HackSafe

Smart Contract Security Audit Report

Bezant

April **2022**

Security Status

★★★★⯪

www.hacksafe.io

Audit Details

Audited project
Bezant

Deployer address
0x67eEd7125ca2b9d1859C4d824a675bD1fa45256d

Client contacts
Bezant team

Blockchain
Ethereum

Website
Not Provided by the Bezant team

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.

Background

HeckSafe was commissioned by Bezant to perform an audit of smart contracts:

- https://etherscan.io/address/0xe1aee98495365fc179699c1bb3e761fa716bee62#code

Contract Details

Token contract details for 21.04.2022

Contract name	: BezantToken
Contract address	: 0xE1Aee98495365fc179699C1bB3E761FA716beE62
Total supply	: 999,999,820.000000000000000002
Token Ticker	: BZNT
Decimals	: 18
Token Holders	: 3,291
Transactions count	: 32,983
Contract deployer address	: 0x67eEd7125ca2b9d1859C4d824a675bD1fa45256d
Owner address	: 0x67eEd7125ca2b9d1859C4d824a675bD1fa45256d

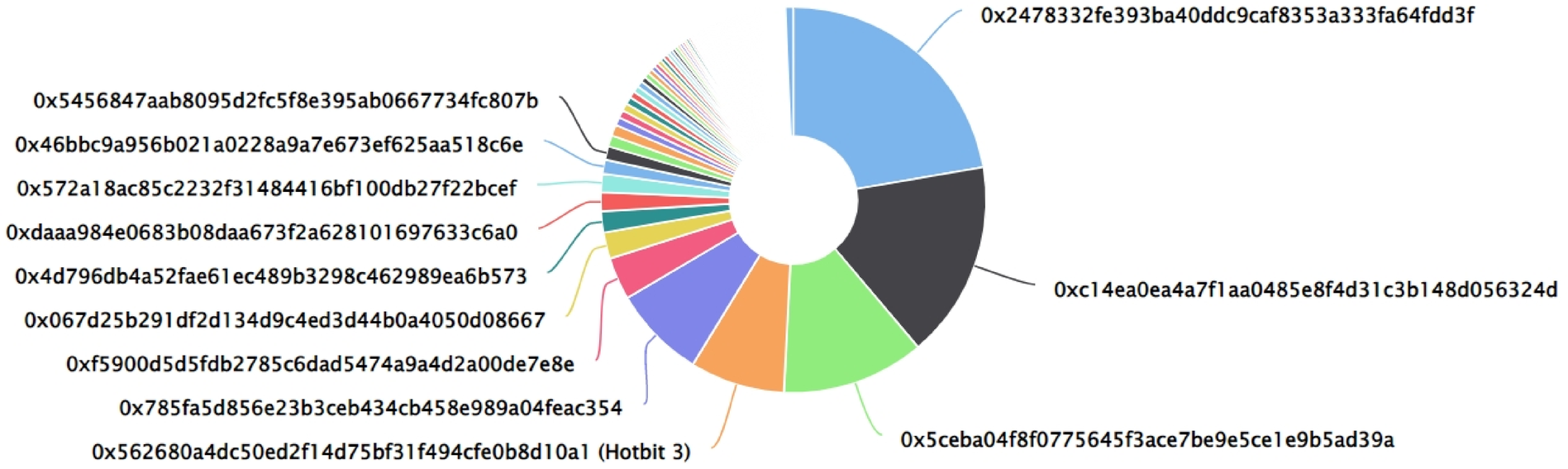
BezantToken Token Distribution

The top 500 holders collectively own 99.33% (993,324,186.54 Tokens) of BezantToken

Token Total Supply: 999,999,820.00 Token | Total Token Holders: 3,291

BezantToken Top 500 Token Holders

Source: Etherscan.io



BezantToken Top 10 Token Holders

(A total of 771,882,343.42 tokens held by the top 10 accounts from the total supply of 999,999,820.00 token)

Rank	Address	Quantity (Token)	Percentage
1	0x2478332fe393ba40ddc9caf8353a333fa64fdd3f	222,784,464.5	22.2785%
2	0xc14ea0ea4a7f1aa0485e8f4d31c3b148d056324d	165,158,895.54124158286933318	16.5159%
3	0x5ceba04f8f0775645f3ace7be9e5ce1e9b5ad39a	120,000,000	12.0000%
4	Hotbit 3	79,643,702.972991858716608281	7.9644%
5	0x785fa5d856e23b3ceb434cb458e989a04feac354	77,810,229.24895711	7.7810%
6	0xf5900d5d5fdb2785c6dad5474a9a4d2a00de7e8e	35,488,558	3.5489%
7	0x067d25b291df2d134d9c4ed3d44b0a4050d08667	22,099,600	2.2100%
8	0x4d796db4a52fae61ec489b3298c462989ea6b573	17,634,529.91926096	1.7635%
9	0xdaaa984e0683b08daa673f2a628101697633c6a0	15,762,363.23387347	1.5762%
10	0x572a18ac85c2232f31484416bf100db27f22bcef	15,500,000	1.5500%

Contract functions details

+ Migrations
    -[Pub] Migrations
    -[Pub] transferOwnership
      -modifiers: onlyOwner

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

+ [Int] tokenRecipient
    -[Pub] receiveApproval

+ BezantERC20Base
    -[Pub] BezantERC20Base #
    -[Int] _transfer #
    -[Pub] transfer #
    -[Pub] transferFrom #
    -[Pub] approve #
    -[Pub] approveAndCall #
    -[Pub] burn #
    -[Pub] burnFrom

+ BezantToken (Migrations, BezantERC20Base)
    -[Pub] BezantToken
      -modifiers: onlyOwner, BezantERC20Base
    -[Int] _transfer #
    -[Pub] freezeAccountForOwner #
      -modifiers: onlyOwner
    -[Pub] setManagementContractAddress #
      -modifiers: onlyOwner
    -[Pub] freezeAccountForContract #

Issues Checking Status

No.	Title	Status
1.	Unlocked Compiler Version	Low issue
2.	Missing Input Validation	Medium issue
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

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

One medium severity issue found.

1. Missing input validation

- **Description**

  The given input is missing the check for a non-zero address.

- **Location**

  line no.18

- **Recommendation**

  We advise adding the check for the passed-in values to prevent unexpected errors as below:

  Require(address(0) != _new, “_new initialize to zero address”);

Low Severity Issues

One low severity issue found.

1. Scoping and Declarations.

Unused function.

- **Description**

  The contract utilizes an unlocked compiler version. An unlocked compiler version in the contract's source code permits the user to compile it at or above a particular version. This, in turn, leads to differences in the generated bytecode between compilations due to differing compiler version numbers. This can lead to ambiguity when debugging as compiler-specific bugs may occur in the codebase that would be difficult to identify over a span of multiple compiler versions rather than a specific one.

- **Recommendation**

  It is advisable that the compiler version is alternatively locked at the lowest version possible so that the contract can be compiled. For example, for version >=0.4.17 the contract should contain the following line:

  pragma solidity 0.4.17;

Owner Privileges

Owner Privileges (in the period when the owner is not renounced) :

- Bezant Contract:
    - Owner can transfer ownership.
    - Owner can set name of token
    - Owner can freeze account for transferring tokens.
    - Owner can set management contract address.
    - Owner can freeze account for contract.

Conclusion

Smart contract contains low and medium 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.