TechRate
September, 2022

SMART CONTRACTS SECURITY AUDIT REPORT

Techrate_audits Techrate Techrate1

Audit Details

Audited project

White Ethereum

Deployer address

0x37147608Ec35dDd03F9A0f218F90680cE972C79d

Client contacts:

twitter.com/whiteethtoken

Blockchain

Ethereum

Project website:

https://whiteethereum.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 White Ethereum to perform an audit of smart contracts:

- https://etherscan.io/address/0xfe4beb9217cddf2422d4bd65449b76d807b30fe1
- https://etherscan.io/address/0xbbb3744f6232cefd5f53395e1081f03acbab6d36
- https://etherscan.io/address/0x9a19e06322d1fe9bedbd3f6555803de2713c1762
- https://etherscan.io/address/0x2fd6f383290f3640100119cbe175f0691f86a4e4
- https://etherscan.io/address/0xbfd02a8b75cc2cc4f6de06b0c2340bd6f8862a49
- https://etherscan.io/address/0xf9550ee7acdd3e5a6b932a920a345a56069075dd
- https://etherscan.io/address/0x92eb03d795fd917e289f2e53301f7df5e2526de1
- https://etherscan.io/address/0x5e6f20de931848523b2a91f0330107a92e7e0a22

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.

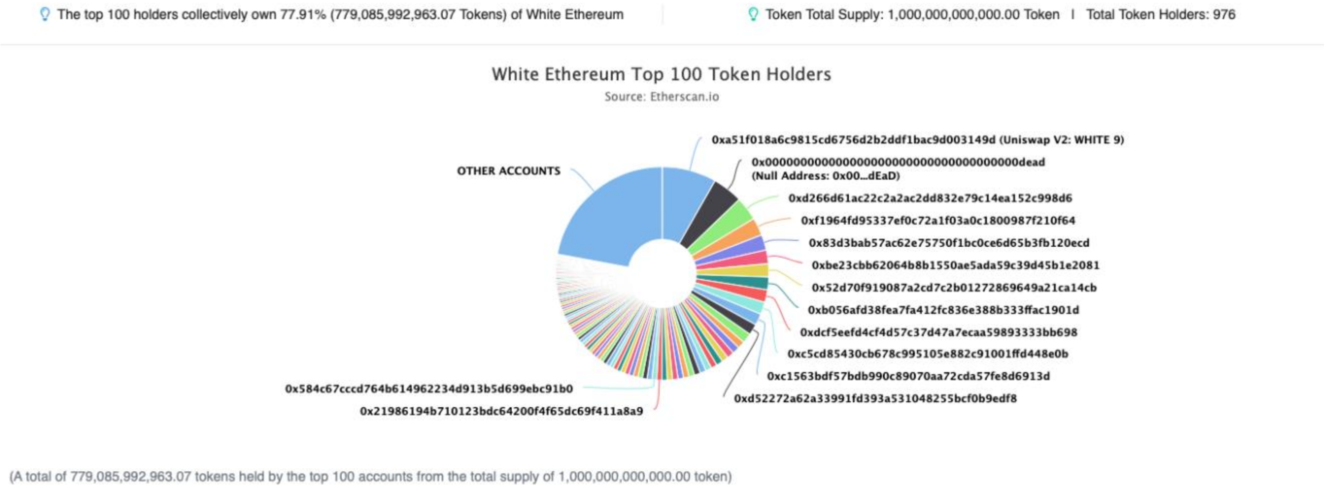
The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Contracts Details

Token contract details for 18.09.2022

Contract name	White Ethereum
Contract address	0xFe4BEb9217cdDf2422d4bd65449b76d807b30fe1
Total supply	1,000,000,000,000
Token ticker	WHITE
Decimals	9
Token holders	976
Transactions count	11,777
Top 100 holders dominance	77.91%
Contract deployer address	0x37147608Ec35dDd03F9A0f218F90680cE972C79d
Owner address	0x0000000000000000000000000000000000000000

White Ethereum Token Distribution



The top 100 holders collectively own 77.91% (779,085,992,963.07 Tokens) of White Ethereum

Token Total Supply: 1,000,000,000,000.00 Token | Total Token Holders: 976

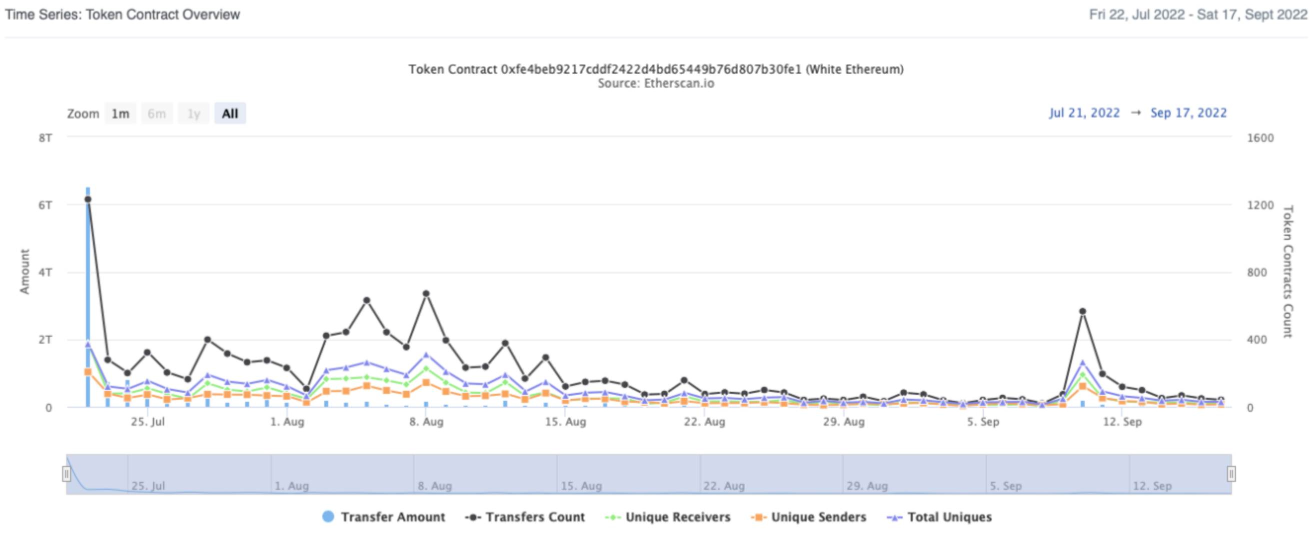
White Ethereum Top 100 Token Holders

Source: Etherscan.io

0xa51f018a6c9815cd6756d2b2ddf1bac9d003149d (Uniswap V2: WHITE 9)
0x000000000000000000000000000000000000dead (Null Address: 0x00...dEaD)
OTHER ACCOUNTS
0xd266d61ac22c2a2ac2dd832e79c14ea152c998d6
0xf1964fd95337ef0c72a1f03a0c1800987f210f64
0x83d3bab57ac62e75750f1bc0ce6d65b3fb120ecd
0xbe23cbb62064b8b1550ae5ada59c39d45b1e2081
0x52d70f919087a2cd7c2b01272869649a21ca14cb
0xb056afd38fea7fa412fc836e388b333ffac1901d
0xdcf5eefd4cf4d57c37d47a7ecaa59893333bb698
0xc5cd85430cb678c995105e882c91001ffd448e0b
0xc1563bdf57bdb990c89070aa72cda57fe8d6913d
0x584c67cccd764b614962234d913b5d699ebc91b0
0xd52272a62a33991fd393a531048255bcf0b9edf8
0x21986194b710123bdc64200f4f65dc69f411a8a9

(A total of 779,085,992,963.07 tokens held by the top 100 accounts from the total supply of 1,000,000,000,000.00 token)

White Ethereum Contract Interaction Details



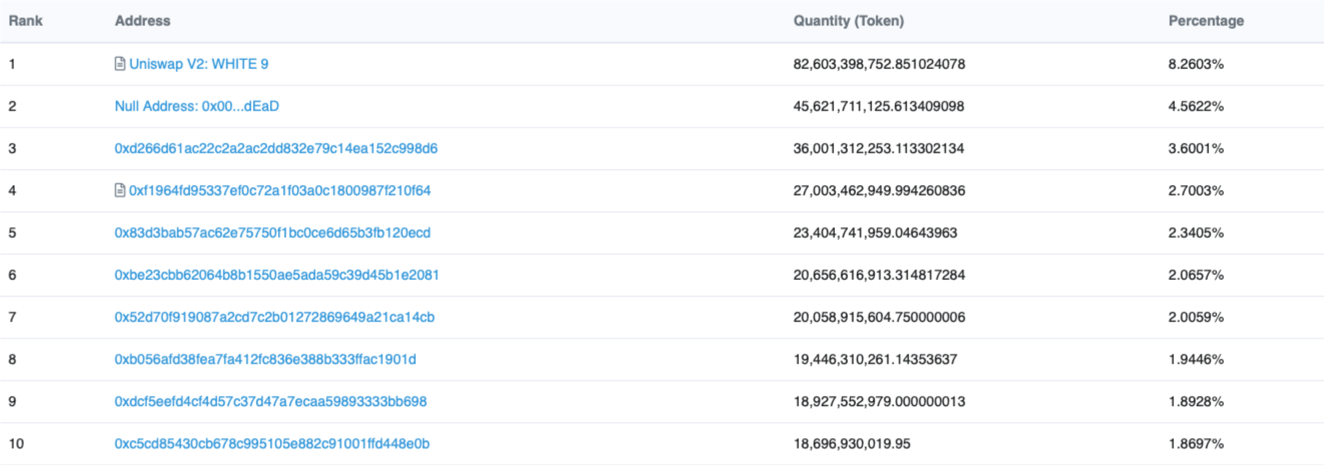
Time Series: Token Contract Overview

Fri 22, Jul 2022 - Sat 17, Sept 2022

Token Contract 0xfe4beb9217cddf2422d4bd65449b76d807b30fe1 (White Ethereum)

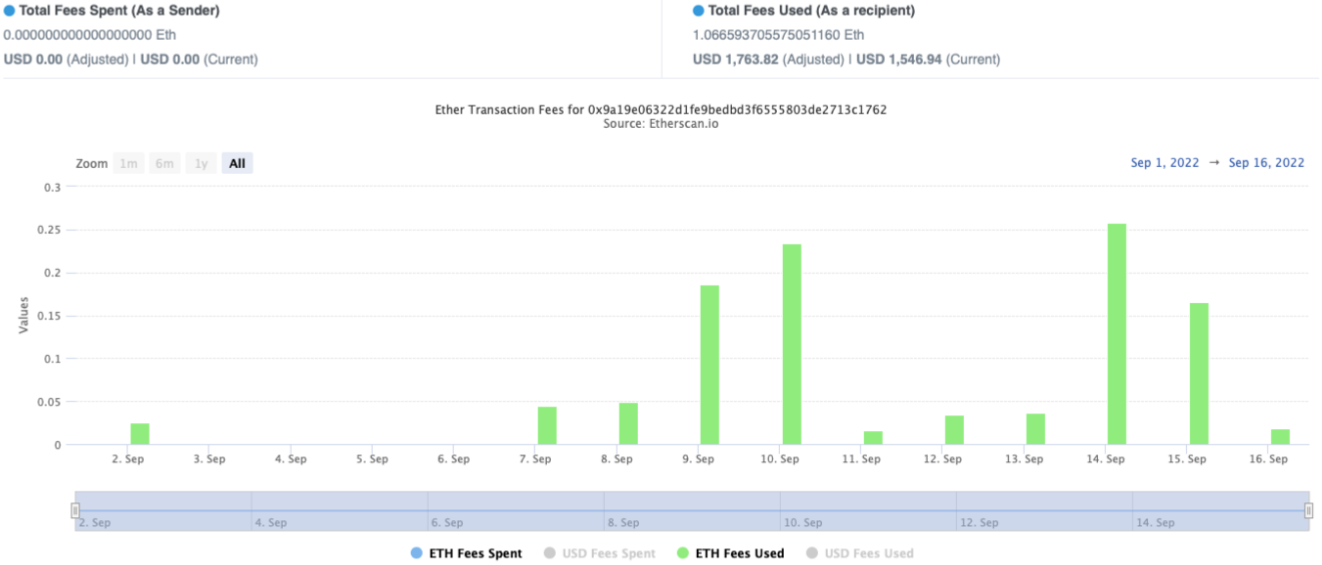
Source: Etherscan.io

White Ethereum Top 10 Token Holders



Rank	Address	Quantity (Token)	Percentage
1	Uniswap V2: WHITE 9	82,603,398,752.851024078	8.2603%
2	Null Address: 0x00...dEaD	45,621,711,125.613409098	4.5622%
3	0xd266d61ac22c2a2ac2dd832e79c14ea152c998d6	36,001,312,253.113302134	3.6001%
4	0xf1964fd95337ef0c72a1f03a0c1800987f210f64	27,003,462,949.994260836	2.7003%
5	0x83d3bab57ac62e75750f1bc0ce6d65b3fb120ecd	23,404,741,959.04643963	2.3405%
6	0xbe23cbb62064b8b1550ae5ada59c39d45b1e2081	20,656,616,913.314817284	2.0657%
7	0x52d70f919087a2cd7c2b01272869649a21ca14cb	20,058,915,604.750000006	2.0059%
8	0xb056afd38fea7fa412fc836e388b333ffac1901d	19,446,310,261.14353637	1.9446%
9	0xdcf5eefd4cf4d57c37d47a7ecaa59893333bb698	18,927,552,979.000000013	1.8928%
10	0xc5cd85430cb678c995105e882c91001ffd448e0b	18,696,930,019.95	1.8697%

WhiteProxyLight TxnFees



● **Total Fees Spent (As a Sender)**
0.000000000000000000 Eth
USD 0.00 (Adjusted) | **USD 0.00** (Current)

● **Total Fees Used (As a recipient)**
1.066593705575051160 Eth
USD 1,763.82 (Adjusted) | **USD 1,546.94** (Current)

Ether Transaction Fees for 0x9a19e06322d1fe9bedbd3f6555803de2713c1762
Source: Etherscan.io

White Ethereum functions details

```
+  Context
   - [Int] _msgSender

 + [Int] IERC20
   - [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

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

 + [Int] IUniswapV2Factory
   - [Ext] createPair #

 + [Int] IUniswapV2Router02
   - [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #
   - [Ext] factory
   - [Ext] WETH
   - [Ext] addLiquidityETH ($)

 +  WhiteEthereum (Context, IERC20, Ownable)
   - [Pub] <Constructor> #
   - [Pub] name
   - [Pub] symbol
   - [Pub] decimals
   - [Pub] totalSupply
   - [Pub] balanceOf
```

- [Pub] transfer #
- [Pub] allowance
- [Pub] approve #
- [Pub] transferFrom #
- [Ext] setCooldownEnabled #
  - modifiers: onlyOwner
- [Prv] tokenFromReflection
- [Prv] _approve #
- [Prv] _transfer #
- [Prv] swapTokensForEth #
  - modifiers: lockTheSwap
- [Ext] setStandardTax #
  - modifiers: onlyOwner
- [Ext] removeLimits #
  - modifiers: onlyOwner
- [Prv] sendETHToFee #
- [Ext] openTrading #
  - modifiers: onlyOwner
- [Prv] _tokenTransfer #
- [Prv] _transferStandard #
- [Prv] _takeTeam #
- [Prv] _reflectFee #
- [Ext] <Fallback> ($)
- [Ext] manualswap #
- [Ext] manualsend #
- [Prv] _getValues
- [Prv] _getTValues
- [Prv] _getRValues
- [Prv] _getRate
- [Prv] _getCurrentSupply

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

Verifier functions details

```
+ [Lib] Pairing
   - [Int] negate
   - [Int] plus
   - [Int] scalar_mul
   - [Int] pairing

 +  Verifier
   - [Int] verifyingKey
   - [Pub] verifyProof
```

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

WhiteProxyLight functions details

```
+ [Int] IWhiteInstance
   - [Ext] token
   - [Ext] denomination
   - [Ext] deposit ($)
   - [Ext] withdraw ($)

 +  WhiteProxyLight
   - [Ext] deposit ($)
   - [Ext] withdraw ($)
   - [Ext] backupNotes #
```

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

ETHWhite functions details

```
+ [Int] IHasher
    - [Ext] MiMCSponge

 +  MerkleTreeWithHistory
    - [Pub] <Constructor> #
    - [Pub] hashLeftRight
    - [Int] _insert #
    - [Pub] isKnownRoot
    - [Pub] getLastRoot

 +  ReentrancyGuard
    - [Pub] <Constructor> #

 + [Int] IVerifier
    - [Ext] verifyProof #

 +  White (MerkleTreeWithHistory, ReentrancyGuard)
    - [Pub] <Constructor> #
       - modifiers: MerkleTreeWithHistory
    - [Ext] deposit ($)
       - modifiers: nonReentrant
    - [Int] _processDeposit #
    - [Ext] withdraw ($)
       - modifiers: nonReentrant
    - [Int] _processWithdraw #
    - [Pub] isSpent
    - [Ext] isSpentArray

 +  ETHWhite (White)
    - [Pub] <Constructor> #
       - modifiers: White
    - [Int] _processDeposit #
    - [Int] _processWithdraw #
```

($) = 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:

- backupNotes function only emits EncryptedNote event.

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

- White Ethereum:
  - Owner can enable/disable cooldownEnabled.
  - Owner can change _standardTax.
  - Owner can change _maxTxAmount and _maxWalletSize.
  - Owner can enable trading.
  - _feeAddrWallet can manually swap and send ETH to _feeAddrWallet.
- ETHWhite:
  - Owner can blacklist addresses.

Testnet deployment

Contracts Description Table

Contract	Type	Bases		
└	**Function Name**	**Visibility**	**Mutability**	**Modifiers**
WhiteEthereum	Implementation	Context, IERC20, Ownable		
└	transfer	Public ❗	🛑	NO❗
└	approve	Public ❗	🛑	NO❗
└	transferFrom	Public ❗	🛑	NO❗
└	setCooldownEnabled	External ❗	🛑	onlyOwner
└	setStandardTax	External ❗	🛑	onlyOwner
└	removeLimits	External ❗	🛑	onlyOwner
└	openTrading	External ❗	🛑	onlyOwner
└	manualswap	External ❗	🛑	NO❗
└	manualsend	External ❗	🛑	NO❗

Legend

Symbol	Meaning
🛑	Function can modify state
💵	Function is payable

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 locking details are provided by the team:
https://etherscan.io/tx/0x3b07e5aef189965bf6dc8a7419022efe1f758a0d893ff6c0e85bf77928cd26e1

Ownership renounce details are provided by the team:
https://etherscan.io/tx/0x49ad8c34a5682e07213374c3059806e1fe3c31bf801b6380d0aacdb8f5324b99

Security score: 93.

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.