INVARIANT AUDITING
SOLUTIONS

MG Token Smart Contract Audit

Executive Summary

The Millionaire Game (MG) token, which complies with the ERC20 standard, is currently deployed and publicly viewable at the following web address: https://etherscan.io/address/0x795258Ff27bDf2Fe7c25931f5d23356B63d75AD5.

The MG token incorporates two admin-specific functions, namely **'mint'** and **'burn'**. It should be noted that the administrative entity initially had the authority to burn tokens from any account. However, they have subsequently relinquished this ownership.

The maximum limit for the MG token supply is established at one billion (1,000,000,000) tokens.

Methodology

1. Static Analysis: mythril, slither
2. Manual Inspection: code and unit tests
3. Invariant Violation Testing: echidna

Token Information

Chain	Ethereum
Token Address	0x795258Ff27bDf2Fe7c25931f5d23356B63d75AD5
Name	Millionaire Game
Symbol	MG
Decimals	18

Vulnerability Checklist

Reentrancy Vulnerability	No
Arithmetic Overflow Underflow	No
Dead-code	No

Upgradeable Contract	No
Arbitrary Contract Call	No
Arbitrary Storage Write	No
Delegate Call to Arbitrary Contract	No
Low-level Calls	No
Dependence on Predictable Variables	No
Signature Verification	No
Unbounded Loops	No
Improper Events	No
Improper Authorization Design	No
Oracle Issues	No
Logical Issues	No
Centralization Issues	Yes

Centralization Issues

Does the contract contain admin-only functions?	Yes
Are the admin-only functions standard?	'mint' and 'burn' are common
Does the token contain a black or block list?	No
Does the token allocation match the whitepaper?	Yes

Exclusive Admin-only Functions

'mint' Function Description

The **'mint'** function within this contract permits the administrative entity to produce tokens for any specified address, provided the total supply remains under the maximum limit of 1 billion tokens.

However, considering the fact that the administrator has already generated the maximum permissible quantity of 1 billion tokens shortly after the contract's deployment, the capacity to further expand the token supply through the 'mint' function is now infeasible.

On-chain 'mint' Calls

mint(address to, uint256 value)	
Time and TxHash	**Call**
May-11-2023 10:02:11 AM +UTC	mint(to=0x795258ff27bdf2fe7c25931f5d23356b63d75ad5, value=100000000000000000000000000)
0x81b2d8844c12ec31b75aa18a6b517bfa464d3ad43aaff0941ed71b8750a14976	

'burn' Function Description

The **'burn'** function, accessible exclusively to the administrator, has the capability to annihilate the token holdings of any given holder.

But since the deployer of the MG token has relinquished their ownership, the activation of the **'burn'** function has become unfeasible. The burn function was never called for the token.

Transfer of Ownership and Admin Roles

The ownership of the MG token contract was initially held by the Millionaire Game deployer within the blockchain range from block 17236340 to 17243151. Subsequently, the MG token deployer has relinquished their ownership rights, rendering the administrative-specific functions inaccessible and non-executable by any party.

On-Chain 'renounceRole' Calls

<table>
<tr><td colspan="2">renounceRole(bytes32 role, address account)</td></tr>
<tr><td>Time and TxHash</td><td>Call</td></tr>
<tr><td>May-12-2023 07:38:35 AM +UTC

0x60f4dade8ae3dad47f854fe50402bf4fc5fe6ff6aed5acafb82d5a2027b9c286</td><td>renounceRole(role=0x1effbbff9c66c5e59634f24fe842750c60d18891155c32dd155fc2d661a4c86d, account=0xA24692D171732722D62b8E3f57338F50aE1C0137)</td></tr>
<tr><td colspan="2">Role `0x1effbbff9c66c5e59634f24fe842750c60d18891155c32dd155fc2d661a4c86d` is not used in the contract and this was likely an operations mistake
This transaction effectively did not change anything</td></tr>
<tr><td>Time and TxHash</td><td>Call</td></tr>
<tr><td>May-12-2023 07:52:35 AM +UTC

0x34c274d3f1e3991843d32cba3301c2750ebc2c836b8452759cd774616b42cfa9</td><td>renounceRole(role=0x0000000000000000000000000000000000000000000000000000000000000000, account=0xA24692D171732722D62b8E3f57338F50aE1C0137)</td></tr>
<tr><td colspan="2">Role `0x0000000000000000000000000000000000000000000000000000000000000000` is the DEFAULT_ADMIN_ROLE
After this transaction, the deployer can no longer add or remove accounts that can call admin-only functions</td></tr>
<tr><td>Time and TxHash</td><td>Call</td></tr>
<tr><td>May-12-2023 09:09:47 AM +UTC

0x63fa2e2a6f14af0ae46f6a2036410f974e7791da52cd521767d068c872b93c1e</td><td>renounceRole(role=0x154c00819833dac601ee5ddded6fda79d9d8b506b911b3dbd54cdb95fe6c3686, account=0xA24692D171732722D62b8E3f57338F50aE1C0137)</td></tr>
<tr><td colspan="2">Role `0x154c00819833dac601ee5ddded6fda79d9d8b506b911b3dbd54cdb95fe6c3686` is the MINT_ROLE
After this transaction, the deployer can no longer call the mint function</td></tr>
</table>

ERC20 Implementation

The core ERC20 functionality of the Millionaire Game token utilizes code from the solmate library. Consequently, its core implementation is based on well-reviewed and extensively tested code.

The **'ERC20Capped.sol'** is the solmate 'ERC20.sol' modified to have a maximum token supply cap.

Token Supply and Transfer Activity

Upon deployment, the Millionaire Game token immediately minted its maximal token supply of 1 billion tokens. These minted tokens were directly transferred to the account of the token deployer. Evidence of this transaction can be found at the following link: https://etherscan.io/tx/0x81b2d8844c12ec31b75aa18a6b517bfa464d3ad43aaff0941ed71b8750a14976.

Since the deployment entity has relinquished its ownership rights, it should be noted that there is no available mechanism to augment the supply of MG tokens further.

The MG token deployer then executed the following transfers:

1. A transfer of 201,800,000 tokens was made to the Prize pool, as documented in this transaction: https://etherscan.io/tx/0xcb2d983587bc67ce7de74610d53ae8d1578d2b01c2e53bba675b15a8b9f2f3d3.
2. A transfer of 69,000,000 tokens was made to the CEX Listings pool, as captured in this transaction: https://etherscan.io/tx/0x191abd99a1852440ac62b04b5a9748bfdee7e60ebf2431e0ff1c63f136d93e08.
3. Finally, a transfer of 729,200,000 tokens was made to the Liquidity pool, as indicated in this transaction: https://etherscan.io/tx/0x8fad50a5defc92dd5bf02b83ccc9b376fb1320403fe4cba987b497aa749c9d68.

These token transfers match the token allocation stipulated on the Millionaire Game's official website and whitepaper.