HackSafe

Smart Contract Security Audit Report

MATIC

June 2022

Security Status

★ ★ ★ ★ ★

www.hacksafe.io

Audit Details

Audited project
MATIC

Deployer address
0x78655080b65f42E2ceE5FA5673689CC44D4E1cFC

Client contacts
Matic team

Blockchain
Ethereum

Website
https://polygon.technology/

Disclaimer

This is a limited report on our findings based on our analysis, in accordance with good industry practice as at the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report. While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the below disclaimer below – please make sure to read it in full.

DISCLAIMER: By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice. No one shall have any right to rely on the report or its contents, and TechRate and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (HackSafe) owe no duty of care towards you or any other person, nor does HackSafe make any warranty or representation to any person on the accuracy or completeness of the report. The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and HackSafe hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, HackSafe hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against HackSafe, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report.

The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed.

Procedure

Step 1 - In-Depth Manual Review

Manual line-by-line code reviews to ensure the logic behind each function is sound and safe from various attack vectors. This is the most important and lengthy portion of the audit process (as automated tools often cannot find the nuances that lead to exploits such as flash loan attacks).

Step 2 - Automated Testing

Simulation of a variety of interactions with your Smart Contract on a test blockchain leveraging a combination of automated test tools and manual testing to determine if any security vulnerabilities exist.

Step 3 – Leadership Review

The engineers assigned to the audit will schedule meetings with our leadership team to review the contracts, any comments or findings, and ask questions to further apply adversarial thinking to discuss less common attack vectors.

Step 4 - Resolution of Issues

Consulting with the team to provide our recommendations to ensure the code's security and optimize its gas efficiency, if possible. We assist project team's in resolving any outstanding issues or implementing our recommendations.

Step 5 - Published Audit Report

Boiling down results and findings into an easy-to-read report tailored to the project. Our audit reports highlight resolved issues and any risks that exist to the project or its users, along with any remaining suggested remediation measures. Diagrams are included at the end of each report to help users understand the interactions which occur within the project.

Background

HackSafe was commissioned by MATIC to perform an audit of smart contract:

- https://etherscan.io/address/0x7D1AfA7B718fb893dB30A3aBc0Cfc608AaCfeBB0#code

The purpose of the audit was to achieve the

- Ensutre that the smart contract functions as intended.
- Identify potential security issues with the smart contract.

The information in this report should be understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Contract Details

Token contract details for 30.06.2022

Token Type	: ERC20
Contract name	: MaticToken
Contract address	: 0x7D1AfA7B718fb893dB30A3aBc0Cfc608AaCfeBB0
Compiler version	: v0.5.2+commit.1df8f40c
Total supply	: 10,000,000,000
Token Ticker	: MATIC
Decimals	: 18
Token Holders	: 450,408
Top 100 token holder's dominance	: 88.32%
Transactions count	: 4,221,267
Contract deployer address	: 0x78655080b65f42E2ceE5FA5673689CC44D4E1cFC
Owner address	: No Owner

Social profiles

Twitter Profile	: https://twitter.com/0xPolygon
Github Profile	: https://github.com/maticnetwork/
Whitepaper link	: https://github.com/maticnetwork/whitepaper
Telegram Profile	: https://t.me/polygonofficial
Coinmarketcap profile	: https://coinmarketcap.com/currencies/polygon/
Coingecko profile	: https://www.coingecko.com/en/coins/polygon
Uniswap profile:	https://v2.info.uniswap.org/pair/0x819f3450da6f110ba6ea52195b3beafa246062de/
Reddit profile	: https://www.reddit.com/r/0xPolygon/
Discord profile	: https://discord.com/invite/polygon

Claimed Smart Contract Features

Claimed Feature Detail	Our Observation
Tokenomics : • **Name** : MaticToken • **Symbol** : MATIC • **Decimals** : 18 • **Protocol** : ERC20 • **Max Total supply** : 10,000,000,000	Yes, This is valid.

Audit Summary

According to the standard audit assessment, Customer`s solidity smart contracts are “well Secure”. This token contract does not contain owner control, which do make it fully decentralized as owner does not have control over smart contract.

Insecure	Poor secured	Secure	Well-secured

You are here

We used various tools like Slither, Mythril and Remix IDE. At the same time this finding is based on critical analysis of the manual audit. All issues found during analysis were manually reviewed and applicable vulnerabilities are presented in the issues checking status.

We found 0 critical, 0 high, 0 medium and 0 low and some very low-level issues. These issues are not critical ones.

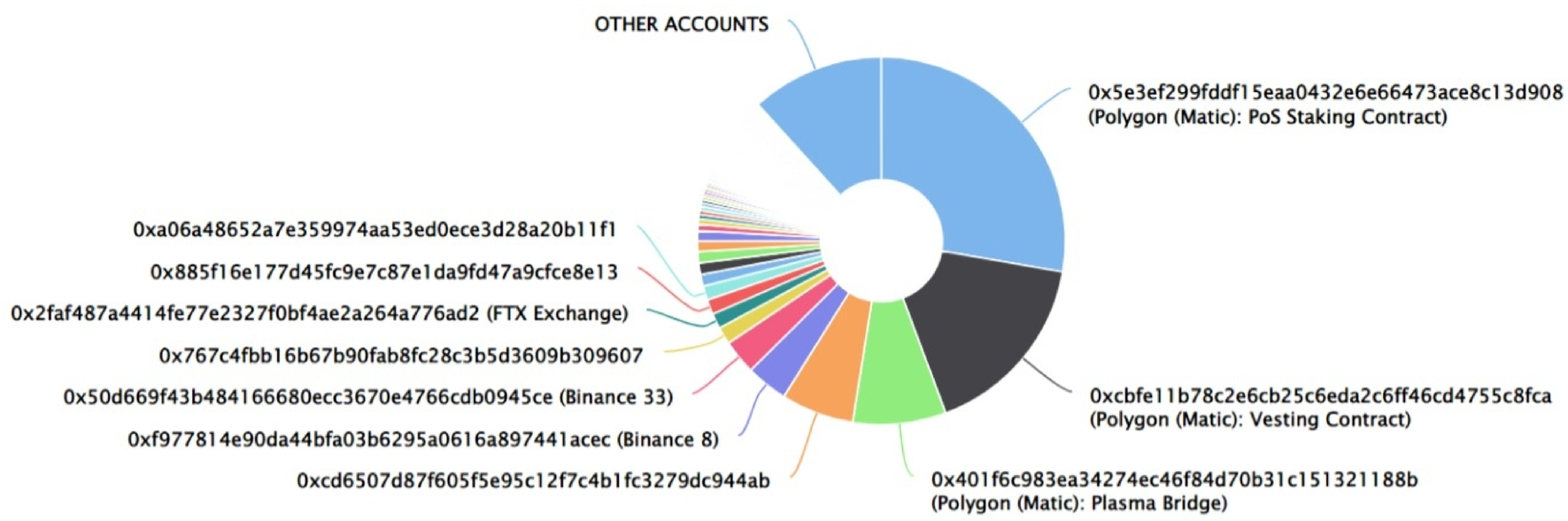
MATIC Distribution

The top 100 holders collectively own 88.29% (8,828,735,961.76 Tokens) of Matic Token

Token Total Supply: 10,000,000,000.00 Token | Total Token Holders: 450,434

Matic Token Top 100 Token Holders

Source: Etherscan.io



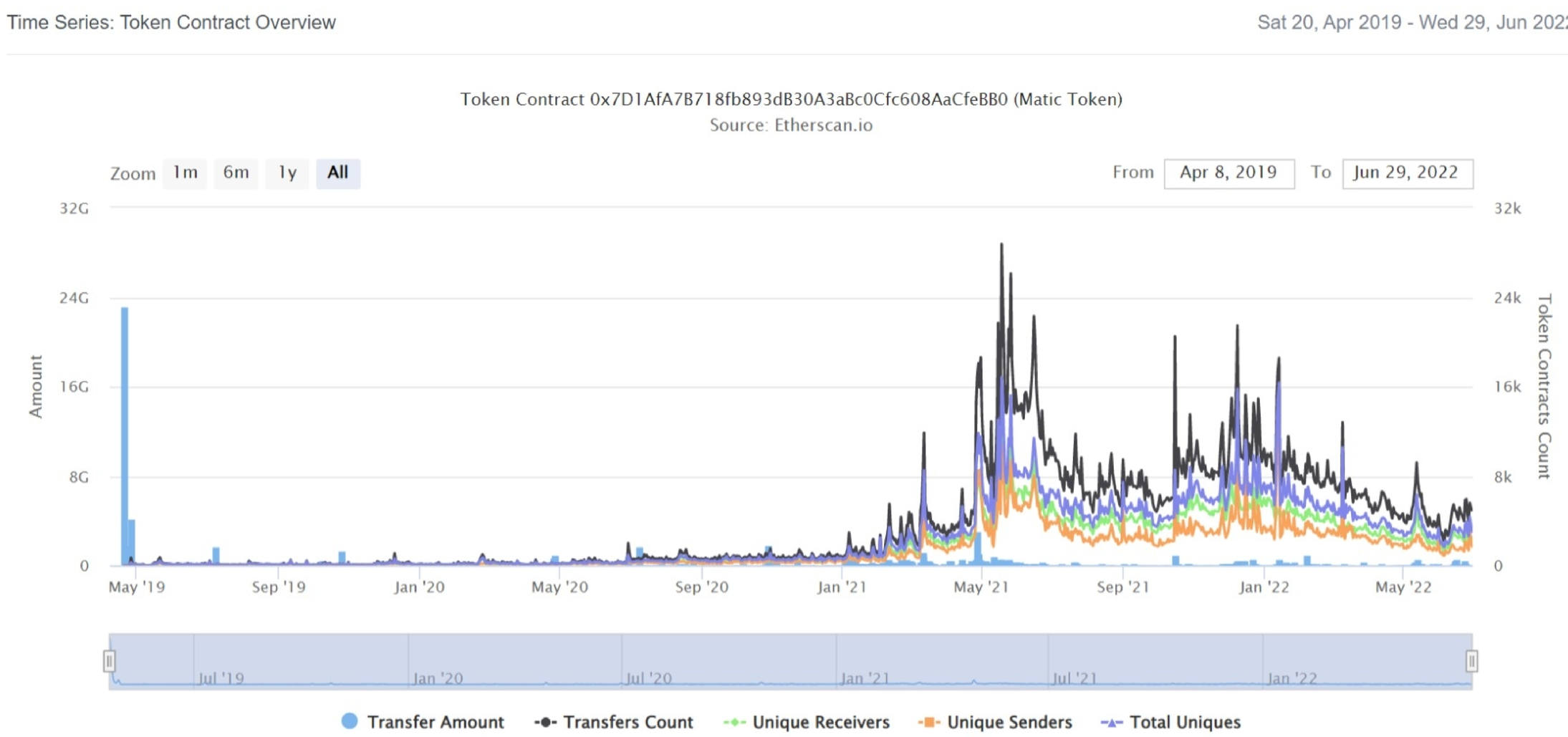
MATIC Top 20 Token Holders

(A total of 8,828,735,961.76 tokens held by the top 100 accounts from the total supply of 10,000,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	Polygon (Matic): PoS Staking Contract	2,771,617,706.611931845726836148	27.7162%
2	Polygon (Matic): Vesting Contract	1,659,914,448	16.5991%
3	Polygon (Matic): Plasma Bridge	820,269,193.94398339474759366	8.2027%
4	0xcd6507d87f605f5e95c12f7c4b1fc3279dc944ab	639,677,517	6.3968%
5	Binance 8	367,493,226.989795965841358993	3.6749%
6	Binance 33	302,000,000	3.0200%
7	0x767c4fbb16b67b90fab8fc28c3b5d3609b309607	153,522,448.095432116527724652	1.5352%
8	FTX Exchange	133,044,523.614502331486733572	1.3304%
9	0x885f16e177d45fc9e7c87e1da9fd47a9cfce8e13	130,919,948.074665317850693876	1.3092%
10	0xa06a48652a7e359974aa53ed0ece3d28a20b11f1	125,001,000	1.2500%
11	Binance 34	103,000,000	1.0300%
12	0x5a52e96bacdabb82fd05763e25335261b270efcb	100,577,528.722793867197916053	1.0058%
13	0x3b7bb88db769923dc2ee1e9e6a83c00a74c407d2	100,000,100	1.0000%
14	0x0d16c4a9c9f3a2440ffa403b8ed105b88794e356	90,422,580	0.9042%
15	0xa83b11093c858c86321fbc4c20fe82cdbd58e09e	89,486,326.478436918703972283	0.8949%
16	0x766ee93384795a08632e2cecc82a593e55bcf969	57,339,449.541	0.5734%
17	Gemini 6	45,665,000	0.4567%
18	Binance US 2	39,341,064.503388481256163814	0.3934%
19	0x73af3bcf944a6559933396c1577b257e2054d935	36,310,949	0.3631%
20	Crypto.com	33,674,805.710223865467601046	0.3367%

MATIC Distribution

MATIC Contract Overview



Contract functions details

+[Int] IERC20
- -[Ext] transfer
- -[Ext] approve
- -[Ext] transferFrom
- -[Ext] totalSupply
- -[Ext] balanceOf
- -[Ext] allowance

+[Lib] SafeMath
- -[Int] mul
- -[Int] div
- -[Int] sub
- -[Int] add
- -[Int] mod

+ ERC20 (IERC20)
- -[Pub] totalSupply
- -[Pub] balanceOf
- -[Pub] allowance
- -[Pub] transfer #
- -[Pub] approve #
- -[Pub] transferFrom #
- -[Pub] increaseAllowance #
- -[Pub] decreaseAllowance #
- -[Int] _transfer #
- -[Int] _mint #
- -[Int] _burn #
- -[Int] _burnFrom #

+ [Lib] Roles
- -[Int] add
- -[Int] remove
- -[Int] has

+ PauserRole
- -[Int] <constructor>
- -[Pub] isPauser
- -[Pub] addPauser
  - -modifiers: onlyPauser
- -[Pub] renouncePauser

Contract functions details

```
+ Coin98 (Context, Ownable, Pausable, IERC20)
    -[Int] _addPauser
    -[Int] _removePauser
    +Pausable (PauserRole)
    -[Int] <constructor>
    -[Pub] paused
    -[Pub] pause
      -modifiers: onlyPauser whenNotPaused
    -[Pub] unpause
      -modifiers: onlyPauser whenPaused

+ERC20Pausable (ERC20, Pausable)
    -[Pub] transfer
      -modifiers: whenNotPaused
    -[Pub] transferFrom #
      -modifiers: whenNotPaused
    -[Pub] approve #
      -modifiers: whenNotPaused
    -[Pub] increaseAllowance #
      -modifiers: whenNotPaused
    -[Pub] decreaseAllowance #
      -modifiers: whenNotPaused

+ERC20Detailed (IERC20)
    -[Pub] constructor #
    -[Pub] name
    -[Pub] symbol
    -[Pub] decimals

+MaticToken (ERC20Pausable, ERC20Detailed)
    -[Pub] <constructor> #
```

($) = payable function

= non-constant function

Issues Checking Status

No.	Title	Status
1.	Unlocked Compiler Version	Passed
2.	Missing Input Validation	Passed
3.	Race conditions and Reentrancy. Cross-function race conditions.	Passed
4.	Possible delays in data delivery	Passed
5.	Oracle calls.	Passed
6.	Timestamp dependence.	Passed
7.	Integer Overflow and Underflow	Passed
8.	DoS with Revert.	Passed
9.	DoS with block gas limit.	Passed
10.	Methods execution permissions.	Passed
11.	Economy model of the contract.	Passed
12.	Private use data leaks.	Passed
13.	Malicious Event log.	Passed
14.	Scoping and Declarations.	Passed
15.	Uninitialized storage pointers.	Passed
16.	Arithmetic accuracy.	Passed
17.	Design Logic.	Passed
18.	Safe Open Zeppelin contracts implementation and usage.	Passed
19.	Incorrect Naming State Variable	Passed
20.	Compiler version too old	Passed

Severity Definitions

Risk Level	Description
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to assets loss or data manipulations.
High	High-level vulnerabilities are difficult to exploit; however, they also have a significant impact on smart contract execution, e.g., public access to crucial functions
Medium	Medium-level vulnerabilities are important to fix; however, they can't lead to assets loss or data manipulations.
Low	Low-level vulnerabilities are mostly related to outdated, unused, etc. code snippets that can't have a significant impact on execution.

Security Issues

Critical Severity Issues
No critical severity issue found.

High Severity Issues
No high severity issue found.

Medium Severity Issues
No medium severity issues found.

Low Severity Issues
No low severity issue found.

Centralization

Pauser Privileges

Pauser can add other pauser addresses to let them pause the transfers of the tokens.

This smart contract has some functions which can be executed by the pauser addresses only. If their wallet private key would be compromised, then it would create trouble.

Conclusion

Smart contract contains low severity issues! The further transfer and operations with the fund raised are not related to this particular contract.

HackSafe note: Please check the disclaimer above and note, the audit makes no statements or warranties on business model, investment attractiveness or code sustainability. The report is provided for the only contract mentioned in the report and does not include any other potential contracts deployed by Owner.