

# Token Sale Audit

*Done by [HungryDev.pro](#) team*

The code is located in the open-source github gist [Token Contract](#) and [Token Sale Contract](#).

All of the issues are classified using the popular OWASP risk rating model. It estimates the severity taking into account both the likelihood of occurrence and the impact of consequences

		Severity		
		Medium	High	Critical
Impact	High			
	Medium			
	Low			
		Low	Medium	High
		Likelihood		

## *Description of the complex of procedures for auditing a smart contract*

### Primary architecture review

- Checking the architecture of the contract.
- Check for linearity, shortness and self-documentation.
- Static verification and code analysis for validity and the presence of syntactic errors.
- Correctness of the code.

### SUMMARY

The code is well organised. Code style follow to the solidity recommendations. There were no critical errors found.. Only one issue with a high severity was identified. Most of the comments regard edge case scenarios and contain advice that will allow easier maintenance of the crowd-sale process in all of the circumstances

### FOUND ISSUES

Severity: **MEDIUM** (Impact: **MEDIUM**, Likelihood: **LOW**)

Dates of ICO stages are not presented in time zone of Madrid, Spain.

Severity: **HIGH** (Impact: **HIGH**, Likelihood: **MEDIUM**)

There is no validation on the purchase of the last token and refund from purchase.

## NOTES AND SUGGESTIONS

- Change functions scope in Sales Contract from **internal** to **private**.
- Lack of comments on functions and some of them done in Russian.
- Better to lock pragmas to specific compiler version.
- Implement reentrancy guard on **closeSale**, **sale1**, **sale2**, **sale3** functions.

## Update

### Executive Summery

The smart contract audit did not discover any issues of critical severity.

### Files Audited

<https://gist.github.com/Smart-Contract-Web/ae8e1a217f9355dad667526b12b751b6>  
<https://gist.github.com/Smart-Contract-Web/d1492c53eb4a34f40eeb1cc88669af51>

### Critical

No critical issues found

### Possible bug

No critical issues found

### Testing

Testing smart contract was successful. No critical issue found.

### Notice

Owner of the Sale contract should be careful with access to the contract because in case of lose access to the contract. The withdraw function *transferEthFromContract* can't be called anymore.