© Hexlant Inc.
340 Gangnam-daero
Seoul,
Republic of Korea 06242
Hexlant.com

BBF
SMART CONTRACT
AUDIT REPORT

Audit Date
10 JAN 2022

Category
Token Contract

Auditor
Hexlant Audit Team

This audit report specifies that the Hexlant Technical Team validated and notified that it has no technical defects.

AUDIT OVERVIEW

PUBLISHED INFORMATION	
REPORT NUMBER	ERC20220110cm
DATE	2022/01/10
PUBLISHER	Henry / henry@hexlant.com

PROJECT INFORMATION			
TITLE	Bubblefong		
SYMBOL	BBF		
PLATFORM	ETHEREUM	TOKEN TYPE	ERC-20
TOTAL SUPPLY	1,000,000,000 BBF		
CONTRACT ADDRESS	0xde075d9adbd0240b4462f124af926452ad0bac91		

VULNERABILITY ANALYSIS		
CRITICAL	0	No relevant provision
HIGH	0	No relevant provision
MEDIUM	0	No relevant provision
LOW	0	No relevant provision

CENTRALIZED FUNCTION		
FREEZE	YES	Ability to freeze tokens in accounts. (The administrator can freeze the hacker's account in case of hacking.)
PAUSE	YES	Ability to pause functions related to token transmission in a contract (This is used when the administrator needs to prevent the movement of assets due to token swaps or hacking.)
LOCKUP	NO	Ability to block token transfers for a period of time (Administrators can set lockout periods for investors, team members, advisors, etc.)
BURN	YES	Ability to reduce total supply by burning tokens
MINT	NO	Ability to increase total supply by minting tokens

COMPANY PROPOSAL

Hexlant is a blockchain technology company founded in 2018 by security, network, and software experts from Samsung Electronics. They discovered security defects in smart contracts and blockchain protocols, so they established Hexlant to demonstrate the technical stability of the blockchain ecosystem.

At Hexlant, we support more than 20 blockchain networks directly to understand the blockchain operating system entirely. Furthermore, we have developed security algorithms for private keys and network monitoring technology. We have developed technologies that work on all blockchain network platforms we support, including Bitcoin, Ethereum, Polkadot, and Cardano(ADA).

We certify smart contract technology based on our experiences in technology operations. We provide blockchain technical guides by testing smart contracts and detecting defects in them. We are dedicated to helping our customers to track down problems in their blockchain businesses and smart contracts to continue operating their services from a service perspective.

Our customers can receive services across blockchain technology, from smart contract security vulnerability audit and owner key management to blockchain wallet system establishment. Currently, more than 200 of our customers have started and operated blockchain businesses based on our services and have achieved 12 trillion KRW in accumulated assets.

Initials for identification purposes:

For identification purposes
Hexlant.

CONTENTS

ANALYSIS PURPOSE

This report analyzes and summarizes the results of published contract codes to determine whether they meet the requirements and identify security vulnerabilities and problems that may arise in practice. Hexlant Technical Team conducted this code analysis to verify the following factors:

- Proper operation of the implemented functions
- Security risks during the operation
- Preparation for the potential issues in off-chain transactions
- Readability and completeness of the contract codes

VULNERABILITY CLASSIFICATION

This vulnerability verification evaluates and classifies as below:

● **Critical Severity**

The critical-severity phase is a significant security flaw and causes fatal issues such as asset theft, freezing, and additional issuance. This defect must be corrected.

● **High Severity**

The high-severity phase is an item that can cause security defects due to special conditions and is strongly recommended for correction.

● **Medium Severity**

The medium-severity phase is not a security flaw but causes inefficient contract behavior. It is an item that is recommended modification to operate the contract efficiently.

● **Low Severity**

The low-severity phase is an item with no security issues but is recommended for modifications to improve the contract structure.

BBF CONTRACT **VULNERABILITY ANALYSIS**		
● **CRITICAL**	0	No relevant provision
● **HIGH**	0	No relevant provision
● **MEDIUM**	0	No relevant provision
● **LOW**	0	No relevant provision

FUNCTION SUMMARY

- **Ownable**
  This function provides features related to contract ownership. This function can limit the ability to execute functions to a specific address by using the onlyOwner Modifier.

- **ERC20Burnable**
  This function provides features related to token burning. Only burning the balance of the token holder or the allowance is available.

- **BBF**
  BBF is the leading contract of BBF. It provides additional features essential to the ecosystem, such as Burn and freeze.

Function 1. Contract

It is used to express contracts in container form, including state variables and functions.

Contract	Description
Context	Contract context
Ownable	Function related to contract ownership
Pausable	Function related to contract pause status
Freezable	Function related to contract frozen status
ERC20	Function related to ERC20 standard interface
ERC20Burnable	Function related to token burning
BBF	BBF main function

Function 2. Interface

It is used to define standard functions to implement in the contract.

Interface	Description
IERC20	ERC20 standard interface
IERC20Metadata	ERC20 information interface

Function 3. Library

A contract library that cannot have state variables and does not support inheritance. The library function is called and executed in the context of the calling contract.

Library	Description

Function 4. Variable

It is a variable that expresses the state of the contract. It is used to store information necessary for the contract.

Variable	Description
_owner	Address of contract owner
_paused	Contract pause status
_balances	Token balance table for a specific address
_allowances	Token balance table for a specific address
_totalSupply	Total supply of token
_name	Token name
_symbol	Token symbol
_frozenAccount	A table of whether a specific address is frozen or not

Function 5. Modifier

As a modifier of a function, it is used to ensure that it can be executed only under limited conditions when performing a specific function.

Modifier	Description
onlyOwner	Only the owner of the contract can execute
whenNotPaused	Executable when the contract is not paused
whenPaused	Executable when the contract is paused
whenNotFrozen	Executable when a specific address is not frozen

Function 6. Event

It is a log event that occurs according to the execution of the contract function. It is used to respond to the contract situation in future application use more efficiently.

Event	Description
OwnershipTransferred	Event occurs when transferring the ownership
Paused	Event occurs when pausing the contract
Unpaused	Event occurs when unpausing the contract
Transfer	Event occurs when transferring tokens
Approval	Event occurs when approving a specific address to withdraw
Freeze	Event occurs when freezing an address
Unfreeze	Event occurs when unfreezing an address

Function 7. Function

These are the contract functions that are used to execute features with specific logic required for the contract.

Event	Description
name	Confirm token name
symbol	Confirm token symbol
decimals	Confirm the maximum number of representable decimal places for the token

totalSupply	Confirm the total supply of token
balanceOf	Check the token balance of a specific address
allowance	Confirm the allowance
transfer	Transfer token
approve	Approve other addresses to spend tokens
transferFrom	Transfer tokens that other addresses are approved to spend
increaseAllowance	Increase allowance
decreaseAllowance	Decrease allowance
_transfer	Transfer token(Inner function)
_mint	Mint token(Inner function)
burn	Burn token
_burn	Burn token(Inner function)
burnFrom	Burn tokens that are approved to spend by a specific address
_burnFrom	Burn tokens that are approved to spend by a specific address(Inner function)
_approve	Approve other addresses to spend tokens(Inner function)
transferOwnership	Transfer the contract ownership
renounceOwnership	Renounce the contract owner authority
pause	Pause the contract
unpause	Unpause the contract
isFrozen	Check the frozen status of a specific address
freezeAccount	Freeze a specific account
unfreezeAccount	Unfreeze a specific account
_msgSender	Return the transaction sender
_msgData	Return the transaction call data
_beforeTokenTransfer	Validation check function before transferring tokens

TEST RESULT

Code Coverage

Code coverage is a quantitative index of how much the written test has tested the functionality of the contact code.

There are cases where additional calls are not made to the library and functions implemented in some contracts in the BFF contract.

The coverage index below is the result that reflects the details above:

File Name	Statements	Functions	Lines
BBF.sol	100% (82/83)	100% (41/42)	100% (91/93)

TEST CASE

The table below is a list of actually applied test cases.

Test Case	Result	
Does the token name match it specified at the time of deployment?	PASS	FAIL
Does the token symbol match it specified at the time of deployment?	PASS	FAIL
Does the token decimal match it specified at the time of deployment?	PASS	FAIL
Does the initial supply match it specified at the time of deployment?	PASS	FAIL
Does it allocate the initial supply specified at the time of deployment to the contract deployer?	PASS	FAIL
Are token balances of addresses other than the owner address zero after the deployment?	PASS	FAIL
Does basic token transfer work?	PASS	FAIL
It returns the correct amount of tokens owned by specific addresses.	PASS	FAIL
Does it revert when transferring a token amount that exceeds the balance?	PASS	FAIL
Does it revert when the recipient address is set to 0x0?	PASS	FAIL
Is it possible to approve other addresses to spend tokens on behalf of the owner?	PASS	FAIL
Is it possible to check the allowance?	PASS	FAIL
Is it possible to increase the allowance?	PASS	FAIL
Is it possible to decrease the allowance?	PASS	FAIL
Is it possible to transfer tokens that are approved to spend?	PASS	FAIL
Does it revert if the recipient address is set to 0x0 when transferring tokens approved to spend?	PASS	FAIL
Does it revert if the sender’s balance is insufficient when transferring approved tokens?	PASS	FAIL
Does it revert if the transferring amount exceeds the allowance when transferring approved tokens?	PASS	FAIL
It returns the correct address of the contract owner.	PASS	FAIL
Does it revert if addresses other than the owner attempt to transfer the ownership?	PASS	FAIL
Can the owner transfer the ownership?	PASS	FAIL
Is it possible for the owner to renounce the ownership?	PASS	FAIL

Does it revert if addresses other than the owner renounce the ownership?	PASS	FAIL
Does it revert if it delegates the ownership to 0x0?	PASS	FAIL
Does the token burn function work?	PASS	FAIL
Does it revert if the balance is insufficient when burning tokens?	PASS	FAIL
Does the total supply decrease when burning tokens?	PASS	FAIL
Is it possible to burn approved tokens?	PASS	FAIL
Does it revert if the allowance is insufficient when burning tokens?	PASS	FAIL
Does it revert if the sender’s balance is insufficient when burning approved tokens?	PASS	FAIL
Does it revert if addresses other than the owner attempt to freeze a specific address?	PASS	FAIL
Does it revert if addresses other than the owner attempt to unfreeze frozen addresses?	PASS	FAIL
Can the owner freeze specific addresses?	PASS	FAIL
Can the owner unfreeze specific addresses?	PASS	FAIL
Does it revert when a frozen address attempts to transfer tokens?	PASS	FAIL
Does it revert when a frozen address attempts to transfer approved tokens?	PASS	FAIL
Is it possible to transfer tokens when unfreezing a frozen address?	PASS	FAIL
Is it possible to transfer approved tokens when unfreezing a frozen address?	PASS	FAIL
Does it revert if freezing a frozen address?	PASS	FAIL
Does it revert if unfreezing a non-frozen address?	PASS	FAIL
It can confirm the contract pause status.	PASS	FAIL
The owner can pause the contract.	PASS	FAIL
Does it revert if addresses other than the owner attempt to pause the contract?	PASS	FAIL
The owner can unpause the contract.	PASS	FAIL
Does it revert if addresses other than the owner attempt to unpause the contract?	PASS	FAIL
Does it revert if transfer tokens when the contract is paused?	PASS	FAIL
Does it revert if transfers tokens that are approved to spend when the contract is paused?	PASS	FAIL
Does it revert if unpause the contract when it’s not paused?	PASS	FAIL

VULNERABILITY ANALYSIS

There is no need to modify this contract.

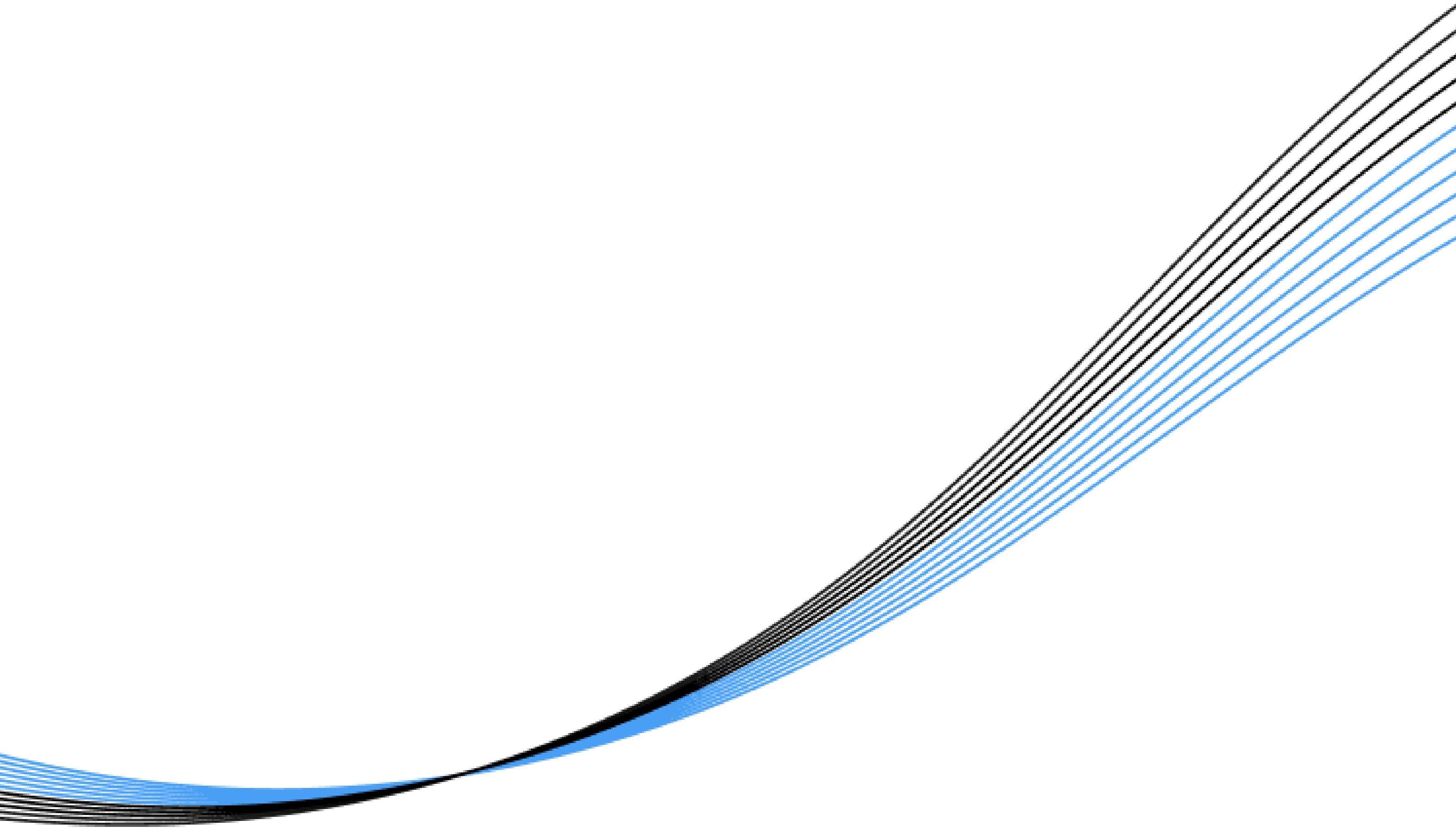
BBF CONTRACT VULNERABILITY ANALYSIS		
● **CRITICAL**	0	No relevant provision
● **HIGH**	0	No relevant provision
● **MEDIUM**	0	No relevant provision
● **LOW**	0	No relevant provision

CONCLUSION

The BFF contract is a contract that includes the freeze and pause function in addition to the ERC-20 standard function. Granting contract owner's authority not only can restrict the token transfer of the entire ecosystem, but it can also freeze specific addresses to pause withdrawals. This contract has added the token burn function that can affect token circulation. By using this function, token holders can burn their tokens and allowance. It also has the pause function, which allows the entire contract to stop functioning in special situations in the swap or token ecosystem.

Declare

The report is based on Hexlant's smart contract security audit results. This report does not guarantee the suitability of the business model, legal regulation, or investment opinion. In addition to the problems described in this report, there may be undiscovered problems, including issues in blockchain network technology or virtual machines. This report is intended for discussion purposes only.



Hexlant.

-

contact@hexlant.com
www.hexlant.com