

Mar. 2021

# Security Audit

REXTRON

TUMatgmcCgc3q6XS4iECadPB3upb1wZwpQ

# HAECHI LABS

[www.haechi.io](http://www.haechi.io)

**CRITICAL ISSUES (critical, high severity): 0**

Bugs and vulnerabilities that enable theft of funds, lock access to funds without possibility to restore it, or lead to any other loss of funds to be transferred to any party; high priority unacceptable bugs for deployment at mainnet; critical warnings for owners, customers or investors.

**ERRORS, BUGS AND WARNINGS (medium, low severity): 0**

Bugs that can trigger a contract failure, with further recovery only possible through manual modification of the contract state or contract replacement altogether; Lack of necessary security precautions; other warnings for owners and users

**OPTIMIZATION**

Possibilities to decrease cost of transactions and data storage of Smart-Contracts.

**NOTES AND RECOMMENDATIONS (very low severity);2**

Tips and tricks, all other issues and recommendations, as well as errors that do not affect the functionality of the Smart-Contract.

**Conclusion:**

In the REXTRON Smart-Contract were found no vulnerabilities and no backdoors.  
The code was manually reviewed for all commonly know and more specific vulnerabilities.

So REXTRON Smart-Contract is safe for use in the main network.

# HAECHI LABS

# Mar. 2021

## Disclaimer

This audit is not a call to participate in the project and applies only to the Smart - Contract code at the specified address.

If you have any questions or are interested in developing/auditing of Smart - Contracts, please contact us and we will consult you.

Telegram: @heachi

E-mail: [info@hachi.io](mailto:info@hachi.io)