TechRate
September, 2022

SMART CONTRACTS SECURITY AUDIT REPORT

Techrate_audits Techrate Techrate1

Audit Details

Audited project

EHIVE

Deployer address

0x31e180e06D771dbAfa3D6Eea452195Ad1020fbDb

Client contacts:

EHIVE team

Blockchain

Ethereum

Project website:

https://ethereumhive.com

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 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) (TechRate) owe no duty of care towards you or any other person, nor does TechRate 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 TechRate 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, TechRate hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against TechRate, 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

TechRate was commissioned by EHIVE to perform an audit of smart contracts:

https://etherscan.io/address/0x4ae2cd1f5b8806a973953b76f9ce6d5fab9cdcfd#code

The purpose of the audit was to achieve the following:

- Ensure that the smart contract functions as intended.
- Identify potential security issues with the smart contract.

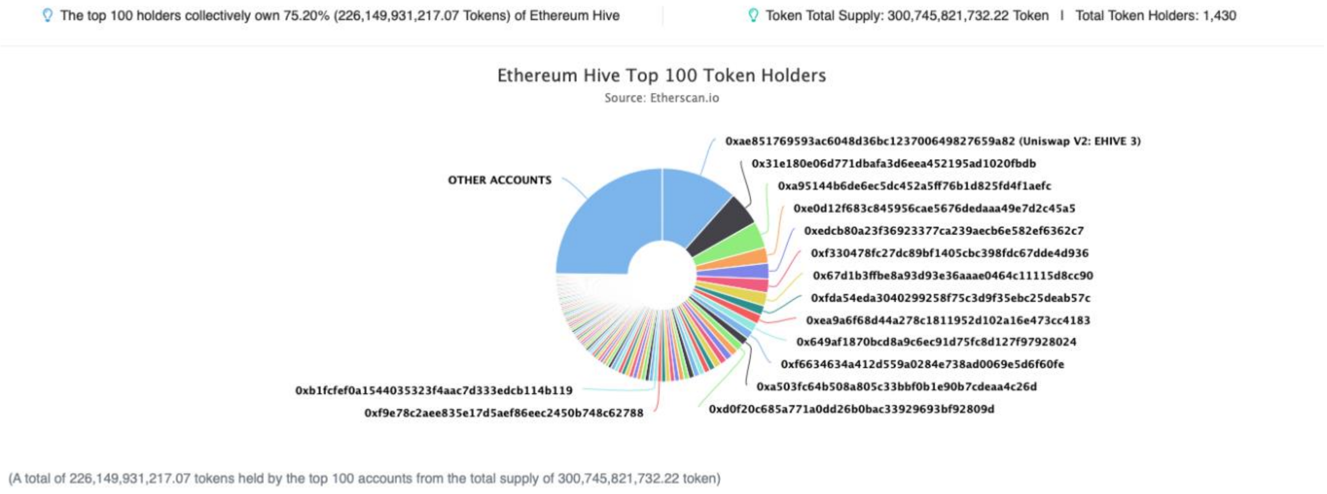
The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Contracts Details

Token contract details for 13.09.2022

Contract name	EHIVE
Contract address	0x4Ae2Cd1F5B8806a973953B76f9Ce6d5FAB9cdcfd
Total supply	300,745,821,732.224613831642812974
Token ticker	EHIVE
Decimals	18
Token holders	1,430
Transactions count	13,827
Top 100 holders dominance	75.20%
Total fees	6
Amount of validators	1
Max transaction amount	2000000000000000000000000000
Max wallet	5000000000000000000000000000
Contract deployer address	0x31e180e06D771dbAfa3D6Eea452195Ad1020fbDb
Owner address	0x31e180e06d771dbafa3d6eea452195ad1020fbdb

EHIVE Token Distribution



The top 100 holders collectively own 75.20% (226,149,931,217.07 Tokens) of Ethereum Hive

Token Total Supply: 300,745,821,732.22 Token | Total Token Holders: 1,430

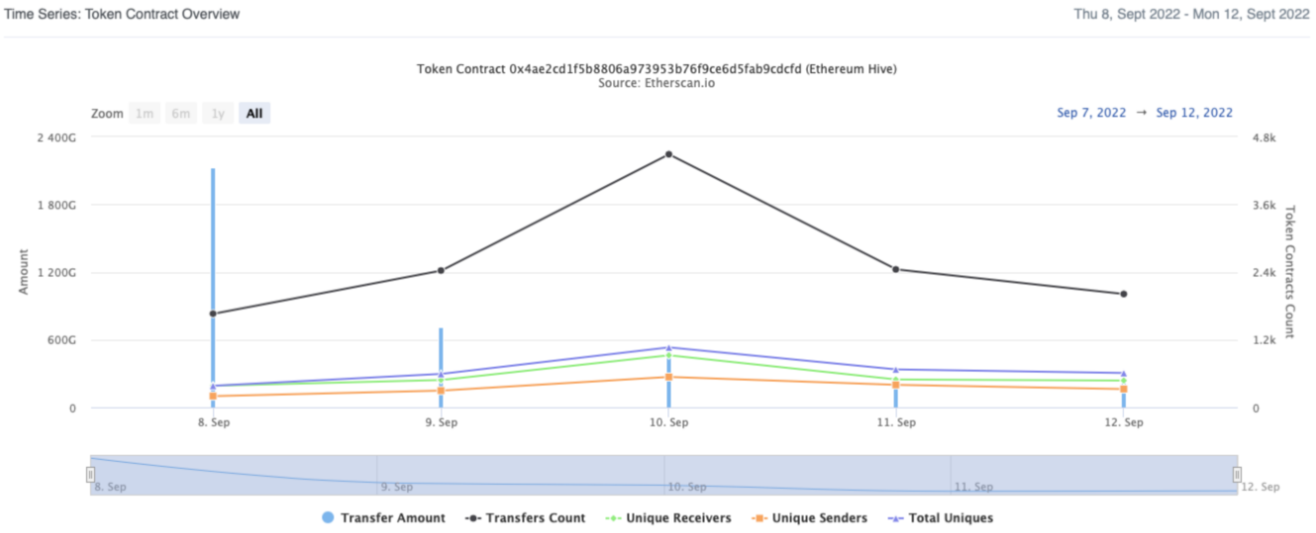
Ethereum Hive Top 100 Token Holders

Source: Etherscan.io

0xae851769593ac6048d36bc123700649827659a82 (Uniswap V2: EHIVE 3)
OTHER ACCOUNTS
0x31e180e06d771dbafa3d6eea452195ad1020fbdb
0xa95144b6de6ec5dc452a5ff76b1d825fd4f1aefc
0xe0d12f683c845956cae5676dedaaa49e7d2c45a5
0xedcb80a23f36923377ca239aecb6e582ef6362c7
0xf330478fc27dc89bf1405cbc398fdc67dde4d936
0x67d1b3ffbe8a93d93e36aaae0464c11115d8cc90
0xfda54eda3040299258f75c3d9f35ebc25deab57c
0xea9a6f68d44a278c1811952d102a16e473cc4183
0x649af1870bcd8a9c6ec91d75fc8d127f97928024
0xf6634634a412d559a0284e738ad0069e5d6f60fe
0xa503fc64b508a805c33bbf0b1e90b7cdeaa4c26d
0xb1fcfef0a1544035323f4aac7d333edcb114b119
0xd0f20c685a771a0dd26b0bac33929693bf92809d
0xf9e78c2aee835e17d5aef86eec2450b748c62788

(A total of 226,149,931,217.07 tokens held by the top 100 accounts from the total supply of 300,745,821,732.22 token)

EHIVE Contract Interaction Details



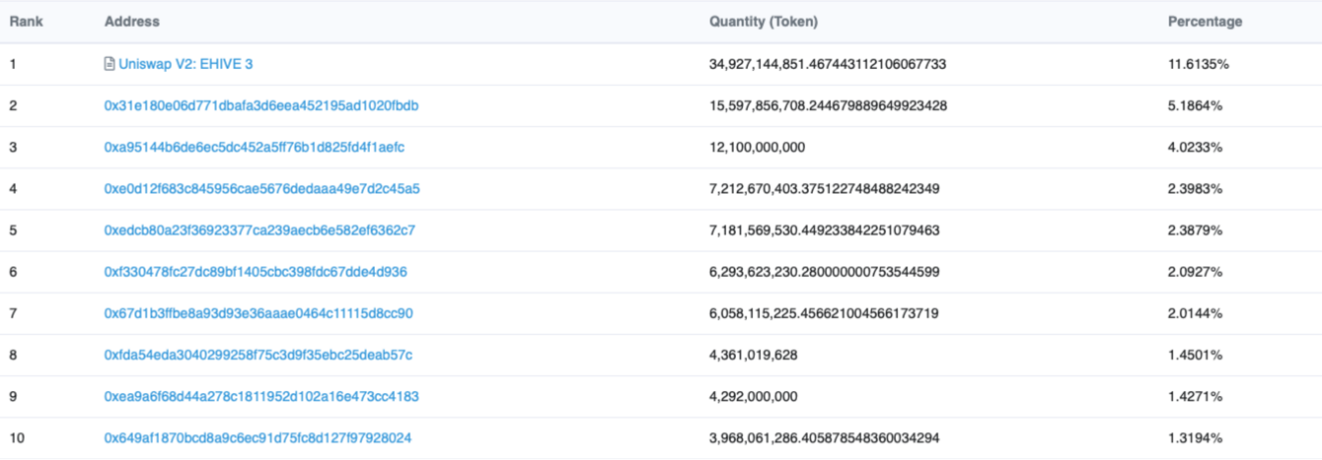
Time Series: Token Contract Overview

Thu 8, Sept 2022 - Mon 12, Sept 2022

Token Contract 0x4ae2cd1f5b8806a973953b76f9ce6d5fab9cdcfd (Ethereum Hive)

Source: Etherscan.io

EHIVE Top 10 Token Holders



Rank	Address	Quantity (Token)	Percentage
1	Uniswap V2: EHIVE 3	34,927,144,851.467443112106067733	11.6135%
2	0x31e180e06d771dbafa3d6eea452195ad1020fbdb	15,597,856,708.244679889649923428	5.1864%
3	0xa95144b6de6ec5dc452a5ff76b1d825fd4f1aefc	12,100,000,000	4.0233%
4	0xe0d12f683c845956cae5676dedaaa49e7d2c45a5	7,212,670,403.375122748488242349	2.3983%
5	0xedcb80a23f36923377ca239aecb6e582ef6362c7	7,181,569,530.449233842251079463	2.3879%
6	0xf330478fc27dc89bf1405cbc398fdc67dde4d936	6,293,623,230.280000000753544599	2.0927%
7	0x67d1b3ffbe8a93d93e36aaae0464c11115d8cc90	6,058,115,225.456621004566173719	2.0144%
8	0xfda54eda3040299258f75c3d9f35ebc25deab57c	4,361,019,628	1.4501%
9	0xea9a6f68d44a278c1811952d102a16e473cc4183	4,292,000,000	1.4271%
10	0x649af1870bcd8a9c6ec91d75fc8d127f97928024	3,968,061,286.405878548360034294	1.3194%

Contract functions details

```
 +  Context
   - [Int] _msgSender
   - [Int] _msgData

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

 + [Int] IERC20Metadata (IERC20)
   - [Ext] name
   - [Ext] symbol
   - [Ext] decimals

 +  ERC20 (Context, IERC20, IERC20Metadata)
   - [Pub] <Constructor> #
   - [Pub] name
   - [Pub] symbol
   - [Pub] decimals
   - [Pub] totalSupply
   - [Pub] balanceOf
   - [Pub] transfer #
   - [Pub] allowance
   - [Pub] approve #
   - [Pub] transferFrom #
   - [Pub] increaseAllowance #
   - [Pub] decreaseAllowance #
   - [Int] _transfer #
   - [Int] _mint #
   - [Int] _burn #
   - [Int] _approve #
   - [Int] _spendAllowance #
   - [Int] _beforeTokenTransfer #
   - [Int] _afterTokenTransfer #

 + [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] MINIMUM_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 #

 +  Ownable (Context)
    - [Pub] <Constructor> #
    - [Pub] owner
    - [Pub] renounceOwnership #
       - modifiers: onlyOwner
    - [Pub] transferOwnership #
       - modifiers: onlyOwner
    - [Int] _transferOwnership #

 + [Lib] SafeMath
    - [Int] tryAdd
    - [Int] trySub
    - [Int] tryMul
    - [Int] tryDiv
    - [Int] tryMod
    - [Int] add
    - [Int] sub
    - [Int] mul
    - [Int] div
    - [Int] mod
    - [Int] sub
    - [Int] div
    - [Int] mod

 +  EHIVE (ERC20, Ownable)
    - [Pub] <Constructor> ($)
    - modifiers: ERC20
  - [Ext] startTrading #
    - modifiers: teamOROwner
  - [Ext] removeLimits #
    - modifiers: teamOROwner
  - [Pub] excludeFromFees #
    - modifiers: teamOROwner
  - [Ext] updateFees #
    - modifiers: onlyOwner
  - [Ext] updateFeeReceiver #
    - modifiers: teamOROwner
  - [Ext] updateSwapTokensThreshold #
    - modifiers: teamOROwner
  - [Ext] isExcludedFromFees
  - [Int] _transfer #
  - [Int] _swapTokensForEth #
  - [Int] _addLiquidity #
  - [Int] swapBack #
  - [Ext] withdrawContractETH #
  - [Ext] forceSwap #
    - modifiers: teamOROwner
  - [Pub] isStaking
  - [Pub] userStaked
  - [Pub] userClaimHistory
  - [Pub] userEarned
  - [Prv] _userEarned
  - [Ext] stake #
    - modifiers: isStakingEnabled
  - [Ext] claim #
    - modifiers: isStakingEnabled
  - [Ext] unstake #
  - [Ext] createValidator #
    - modifiers: teamOROwner
  - [Pub] amountOfValidators
  - [Ext] setStakingState #
    - modifiers: teamOROwner
  - [Ext] <Fallback> ($)


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

Issues Checking Status

	Issue description	Checking status
1.	**Compiler errors.**	Passed
2.	**Race conditions and Reentrancy. Cross-function race conditions.**	Passed
3.	**Possible delays in data delivery.**	Passed
4.	**Oracle calls.**	Passed
5.	**Front running.**	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.	**The impact of the exchange rate on the logic.**	Passed
13.	**Private user data leaks.**	Passed
14.	**Malicious Event log.**	Passed
15.	**Scoping and Declarations.**	Passed
16.	**Uninitialized storage pointers.**	Passed
17.	**Arithmetic accuracy.**	Passed
18.	**Design Logic.**	Passed
19.	**Cross-function race conditions.**	Passed
20.	**Safe Open Zeppelin contracts implementation and usage.**	Passed
21.	**Fallback function security.**	Passed

Security Issues

✓ High Severity Issues

No high severity issues found.

✓ Medium Severity Issues

No medium severity issues found.

✓ Low Severity Issues

No low severity issues found.

Notes:

- Old owner is not removed from exemptions after transferring ownership.
- Claim function resets staking start.
- Rewards are available until maxSupply is reached.

Owner privileges (In the period when the owner is not renounced)

- Owner can change fees.
- Owner and _swapFeeReceiver can start trading.
- Owner and _swapFeeReceiver can disable limitsInEffect.
- Owner and _swapFeeReceiver can exclude addresses from fees.
- Owner and _swapFeeReceiver can change _swapFeeReceiver.
- Owner and _swapFeeReceiver can change swapTokensThreshold.
- Owner and _swapFeeReceiver can manually swap.
- Owner and _swapFeeReceiver can create validators.
- Owner and _swapFeeReceiver can enable/disable staking.
- Anybody can withdraw ETHs to _swapFeeReceiver address.

Testnet deployment

Contracts Description Table

Contract	Type	Bases		
└	**Function Name**	**Visibility**	**Mutability**	**Modifiers**
ERC20	Implementation	Context, IERC20, IERC20Metadata		
└	transfer	Public ❗	🛑	NO❗
└	approve	Public ❗	🛑	NO❗
└	transferFrom	Public ❗	🛑	NO❗
EHIVE	Implementation	ERC20, Ownable		
└	startTrading	External ❗	🛑	teamOROwner
└	removeLimits	External ❗	🛑	teamOROwner
└	excludeFromFees	Public ❗	🛑	teamOROwner
└	updateFees	External ❗	🛑	onlyOwner
└	updateFeeReceiver	External ❗	🛑	teamOROwner
└	updateSwapTokensThreshold	External ❗	🛑	teamOROwner
└	withdrawContractETH	External ❗	🛑	NO❗
└	stake	External ❗	🛑	isStakingEnabled
└	claim	External ❗	🛑	isStakingEnabled
└	unstake	External ❗	🛑	NO❗
└	createValidator	External ❗	🛑	teamOROwner
└	setStakingState	External ❗	🛑	teamOROwner

Legend

Symbol	Meaning
🛑	Function can modify state
💵	Function is payable

* Contract’s time setting may be change to reach better testing performance.

Conclusion

Smart contracts do not contain high severity issues! Liquidity pair contract's security is not checked due to out of scope. The further transfers and operations with the funds raise are not related to this particular contract. Liquidity is adding in wrong proportion.

Liquidity locking details are provided by the team:
https://app.unicrypt.network/amm/uni-v2/pair/0xae851769593ac6048d36bc123700649827659a82

Security score: 87.

TechRate 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.