TechRate
April, 2022

SMART CONTRACTS SECURITY AUDIT REPORT

Audit Details

Audited project

Ukan

Deployer address

0x40f72673331a14bc85d8c430276cb77c571fe70e

Client contacts:

Ukan team

Blockchain

Ethereum

Project website:

Not provided

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) (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 Ukan to perform an audit of smart contracts:
https://etherscan.io/address/0x49bc8340acd3521150d7ccd8a4a3510d2f5130ca#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

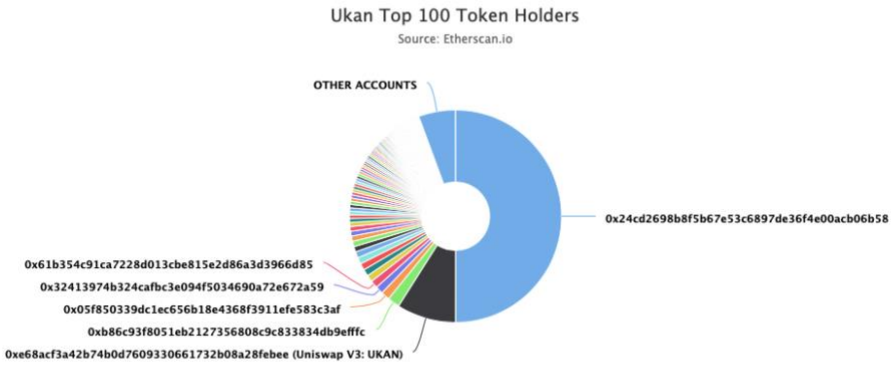
Token contract details for 08.04.2022

Contract name	Ukan
Contract address	0x49bc8340ACD3521150d7cCD8a4a3510D2F5130Ca
Total supply	1,000,000,000,000,000
Token ticker	UKAN
Decimals	18
Token holders	10,086
Transactions count	10,852
Top 100 holders dominance	94.37%
Contract deployer address	0x40f72673331a14bc85d8c430276cb77c571fe70e
Owner address	0x40f72673331a14bc85d8c430276cb77c571fe70e

Ukan Token Distribution

The top 100 holders collectively own 94.37% (943,696,616,450,019.00 Tokens) of Ukan

Token Total Supply: 1,000,000,000,000,000.00 Token | Total Token Holders: 10,086

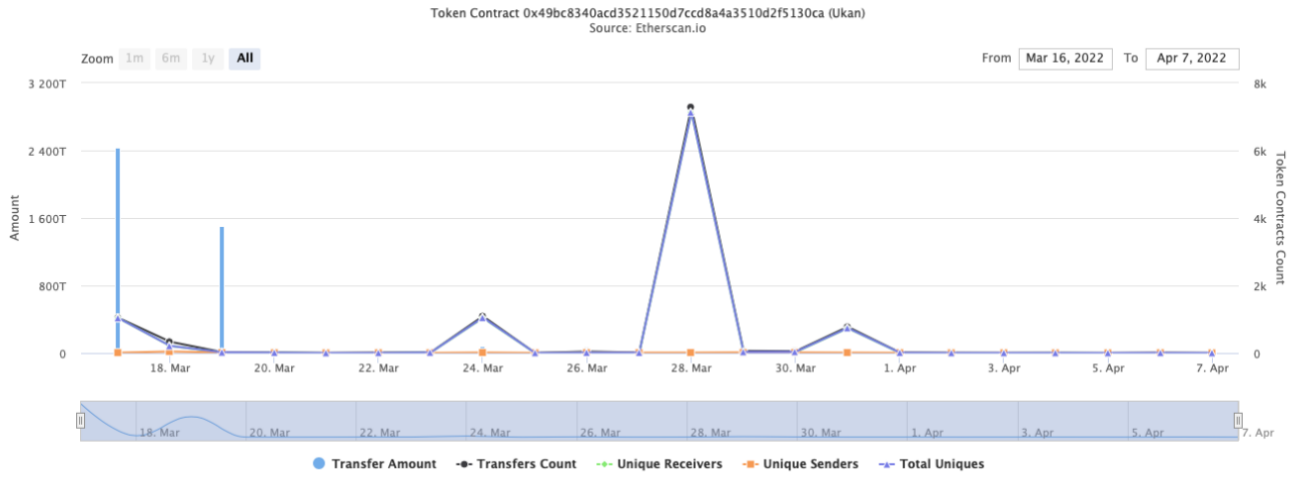


(A total of 943,696,616,450,019.00 tokens held by the top 100 accounts from the total supply of 1,000,000,000,000,000.00 token)

Ukan Contract Interaction Details

Time Series: Token Contract Overview

Thu 17, Mar 2022 - Thu 7, Apr 2022



Ukan Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	0x24cd2698b8f5b67e53c6897de36f4e00acb06b58	500,000,000,000,000.000013274732459483	50.0000%
2	Uniswap V3: UKAN	90,209,251,235,221.159530540266389444	9.0209%
3	0xb86c93f8051eb2127356808c9c833834db9efffc	18,596,823,031,623.39679464825705527	1.8597%
4	0x05f850339dc1ec656b18e4368f3911efe583c3af	13,245,275,968,450.301604650319962234	1.3245%
5	0x32413974b324cafbc3e094f5034690a72e672a59	11,664,751,807,525.006841494623787747	1.1665%
6	0x61b354c91ca7228d013cbe815e2d86a3d3966d85	11,594,875,624,559.048801721775212517	1.1595%
7	0x5fa9399e95602f20c8e356a00dd62f191a0fcbba	10,386,499,592,844.326866415239817305	1.0386%
8	0x669e8f10587240773b5904dd213f183a7d57b14e	10,317,954,585,411.46124394173080744	1.0318%
9	0x8c6ce9530ab421d5e60728e7d334c6ae76f1c56f	10,261,579,727,107.76456913692172388	1.0262%
10	0x1241afc6acf3d1544f113b2e001a3ad73d4508c2	9,816,095,675,002.610920991510111612	0.9816%

Contract functions details

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

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

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

+ 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] _beforeTokenTransfer #
  - [Int] _afterTokenTransfer #

+ ERC20Burnable (Context, ERC20)
  - [Pub] burn #
  - [Pub] burnFrom #

+ ERC20Capped (ERC20)
  - [Pub] <Constructor> #
  - [Pub] cap
  - [Int] _mint #

+ [Lib] Address
  - [Int] isContract
  - [Int] sendValue #
  - [Int] functionCall #
  - [Int] functionCall #
  - [Int] functionCallWithValue #
  - [Int] functionCallWithValue #
  - [Int] functionStaticCall
  - [Int] functionStaticCall
  - [Int] functionDelegateCall #
  - [Int] functionDelegateCall #
  - [Int] verifyCallResult

+ [Int] IERC165
  - [Ext] supportsInterface

+ ERC165 (IERC165)
  - [Pub] supportsInterface

+ [Int] IERC1363 (IERC20, IERC165)
  - [Ext] transferAndCall #
  - [Ext] transferAndCall #
  - [Ext] transferFromAndCall #
  - [Ext] transferFromAndCall #
  - [Ext] approveAndCall #
  - [Ext] approveAndCall #

+ [Int] IERC1363Receiver
  - [Ext] onTransferReceived #

+ [Int] IERC1363Spender
  - [Ext] onApprovalReceived #

+ ERC1363 (ERC20, IERC1363, ERC165)
  - [Pub] supportsInterface
  - [Pub] transferAndCall #
  - [Pub] transferAndCall #
  - [Pub] transferFromAndCall #
  - [Pub] transferFromAndCall #
  - [Pub] approveAndCall #

```
  - [Pub] approveAndCall #
  - [Int] _checkAndCallTransfer #
  - [Int] _checkAndCallApprove #

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

+  TokenRecover (Ownable)
  - [Pub] recoverERC20 #
    - modifiers: onlyOwner

+  ERC20Decimals (ERC20)
  - [Pub] <Constructor> #
  - [Pub] decimals

+  ERC20Mintable (ERC20)
  - [Ext] mintingFinished
  - [Ext] mint #
    - modifiers: canMint
  - [Ext] finishMinting #
    - modifiers: canMint
  - [Int] _finishMinting #

+ [Int] IAccessControl
  - [Ext] hasRole
  - [Ext] getRoleAdmin
  - [Ext] grantRole #
  - [Ext] revokeRole #
  - [Ext] renounceRole #

+ [Lib] Strings
  - [Int] toString
  - [Int] toHexString
  - [Int] toHexString

+  AccessControl (Context, IAccessControl, ERC165)
  - [Pub] supportsInterface
  - [Pub] hasRole
  - [Int] _checkRole
```

- [Pub] getRoleAdmin
- [Pub] grantRole #
  - modifiers: onlyRole
- [Pub] revokeRole #
  - modifiers: onlyRole
- [Pub] renounceRole #
- [Int] _setupRole #
- [Int] _setRoleAdmin #
- [Int] _grantRole #
- [Int] _revokeRole #

+ Roles (AccessControl)
- [Pub] <Constructor> #

+ [Int] IPayable
- [Ext] pay ($)

+ ServicePayer
- [Pub] <Constructor> ($)

+ PowerfulERC20 (ERC20Decimals, ERC20Capped, ERC20Mintable, ERC20Burnable, ERC1363, TokenRecover, Roles, ServicePayer)
- [Pub] <Constructor> ($)
  - modifiers: ERC20,ERC20Decimals,ERC20Capped,ServicePayer
- [Pub] decimals
- [Pub] supportsInterface
- [Int] _mint #
  - modifiers: onlyMinter
- [Int] _finishMinting #
  - modifiers: onlyOwner

($) = 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.

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

- Minter role can mint tokens.
- Owner can finish minting.
- Owner can withdraw ERC20 tokens.

Conclusion

Smart contracts do not contain high severity issues! Liquidity pair contract's security is not checked due to out of scope. Smart contract contains interfaces that is not audited, some functions may work different way. The further transfers and operations with the funds raise are not related to this particular contract.

Liquidity locking details are NOT provided by the team.

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.