#HashEx
BLOCKCHAIN SECURITY

Hashflow Token

smart contracts final audit report

November 2022

hashex.org

contact@hashex.org

Contents

1. Disclaimer

This is a limited report on our findings based on our analysis, in accordance with good industry practice at the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report. While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis and does not constitute investment advice. No one shall have any right to rely on the report or its contents, and HashEx and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers, and other representatives) (HashEx) owe no duty of care towards you or any other person, nor does HashEx make any warranty or representation to any person on the accuracy or completeness of the report. The report is provided "as is", without any conditions, warranties, or other terms of any kind except as set out in this disclaimer, and HashEx hereby excludes all representations, warranties, conditions, and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, HashEx hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against HashEx, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of the use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed. HashEx owns all copyright rights to the text, images, photographs, and other content provided in the following document. When using or sharing partly or in full, third parties must provide a direct link to the original document mentioning the author (hashex.org).

2. Overview

HashEx was commissioned by the Hashflow team to perform an audit of their smart contract. The audit was conducted between 08/11/2022 and 10/11/2022.

The purpose of this audit was to achieve the following:

- Identify potential security issues with smart contracts
- Formally check the logic behind given smart contracts.

Information in this report should be used for understanding the risk exposure of smart contracts, and as a guide to improving the security posture of smart contracts by remediating the issues that were identified.

The code is available at 0xb3999F658C0391d94A37f7FF328F3feC942BcADC in Ethereum mainnet and at 0x44Ec807ce2F4a6F2737A92e985f318d035883e47 in the mainnet of Binance Smart Chain (BSC).

2.1 Summary

Project name	Hashflow Token
URL	https://hashflow.com
Platform	Ethereum, Binance Smart Chain
Language	Solidity

2.2 Contracts

Name	Address
HFT	0xb3999F658C0391d94A37f7FF328F3feC942BcADC

3. Found issues

Low	1 (25%)
Info	3 (75%)

C1. HFT

ID	Severity	Title	Status
C1-01	Low	Gas optimization	Acknowledged
C1-02	Info	Typos	Acknowledged
C1-03	Info	Contract lifetime	Acknowledged
C1-04	Info	Mint with restrictions	Acknowledged

4. Contracts

C1. HFT

Overview

An ERC-20 standard implementation. The token extends the standard by supporting the voting and votes delegation as well as EIP-2612 Permit extension. The voting model is forked from the known and well-audited COMP token developed by Compound Finance.

Issues

C1-01 Gas optimization

Low Acknowledged

To optimize the storage layout `miner` and `mintCap` state variables should be declared one after another to pack them in one slot and to save gas.

C1-02 Typos

Info Acknowledged

The version deployed to the Ethereum network contains a typo in the SafeMath library NatSpec description of the `trySub()` function. Spelling error in 'substraction'.

C1-03 Contract lifetime

Info Acknowledged

The token's lifetime is limited by the `uint32` variable for storing the `block.number`. With the current rate of BSC of 2-3 seconds per block, 2^32 ~= 4.3B will be overflowed in approximately 400 years. The rate of the Ethereum network is approximately 4-5 times slower.

The total supply is stored into `uint96` variable, meaning it's possible to fully mint 2^96 ~= 79B tokens in 7 minting events, 6 of which doubles the supply (started from 1B of initial total supply upon the contract deployment) leading to 64B tokens and 1 mint with the reduced cap to reach 79B. The soonest possible time the total supply reaches `type(uint96).max` blocking

new tokens issuing is `10 * 365 days` after the launch.

C1-04 Mint with restrictions

● Info ✓ Acknowledged

The token has open mint with the following restrictions.

1. The first mint after deploying is available in no sooner than 4 years, i.e., Sun Apr 12, 2026, in Ethereum and Sat Oct 24, 2026, in BSC, all further mints require a 365-day cooldown.
2. New tokens issuing is also limited in maximum token supply increase: it can't increase more than two times, i.e., a maximum number of tokens that can be issued during one mint procedure is close to the total supply at the moment of mint.
3. Calling the mint function is allowed only for a single privileged address with the `minter` role. Both Ethereum and BSC token contracts have their minters set to the Gnosis MultiSig contracts with a 3-out-of-6 threshold at the moment of issuance of this report.

We urge users to monitor total supply bounces by the end of the mint lock period. We also advise transferring `minter` to Timelock contract with a minimum delay of at least 24 hours and `MultiSig` as admin or transfer governance rights to DAO. This will provide users with forehanded information about upcoming mint or make this decision community-based.

5. Conclusion

1 low severity issue was found during the audit.

The contracts are highly dependent on the accounts participating in the MultiSig contract that owns the HFT token. Users using the project have to trust the project team, owner and that the owner's accounts are properly secured, and that the third-party applications work properly.

This audit includes recommendations on improving the code and preventing potential attacks.

Appendix A. Issues' severity classification

- **Critical.** Issues that may cause an unlimited loss of funds or entirely break the contract workflow. Malicious code (including malicious modification of libraries) is also treated as a critical severity issue. These issues must be fixed before deployments or fixed in already running projects as soon as possible.
- **High.** Issues that may lead to a limited loss of funds, break interaction with users, or other contracts under specific conditions. Also, issues in a smart contract, that allow a privileged account the ability to steal or block other users' funds.
- **Medium.** Issues that do not lead to a loss of funds directly, but break the contract logic. May lead to failures in contracts operation.
- **Low.** Issues that are of a non-optimal code character, for instance, gas optimization tips, unused variables, errors in messages.
- **Informational.** Issues that do not impact the contract operation. Usually, informational severity issues are related to code best practices, e.g. style guide.

Appendix B. List of examined issue types

- Business logic overview
- Functionality checks
- Following best practices
- Access control and authorization
- Reentrancy attacks
- Front-run attacks
- DoS with (unexpected) revert
- DoS with block gas limit
- Transaction-ordering dependence
- ERC/BEP and other standards violation
- Unchecked math
- Implicit visibility levels
- Excessive gas usage
- Timestamp dependence
- Forcibly sending ether to a contract
- Weak sources of randomness
- Shadowing state variables
- Usage of deprecated code

 contact@hashex.org

 @hashex_manager

 blog.hashex.org

 linkedin

 github

 twitter

#HashEx
BLOCKCHAIN SECURITY