

SECURITY AUDIT REPORT

QoWatt cards-staking smart contract


by  ARDA
on May 6, 2024



Table of Content

Disclaimer	3
Terminology	3
Audit Summary	4
Inherent Risks	5
Code Issues & Recommendations	7
Test Issues & Recommendations	8

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 and safety of the code, bugfree status or any other statements of the contract.

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/GoWattEcosystem/gowatt-sc>
- **Commit:** eef18d20f118619a39829b835da8144383ce67d4
- **Path to Smart contract:** ./contracts/staking-cards/

Scope of final audit

- **Repository:** <https://github.com/GoWattEcosystem/gowatt-sc>
- **Commit:** d02f3fcef4c2f72dab0462ee069c512611724f54
- **Path to Smart contract:** ./contracts/staking-cards/

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.

3 inherent risks in the final commit

0 issue in the final commit

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

Severity	Reported			Remaining		
	Code	Test	Other	Code	Test	Other
Critical	2	0	0	0	0	0
Major	7	0	0	0	0	0
Medium	10	1	0	0	0	0
Minor	21	0	0	0	0	0

Inherent Risks

R1: Users are not guaranteed to be able to claim boosted rewards.

This is because boosted rewards are in QoWatt coins, and can be claimed only if coins are available in the contract, which is not predictable. Indeed, it depends on whether users mint cards, as it is the only source of coins in the Staking Cards contract. However, even if boosted rewards cannot be claimed in case there are no coins in the contract, users can still use these unclaimed boosted rewards to mint new cards or upgrade their cards.

R2: Users have no guarantee on the rewards which are distributed per block in each pool.

This is because at any time the owner can stop producing rewards, reduce the rewards reserve, change the rewards factor, or change the distribution of rewards between pools.

R3: Users can earn less rewards than they should.

This is because the total number of shares in the Staking Cards can be overestimated, hence the rewards per share (RPS) is underestimated, for the following reasons:

- When a user interacts with the contract, the RPS is updated before removing the shares which have expired in previous epochs. Therefore the RPS increase and the RPS history are computed using an overestimated total number of shares.
- The bonus shares of a user who is inactive contributes to the total number of shares for 14 days, which is the maximum time before a bonus share can

expire, even if the accurate expiry of the user's bonus shares is shorter, e.g. only 2 days.

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.

