



SMART CONTRACT SECURITY AUDIT

Bugatti

October, 2021

Website: soken.io

Table of Contents

Table of Contents	2
Disclaimer	3
Procedure	4
Terminology	5
Limitations	5
Token Contract Details for 23.10.2021	6
Audit Details	6
Social Profiles	7
Token Contract Overview	7
Contract Function Details	9
Vulnerabilities checking	13
Security Issues	14
Conclusion	16
Soken Contact Info	17

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 23.10.2021

Contract Name: **Bugatti**

Deployed address: **0x106B5466813de81B3ab644206Ab97A1C02ab0c8D**

Total Supply: **21,000**

Token Tracker: **BGT**

Decimals: **9**

Token holders: **1,261**

Transactions count: **4,838**

Top 100 holders dominance: **99.13%**

Audit Details



Project Name: **Bugatti**

Language: **Solidity**

Compiler version: **v.0.6.12**

Blockchain: **HECO Chain**

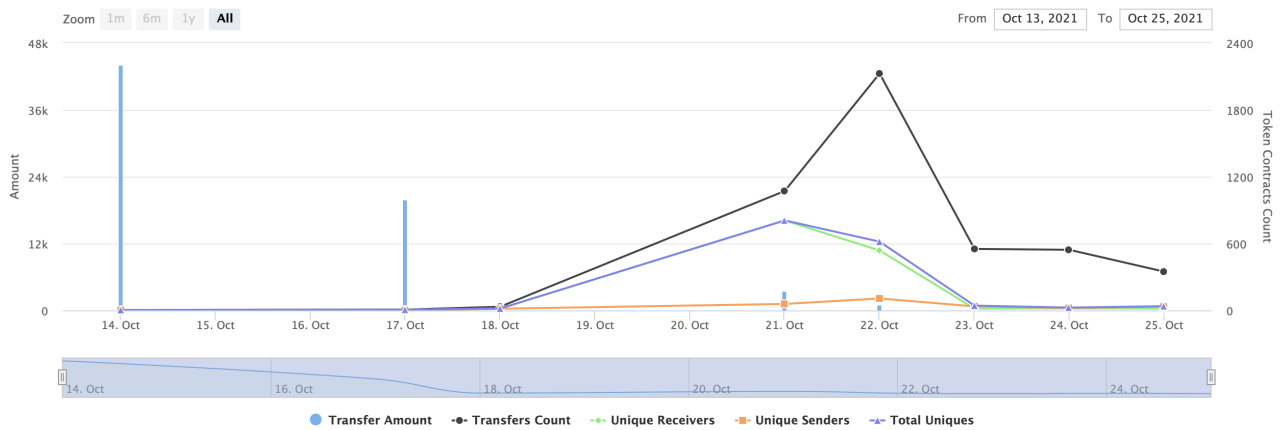
Social Profiles

Project Website: <http://bugattinft.info>

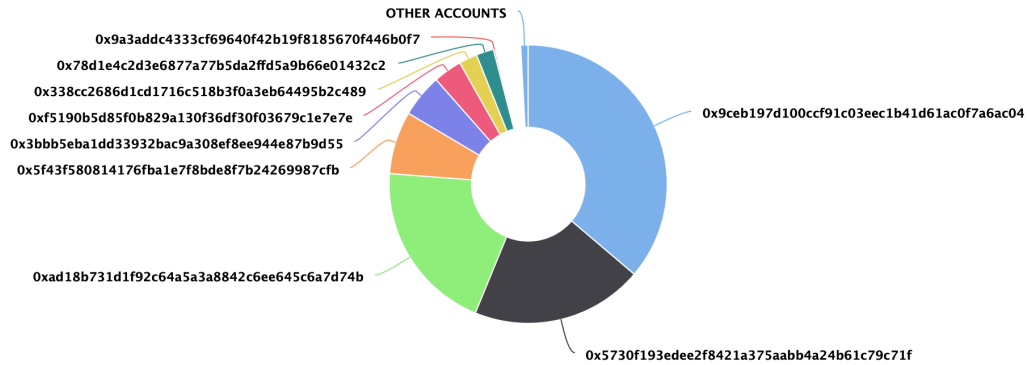
Project Twitter: https://twitter.com/bugatti_nft

Project Facebook: <https://www.facebook.com/Bugatti-NFT>

Token Contract Overview



BGT Top 10 Holders



BGT Token Distribution

Rank	Address	Quantity (Token)	Percentage
1	0x9ceb197d100ccf91c03eec1b41d61ac0f7a6ac04	7,604.577052224	36.2123%
2	0x5730f193edee2f8421a375aabb4a24b61c79c71f	4,200	20.0000%
3	0xad18b731d1f92c64a5a3a8842c6ee645c6a7d74b	4,200	20.0000%
4	0x5f43f580814176fba1e7f8bde8f7b24269987cfb	1,530.763941544	7.2894%
5	0x3bbb5eba1dd33932bac9a308ef8ee944e87b9d55	1,049.001172381	4.9952%
6	0xf5190b5d85f0b829a130f36df30f03679c1e7e7e	700.532634625	3.3359%
7	0x338cc2686d1cd1716c518b3f0a3eb64495b2c489	444.03696462	2.1145%
8	0x78d1e4c2d3e6877a77b5da2ffd5a9b66e01432c2	427.969855983	2.0380%
9	0x9a3addc4333cf69640f42b19f8185670f446b0f7	40.305841913	0.1919%
10	0x0000000000000000000000000000000000000000	28.743938436	0.1369%

Contract Function Details

- + [Int] IERC20.sol
 - [Ext] totalSupply
 - [Ext] balanceOf
 - [Ext] transfer #
 - [Ext] allowance #
 - [Ext] approve
 - [Ext] transferFrom #
- + [Lib] SafeMath
 - [Int] add
 - [Int] sub
 - [Int] sub
 - [Int] mul
 - [Int] div
 - [Int] div
 - [Int] mod
 - [Int] mod
 - [Int] _msgSender
 - [Int] _msgData
- + [Lib] Address.sol
 - [Int] isContract
 - [Int] sendValue #
 - [Int] functionCall #
 - [Int] functionCall #
 - [Int] functionCallWithValue #
 - [Int] functionCallWithValue #
 - [Int] functionStaticCall #
 - [Int] functionStaticCall #
 - [Int] _verifyCallResult #
- + Ownable.sol (Context)
 - [Pub] owner
 - [Pub] renounceOwnership #
 - modifiers: onlyOwner
 - [Pub] transferOwnership #
 - modifiers: onlyOwner
 - [Pub] geUnlockTime
 - [Pub] lock
 - [Pub] unlock

+ [Int] IUniswapV2Factory

- [Ext] feeTo
- [Ext] feeToSetter
- [Ext] getPair
- [Ext] allPairs
- [Ext] allPairsLength
- [Ext] createPair #
- [Ext] setFeeTo #
- [Ext] setFeeToSetter #

+ [Int] IUniswapV2Pair

- [Ext] name
- [Ext] symbol
- [Ext] decimals
- [Ext] totalSupply
- [Ext] balanceOf
- [Ext] allowance
- [Ext] approve #
- [Ext] transfer #
- [Ext] transferFrom #
- [Ext] DOMAIN_SEPARATOR
- [Ext] PERMIT_TYPEHASH
- [Ext] nonces
- [Ext] permit #
- [Ext] _LIQUIDITY
- [Ext] factory
- [Ext] token0
- [Ext] token1
- [Ext] getReserves
- [Ext] price0CumulativeLast
- [Ext] price1CumulativeLast
- [Ext] kLast
- [Ext] mint
- [Ext] burn #
- [Ext] swap #
- [Ext] skim #
- [Ext] sync #
- [Ext] initialize #

+ [Int] IUniswapV2Router01

- [Ext] factory
- [Ext] WETH
- [Ext] addLiquidity #
- [Ext] addLiquidityETH (\$)

- [Ext] removeLiquidity #
- [Ext] removeLiquidityETH #
- [Ext] removeLiquidityWithPermit #
- [Ext] removeLiquidityETHWithPermit #
- [Ext] swapExactTokensForTokens #
- [Ext] swapTokensForExactTokens #
- [Ext] swapExactETHForTokens (\$)
- [Ext] swapTokensForExactETH #
- [Ext] swapExactTokensForETH #
- [Ext] swapETHForExactTokens (\$)
- [Ext] quote
- [Ext] getAmountOut
- [Ext] getAmountIn
- [Ext] getAmountsOut
- [Ext] getAmountsIn

- + [Int] IUniswapV2Router02 (IUniswapV2Router01)
 - [Ext] removeLiquidityETHSupportingFeeOnTransferTokens #
 - [Ext] removeLiquidityETHWithPermitSupportingFeeOnTransferTokens #
 - [Ext] swapExactTokensForTokensSupportingFeeOnTransferTokens #
 - [Ext] swapExactETHForTokensSupportingFeeOnTransferTokens (\$)
 - [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #

- + [Int] IWrap
 - [Ext] withdraw

- + Bugatti is Context, IERC20, Ownable
 - [Pub] setDev
 - [Pub] setFomo
 - [Pub] setWrap
 - [Pub] name
 - [Pub] symbol
 - [Pub] decimals
 - [Pub] totalSupply
 - [Pub] balanceOf
 - [Pub] transfer #
 - [Pub] allowance
 - [Pub] approve #
 - [Pub] transferFrom #
 - [Pub] increaseAllowance
 - [Pub] decreaseAllowance
 - [Pub] name
 - [Pub] symbol
 - [Pub] decimals
 - [Pub] totalSupply

- [Pub] balanceOf
- [Pub] transfer #
- [Pub] allowance
- [Pub] approve #
- [Pub] transferFrom #
- [Pub] increaseAllowance
- [Pub] decreaseAllowance
- [Pub] isExcludedFromReward
- [Pub] deliver
- [Pub] tokenFromReflection
- [Pub] excludeFromReward
- [Ext] includeInReward
- [Pub] excludeFromFee
- [Pub] includeInFee
- [Ext] setMaxTxPercent
- [Pub] setSwapAndLiquifyEnabled
- [Prv] _reflectFee
- [Prv] _getTValues
- [Prv] _getRValues
- [Prv] _getRate
- [Prv] _getCurrentSupply
- [Prv] _takeTax
- [Prv] removeAllFee
- [Prv] restoreAllFee
- [Pub] isExcludedFromFee
- [Prv] _approve
- [Prv] _transfer
- [Prv] swapAndLiquify
- [Prv] swapTokensForUsdt
- [Prv] swapTokensForEth
- [Prv] addLiquidityUsdt
- [Prv] addLiquidity
- [Prv] _tokenTransfer
- [Prv] _transferStandard
- [Prv] _transferToExcluded
- [Prv] _transferFromExcluded
- [Prv] _transferBothExcluded

(\$) = payable function

= non-constant function

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	Low-severity issues
Outdated Compiler 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

Security Issues

1) Owner privileges:

The contract contains ownership functionality and ownership is not renounced which allows the creator or current owner to modify contract behavior (for example, disable selling or mint new tokens).

2) Out of Gas issue:

The function `includeInReward()` uses the loop to find and remove addresses from the `_excluded` list. Function will be aborted with `OUT_OF_GAS` exception if there will be a long excluded addresses list.

```
function includeInReward(address account) external onlyOwner() {
    require(!_isExcluded[account], "Account is already excluded");
    for (uint256 i = 0; i < _excluded.length; i++) {
        if (_excluded[i] == account) {
            _excluded[i] = _excluded[_excluded.length - 1];
            _tOwned[account] = 0;
            _isExcluded[account] = false;
            _excluded.pop();
            break;
        }
    }
}
```

3) Out of Gas issue:

The function `_getCurrentSupply` also uses the loop for evaluating total supply. It also could be aborted with `OUT_OF_GAS` exception if there will be a long excluded addresses list.

```
function _getCurrentSupply() private view returns(uint256, uint256) {
    uint256 rSupply = _rTotal;
    uint256 tSupply = _tTotal;
    for (uint256 i = 0; i < _excluded.length; i++) {
        if (_rOwned[_excluded[i]] > rSupply || _tOwned[_excluded[i]] > tSupply) return (_rTotal, _tTotal);
        rSupply = rSupply.sub(_rOwned[_excluded[i]], "sub rSupply");
        tSupply = tSupply.sub(_tOwned[_excluded[i]], "sub tSupply");
    }
    if (rSupply < _rTotal.div(_tTotal)) return (_rTotal, _tTotal);
    return (rSupply, tSupply);
}
```

4) Volatile Code:

The return values of functions

swapExactTokensForETHSupportingFeeOnTransferTokens and *addLiquidityETH* are not properly handled.

Recommendation:

We recommend using variables to receive the return value of the functions mentioned above and handle both success and failure cases if needed by the business logic.

Conclusion

Low-severity issues exist within smart contracts. Smart contracts are free from any critical or high-severity 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

