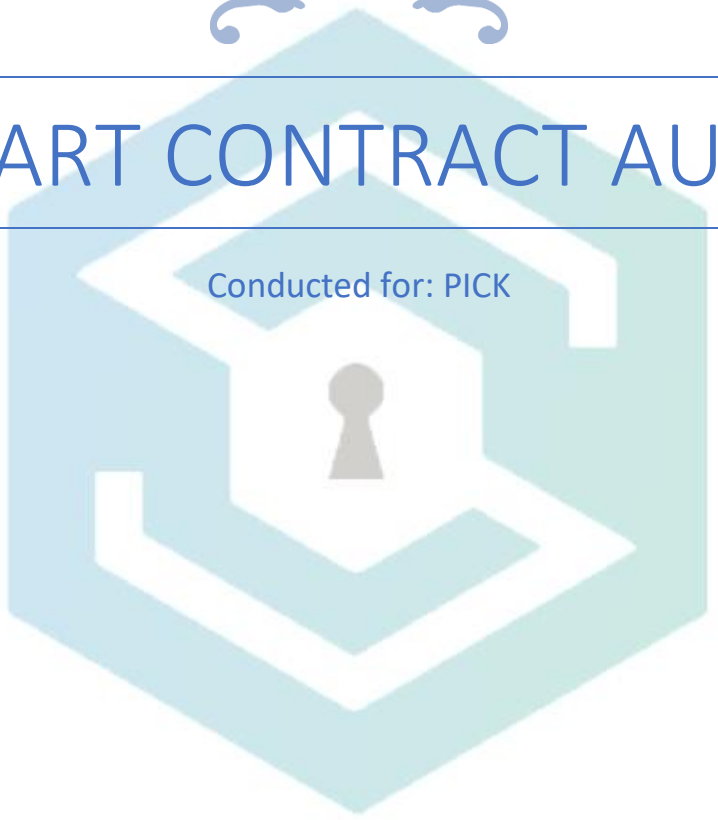
SMART CONTRACT AUDIT

Conducted for: PICK



ZERONIX

Waleed Ahmed
ZERONIX
13/9/2023

Contents

Executive Summary:

The client contacted our Agency to conduct a smart contract audit on their Solidity based smart contract. The smart contract was deployed on the Ethereum Main net. The smart contract is a simple ERC20 contract which basically just inherits the OpenZeppelin ERC20 contract with no additional features. The contract was found to be secure. All of the findings of the audit are detailed inside this report.

Audit conducted by: Waleed Ahmed

Project Background:

The smart contract is written in solidity. The contract was deployed on the Ethereum Main net.

Audit Scope:

Deployed Address	**0x1250c8f5099902ddfb574474612436b0b5Db0a15**
Chain	**Ethereum Mainet**
Language	**Solidity**
Audit Completion Date	**13/9/23**

Audit Summary:

We found:

- **0 Critical risk vulnerabilities**
- **0 High risk vulnerabilities**
- **0 Medium risk vulnerabilities**
- **0 Low risk vulnerabilities**

Severity Definitions:

Risk Level	Description
Critical	Any kind of vulnerability that could lead to direct token or monetary loss
High	Any type of vulnerability that could disrupt the proper functioning of smart contract or indirectly lead to token or monetary loss.
Medium	Any type of vulnerability that could cause undesired actions but no serious disruption or monetary loss
Low	Any type of vulnerability that doesn't have any significant impact on the execution of the proper functioning of contract

Technical Checks:

Checks	Result
Solidity version not specified	Passed
Solidity version too old	Passed
Integer overflow/underflow	Passed
Function input parameters check bypass	Passed
Insufficient randomness used	Passed
Fallback function misuse	Passed
Race Condition	Passed
Logical Vulnerabilities	Passed
Function visibility not explicitly declared	Passed
Use of deprecated keywords/functions	Passed
Out of Gas issue	Passed
Front Running	Passed
Insufficient Decentralization	Passed
Function input parameters lack of check	Passed
Proper function Access Control	Passed
Hardcoded Data	Passed

Code Quality and Documentation:

The audit scope included one smart contract which was written in Solidity programming language. The code is well indented and clear in nature. While the Code lacked commenting.

Audit Findings:

Critical vulnerabilities:

0 critical vulnerabilities were found in the smart contract.

High vulnerabilities:

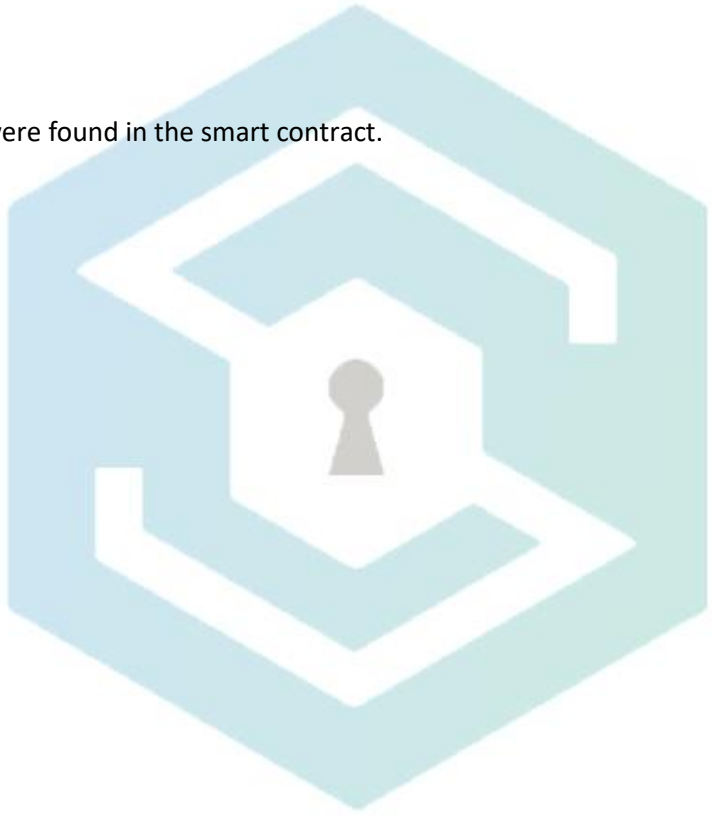
0 high vulnerabilities were found in the smart contract.

Medium vulnerabilities:

0 medium vulnerabilities were found in the smart contract.

Low vulnerabilities:

0 low vulnerabilities were found in the smart contract.



Disclaimer:

The smart contract was tested on a best-effort basis. The smart contract was analyzed with the best security practices known at the time of writing this report. Due to the fact that the total number of test cases is unlimited and the fact that new vulnerabilities in technologies are discovered every day, the audit report makes no guarantees on the security of the contract. While we have done our best in testing this smart contract, it is recommended to not just rely on this audit report alone. A bug bounty program for this smart contract may be created to identify any vulnerabilities within the future.

Conclusion:

The smart contract was tested extensively both automatically and manually. No Vulnerabilities were discovered within it. It is recommended that additional security measures may be undertaken to ensure future security such that of a creation of a bug bounty program.

It is also recommended to use a proxy mechanism in the smart contract to ensure that the smart contract code can be modified in the future.