Balance Network

Smart Contract Audit Report

AUDIT SUMMARY

Balance Network is a new BEP-20 token on the Binance Smart Chain.

For this audit, we reviewed the project team's BalanceNetwork contract at 0x5Cf8eA4278f689B301C4a17DdCa9D5ec8b0B0511 on the Binance Smart Chain Mainnet.

We previously reviewed the project team's token contract here.

AUDIT FINDINGS

> *No findings were identified, though some centralized aspects are present.*
> *Date: May 8th, 2023.*

CONTRACT OVERVIEW

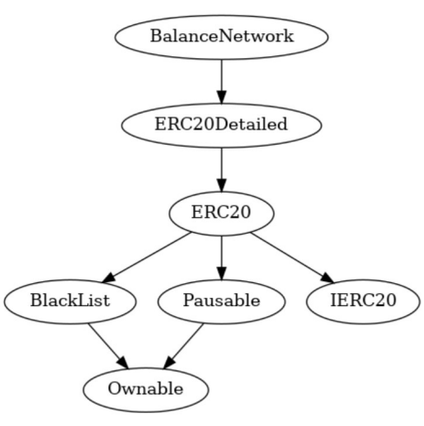
> - *The total supply of the token is set to 200 million [200,000,000] $BLN.*
> - *No mint functions are accessible beyond deployment.*
> - *The owner can burn their own tokens to reduce the total supply at any time.*
> - *At the time of writing this report, there are 216 total token holders. The token allocation is as follows:*
>   - *29.82% of the total supply belongs to the owner.*
>   - *20% of the total supply is locked in a Trustswap token locking contract and will unlock on June 5th, 2023.*
>   - *10% of the total supply is stored in a vesting contract.*
>   - *10% of the total supply is stored in a vesting contract.*
>   - *10% of the total supply is stored in a vesting contract.*
>   - *10% of the total supply is stored in a vesting contract.*
>   - *5% of the total supply is stored in a vesting contract.*
>   - *5% of the total supply is stored in a vesting contract.*
>   - *0.085% of the total supply is in Pancakeswap liquidity.*
>   - *Of that liquidity, 99.87% of the LP tokens are locked in a Trustswap token locking contract and will unlock on September 4th, 2023.*
>   - *The next five EOAs own a cumulative 0.0574% of the total supply.*
>
> - *Blacklisted users are prohibited from participating in transfers.*
> - *The owner can add/remove any address from the transfer blacklist at any time.*
> - *The owner can burn any blacklisted user's full token balance at any time.*
> - *The owner can pause/unpause trading at any time.*
> - *There are no fees associated with transferring tokens.*
> - *As the contract is deployed with Solidity v0.8.12, it is protected from overflows/underflows.*
> - *The contract complies with the BEP-20 token standard.*

AUDIT RESULTS

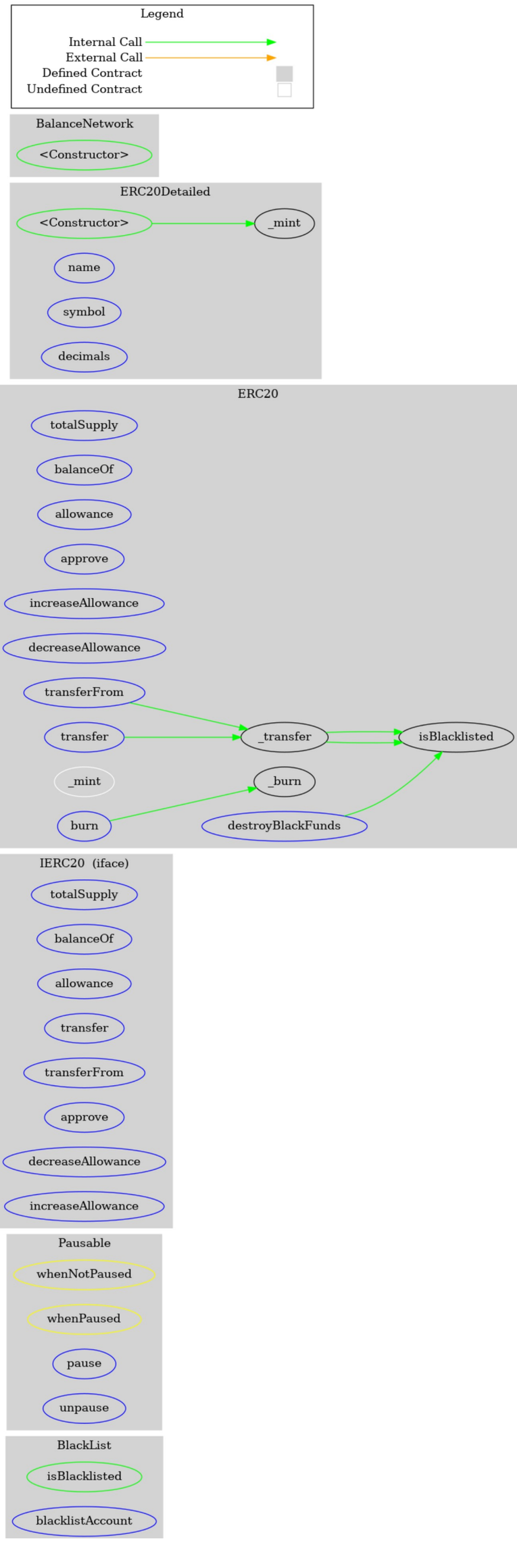
Vulnerability Category	Notes	Result
Arbitrary Jump/Storage Write	N/A	PASS
Centralization of Control	The owner can add any account to the transfer blacklist and burn their full token balance at any time.	WARNING
Compiler Issues	N/A	PASS

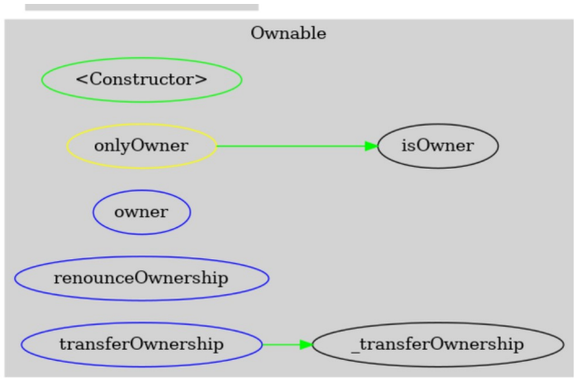
Vulnerability Category	Notes	Result
Delegate Call to Untrusted Contract	N/A	PASS
Dependence on Predictable Variables	N/A	PASS
Ether/Token Theft	N/A	PASS
Flash Loans	N/A	PASS
Front Running	N/A	PASS
Improper Events	N/A	PASS
Improper Authorization Scheme	N/A	PASS
Integer Over/Underflow	N/A	PASS
Logical Issues	N/A	PASS
Oracle Issues	N/A	PASS
Outdated Compiler Version	N/A	PASS
Race Conditions	N/A	PASS
Reentrancy	N/A	PASS
Signature Issues	N/A	PASS
Sybil Attack	N/A	PASS
Unbounded Loops	N/A	PASS
Unused Code	N/A	PASS
Overall Contract Safety		PASS

INHERITANCE CHART



FUNCTION GRAPH


Legend
Internal Call
External Call
Defined Contract
Undefined Contract
BalanceNetwork
<Constructor>
ERC20Detailed
<Constructor>
_mint
name
symbol
decimals
ERC20
totalSupply
balanceOf
allowance
approve
increaseAllowance
decreaseAllowance
transferFrom
transfer
_transfer
isBlacklisted
_mint
_burn
burn
destroyBlackFunds
IERC20 (iface)
totalSupply
balanceOf
allowance
transfer
transferFrom
approve
decreaseAllowance
increaseAllowance
Pausable
whenNotPaused
whenPaused
pause
unpause
BlackList
isBlacklisted
blacklistAccount



FUNCTIONS OVERVIEW

```
($) = payable function
# = non-constant function

Int = Internal
Ext = External
Pub = Public

+  Ownable
   - [Pub]  #
   - [Ext] owner
   - [Pub] isOwner
   - [Ext] renounceOwnership #
      - modifiers: onlyOwner
   - [Ext] transferOwnership #
      - modifiers: onlyOwner
   - [Int] _transferOwnership #

+  BlackList (Ownable)
   - [Pub] isBlacklisted
   - [Ext] blacklistAccount #
      - modifiers: onlyOwner

+  Pausable (Ownable)
   - [Ext] pause #
      - modifiers: onlyOwner,whenNotPaused
   - [Ext] unpause #
      - modifiers: onlyOwner,whenPaused

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

+  ERC20 (IERC20, BlackList, Pausable)
   - [Ext] totalSupply
   - [Ext] balanceOf
   - [Ext] allowance
   - [Ext] approve #
   - [Ext] increaseAllowance #
   - [Ext] decreaseAllowance #
   - [Ext] transferFrom #
   - [Ext] transfer #
   - [Int] _transfer #
      - modifiers: whenNotPaused
   - [Int] _mint #
   - [Ext] burn #
      - modifiers: onlyOwner
   - [Int] _burn #
   - [Ext] destroyBlackFunds #
      - modifiers: onlyOwner

+  ERC20Detailed (ERC20)
   - [Pub]  #
   - [Ext] name
   - [Ext] symbol
   - [Ext] decimals
```

```
+  BalanceNetwork (ERC20Detailed)
   - [Pub]  #
      - modifiers: ERC20Detailed
```

ABOUT SOLIDITY FINANCE

Solidity Finance was founded in 2020 and quickly grew to have one of the most experienced and well-equipped smart contract auditing teams in the industry. Our team has conducted 1500+ solidity smart contract audits covering all major project types and protocols, securing a total of over $50 billion U.S. dollars in on-chain value!
Our firm is well-reputed in the community and is trusted as a top smart contract auditing company for the review of solidity code, no matter how complex. Our team of experienced solidity smart contract auditors performs audits for tokens, NFTs, crowdsales, marketplaces, gambling games, financial protocols, and more!

Contact us today to get a free quote for a smart contract audit of your project!

WHAT IS A SOLIDITY AUDIT?

Typically, a smart contract audit is a comprehensive review process designed to discover logical errors, security vulnerabilities, and optimization opportunities within code. A *Solidity Audit* takes this a step further by verifying economic logic to ensure the stability of smart contracts and highlighting privileged functionality to create a report that is easy to understand for developers and community members alike.

HOW DO I INTERPRET THE FINDINGS?

Each of our Findings will be labeled with a Severity level. We always recommend the team resolve High, Medium, and Low severity findings prior to deploying the code to the mainnet. Here is a breakdown on what each Severity level means for the project:

- **High** severity indicates that the issue puts a large number of users' funds at risk and has a high probability of exploitation, or the smart contract contains serious logical issues which can prevent the code from operating as intended.
- **Medium** severity issues are those which place at least some users' funds at risk and has a medium to high probability of exploitation.
- **Low** severity issues have a relatively minor risk association; these issues have a low probability of occurring or may have a minimal impact.
- **Informational** issues pose no immediate risk, but inform the project team of opportunities for gas optimizations and following smart contract security best practices.