


# SECURITY AUDIT REPORT

## Hatom ush-minter smart contract

by  **ARDA**  
on January 3, 2025



## **Table of Content**

<b>Disclaimer</b>	<b>3</b>
<b>Terminology</b>	<b>3</b>
<b>Audit Summary</b>	<b>4</b>
<b>Inherent Risks</b>	<b>5</b>
<b>Code Issues &amp; Recommendations</b>	<b>6</b>
<b>Test Issues &amp; Recommendations</b>	<b>7</b>

# Disclaimer

The report makes no statements or warranties, either expressed or implied, regarding the security of the code, the information herein or its usage. It also cannot be considered as a sufficient assessment regarding the utility, safety and bugfree status of the code, or any other statements.

This report does not constitute legal or investment advice. It is for informational purposes only and is provided on an "as-is" basis. You acknowledge that any use of this report and the information contained herein is at your own risk. The authors of this report shall not be liable to you or any third parties for any acts or omissions undertaken by you or any third parties based on the information contained herein.

# Terminology

**Inherent risk:** A risk for users that comes from a behavior inherent to the smart contract design.

Inherent risks only represent the risks inherent to the smart contract design, which are a subset of all the possible risks. **No inherent risk doesn't mean no risk.** It only means that no risk inherent to the smart contract design has been identified. Other kind of risks could still be present. For example, the issues not fixed incur risks for the users, or the smart contracts deployed as upgradeable also incur risks for the users.

**Issue:** A behavior unexpected by the users or by the project, or a practice that increases the chances of unexpected behaviors to appear.

**Critical issue:** An issue intolerable for the users or the project, that must be addressed.

**Major issue:** An issue undesirable for the users or the project, that we strongly recommend to address.

**Medium issue:** An issue uncomfortable for the users or the project, that we recommend to address.

**Minor issue:** An issue imperceptible for the users or the project, that we advise to address for the overall project security.

# Audit Summary

## Scope of initial audit

- **Repository:** <https://github.com/HatomProtocol/hatom-ush-minter>
- **Commit:** e49256c9acc72236f4beb34fde6c258fd1acc0c9
- **Path to Smart contract:** ./ush-minter/

## Scope of final audit

- **Repository:** <https://github.com/HatomProtocol/hatom-ush-minter>
- **Commit:** 8d32b272639261f7bf035d4e4a60fd50027ae998
- **Path to Smart contract:** ./ush-minter/

## Report objectives

1. Reporting all **inherent risks** of the smart contract.
2. Reporting all **issues** in the smart contract **code**.
3. Reporting all **issues** in the smart contract **test**.
4. Reporting all **issues** in the **other** parts of the smart contract.
5. Proposing **recommendations** to address all issues reported.

## 1 inherent risk in the final commit

## 0 issue in the final commit

3 issues reported from the initial commit and 0 remaining in the final commit:

Severity	Reported			Remaining		
	Code	Test	Other	Code	Test	Other
Critical	0	0	0	0	0	0
Major	0	0	0	0	0	0
Medium	0	1	0	0	0	0
Minor	2	0	0	0	0	0

# Inherent Risks

## **R1: 1 USH might not be backed by assets with value superior to 1 dollar.**

This is because the USH Minter whitelists "facilitators" which are allowed to mint USH through the Minter, but the Minter can't control that these facilitators always back the minted USH by enough assets.

Note however that the Hatom facilitators at the time this audit was made, namely the USH money market and USH isolated lending modules, implement several mechanisms to increase the chances that 1 USH is always backed by assets with value superior to 1 dollar:

- For each USH borrowed, there is more than 1\$ of collateral locked in the money market,
- The amount of USH that a facilitator can request to mint can be capped, reducing the negative impact a flawed facilitator could have if it requested to mint USH tokens that are not properly backed,
- If on the open market 1 USH can't be redeemed for 1\$ of assets, then the interest rate of the USH money market can be increased to incentivize borrowers repaying their debt, which could increase the buy pressure on USH.
- If on the open market 1 USH can't be redeemed for 1\$ of assets, then it may be possible to perform arbitrages by liquidating USH borrowers in the isolated lending modules, which could increase the buy pressure on USH.

# Code Issues & Recommendations

Since the smart contract code is not open-source, only the remaining issues are published.

# Test Issues & Recommendations

Since the smart contract code is not open-source, only the remaining issues are published.

