ISSUES

CRITICAL

Bugs leading to Ether or token theft, fund access locking or any other loss of Ether/tokens to be transferred to any party (for example, dividends).

MAJOR

Bugs that can trigger a contract failure. Further recovery is possible only by manual modification of the contract state or replacement.

WARNINGS

Bugs that can break the intended contract logic or expose it to DoS attacks.

COMMENTS

Other issues and recommendations reported to/acknowledged by the team.

SECURITY ASSESSMENT METHODOLOGY

Three auditors independently verified the code.

Stages of the audit were as follows:

1. Kick-off call with the client's team
2. Getting access to the source code
3. Performing an audit
4. Providing a detailed intermediary audit report
5. Eliminating identified vulnerabilities and flaws (client's team)
6. Reviewing the fixes
7. Final report
8. Issuing an official security certificate and making a record in the MixBytes Ethereum Audit Ledger (optional)
9. Publishing an audit report in the official MixBytes blog (optional)

03 DETECTED ISSUES

CRITICAL

Not found.

MAJOR

Not found.

WARNINGS

1. LockDrop.sol:85

For accuracy, multiplication should be performed prior to division.

Status:

FIXED at d699af2

2. COLToken.sol:33

We suggest that the `beginLockDrop` method be called only once.

Status:

FIXED at 7bca12e

COMMENTS

1. LockDrop.sol:71

When using the `claimETH` function, a claimer will receive tokens neither during the function call nor after `dropStartTimeStamp`.

Make sure this is a desired behaviour.

Status:

ACKNOWLEDGED

2. LockDrop.sol:89

We recommend processing the result of the `transfer` function.

Status:

FIXED at **379e4bd**

04 CONCLUSION AND RESULTS

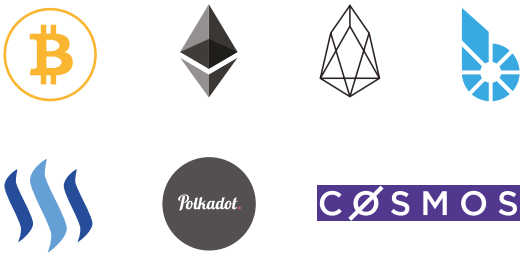
According to our analysis, the **fixed contracts** don't have any vulnerabilities.

ABOUT MIXBYTES

MixBytes is a team of blockchain developers, auditors and analysts keen on decentralized systems. We build open-source solutions, smart contracts and blockchain protocols, perform security audits, work on benchmarking and software testing solutions, consult universities and enterprises, do research, publish articles and documentation.

Stack

Blockchains



JOIN US