soken

SMART CONTRACT SECURITY AUDIT

Polygame

Scan and check this report was posted at Soken Github

March, 2022

Website: soken.io

Table of Contents

Disclaimer

This is a comprehensive report based on our automated and manual examination of cybersecurity vulnerabilities and framework flaws. We took into consideration smart contract based algorithms, as well. Reading the full analysis report is essential to build your understanding of project's security level. It is crucial to take note, though we have done our best to perform this analysis and report, that you should not rely on the our research and cannot claim what it states or how we created it. Before making any judgments, you have to conduct your own independent research. We will discuss this in more depth in the following disclaimer - please read it fully.

DISCLAIMER: You agree to the terms of this disclaimer by reading this report or any portion thereof. Please stop reading this report and remove and delete any copies of this report that you download and/or print if you do not agree to these conditions. This report is for non-reliability information only and does not represent investment advice. No one shall be entitled to depend on the report or its contents, and Soken and its affiliates shall not be held responsible to you or anyone else, nor shall Soken provide any guarantee or representation to any person with regard to the accuracy or integrity of the report. Without any terms, warranties or other conditions other than as set forth in that exclusion and Soken excludes hereby all representations, warrants, conditions and other terms (including, without limitation, guarantees implied by the law of satisfactory quality, fitness for purposes and the use of reasonable care and skills). The report is provided as "as is" and does not contain any terms and conditions. Except as legally banned, Soken disclaims all responsibility and responsibilities and no claim against Soken is made to any amount or type of loss or damages (without limitation, direct, indirect, special, punitive, consequential or pure economic loses or losses) that may be caused by you or any other person, or any damages or damages, including without limitations (whether innocent or negligent).

Security analysis is based only on the smart contracts. No applications or operations were reviewed for security. No product code has been reviewed.

Procedure

Our analysis contains following steps:

1. Project Analysis;

2. Manual analysis of smart contracts:
- Deploying smart contracts on any of the network(Ropsten/Rinkeby) using Remix IDE
- Hashes of all transaction will be recorded
- Behaviour of functions and gas consumption is noted, as well.

3. Unit Testing:
- Smart contract functions will be unit tested on multiple parameters and under multiple conditions to ensure that all paths of functions are functioning as intended.
- In this phase intended behaviour of smart contract is verified.
- In this phase, we would also ensure that smart contract functions are not consuming unnecessary gas.
- Gas limits of functions will be verified in this stage.

4. Automated Testing:
- Mythril
- Oyente
- Manticore
- Solgraph

Terminology

We categorize the finding into 4 categories based on their vulnerability:

- Low-severity issue — less important, must be analyzed
- Medium-severity issue — important, needs to be analyzed and fixed
- High-severity issue —important, might cause vulnerabilities, must be analyzed and fixed
- Critical-severity issue —serious bug causes, must be analyzed and fixed.

Limitations

The security audit of Smart Contract cannot cover all vulnerabilities. Even if no vulnerabilities are detected in the audit, there is no guarantee that future smart contracts are safe. Smart contracts are in most cases safeguarded against specific sorts of attacks. In order to find as many flaws as possible, we carried out a comprehensive smart contract audit. Audit is a document that is not legally binding and guarantees nothing.

Token Contract Details for 30.03.2022

Contract Name: **LockableToken**

Deployed address: **0xcDa6c923458cA9faC8e3354999e866FeAa80B72f**

Total Supply: **5,000,000,000**

Token Tracker: **$PGEM**

Decimals: **18**

Token holders: **4433**

Transactions count: **4466**

Top 100 holders dominance: **100.00%**

Audit Details

Project Name: **Polygame**

Language: **Solidity**

Compiler Version: **v0.8.0**

Blockchain: **Polygon**

Social Profiles

Project Website: **https://polygame.io/**

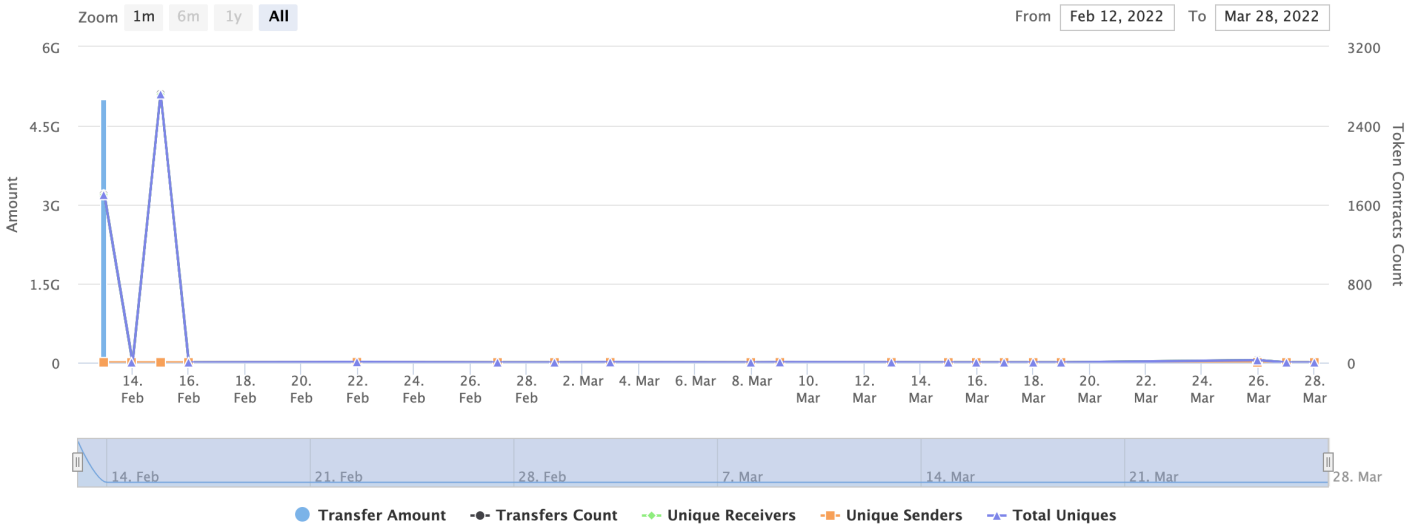
Project Telegram: **https://t.me/polygamers**

Project Facebook: **https://www.facebook.com/polygame.io**

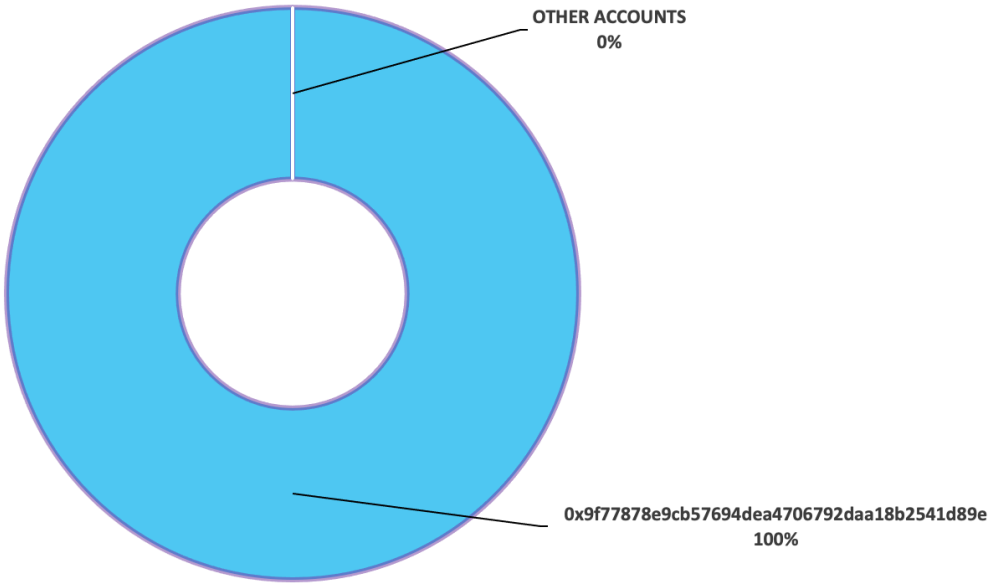
Project Discord: **https://discord.com/invite/5VCmyf4HFJ**

Project YouTube: **https://www.youtube.com/channel/UCON3Lo2AS3J2ISYmVzmlnLQ**

Contract Analytics



$PGEM Token Distribution



$PGEM Top Holders

Rank	Address	Quantity	Percentage
1	0x9f77878e9cb57694dea4706792daa18b2541d89e	4,999,965,621.5	99.9993%
2	0xdd4ffec5e435bee65ca5d411502351f8385c33ba	964.5	0.0000%
3	0x69aa5b58d21d509919dcf35f400c104a4a4d25d8	883.5	0.0000%
4	0x99c13cb5f66ad6e221426ac5eed94a227809eb29	770	0.0000%
5	0xb3a4a1bb2e8e05e38f44a60c02f7eecc415fb156	581	0.0000%
6	0x08641f45f84da7cd8393d7044aba7ea513727db6	566	0.0000%
7	0x30afa2c930ba0f156e5eaf6792116fec0628c941	295	0.0000%
8	0xc0dedc6a05bb682f99fcfbf04f1820594b8796d7	260	0.0000%
9	0xe728ce82d36b72e74679c5e51f0341a3b64a4512	236.5	0.0000%
10	0xf5791bd882173731e233a4a7f0d2ecb172fe5b19	202.5	0.0000%

Vulnerabilities checking

Issue Description	Checking Status
Compiler Errors	Completed
Delays in Data Delivery	Completed
Re-entrancy	Completed
Transaction-Ordering Dependence	Completed
Timestamp Dependence	Completed
Shadowing State Variables	Completed
DoS with Failed Call	Completed
DoS with Block Gas Limit	Completed
Outdated Complier Version	Completed
Assert Violation	Completed
Use of Deprecated Solidity Functions	Completed
Integer Overflow and Underflow	Completed
Function Default Visibility	Completed
Malicious Event Log	Completed
Math Accuracy	Completed
Design Logic	Completed
Fallback Function Security	Completed
Cross-function Race Conditions	Completed
Safe Zeppelin Module	Completed

Conclusion

Smart contracts are free from any critical, high, medium or low-issues.

NOTE: Please check the disclaimer above and note, that audit makes no statements or warranties on business model, investment attractiveness or code sustainability.

Soken Contact Info

Website: www.soken.io

Mob: (+1)416-875-4174

32 Britain Street, Toronto, Ontario, Canada

Telegram: @team_soken

GitHub: sokenteam

Twitter: @soken_team