Mobiloitte
BOTS.APPS.DIGITAL.AI.IoT
BLOCKCHAIN

SMART CONTRACT AUDIT REPORT

For

FX99.IO

Email - info@fx99.io

Prepared By: Shubham Khanna
Address: 105 Cecil St, 13-04 The Octagon, Singapore 069543
http://www.mobiloitte.com.sg/
Email Address: connect@mobiloitte.com.sg

Document Properties

Client	fx99.io
Title	Smart Contract Audit Report
Target	OneSwap
Version	1.0
AUTHOR	Mukund
Reviewed by	Shubham Khanna
Approved by	Shubham Khanna
Classification	Public

Version Info

Version	Date	AUTHOR(s)	Description
1.0	September 21, 2020	Shubam Khanna	Final Release

Contact

For more information about this document and its contents, please contact Mobiloitte Technologies

Name	Arvind Tyagi
Phone	+91-9999525880
Email	connect@mobiloitte.com.sg

Audit Report Summary!

1. **Costly loop :** If array.length is large enough, the function exceeds the block gas limit, and transactions calling it will never be confirmed (None)

2. **Overlap Attack :** the appearance of gigantic arrays is possible (None)

3. **Use of unindexed arguments** : None

4. **Timestamp Dependance** : The timestamp of the block can be slightly manipulated by the miner.
   a. Line number 743 (start = now) : Warning
   b. Severity : Low

5. **Use of call function** : In this case, transfer or send function call is more secure.If required, gas limit should be added (.gas()).
   a. Line number 334 ((bool success,) = recipient.call{ value: amount }("");) : Warning
   b. Severity : Low

6. **Implicit visibility level :** The default function visibility level in contracts is public, in interfaces - external, state variable default visibility level is internal. (Checked)

7. **Non-initialized return value** : Function doesn't initialize return value. As a result, the default value will be returned. (Checked)

8. **Use of assembly** : Inline assembly is a way to access the Ethereum Virtual Machine at a low level. This discards several important safety features of Solidity.
   a. Line Number 310 (assembly { codehash := extcodehash(account) })
   b. Line number 410 (assembly {
      let returndata_size := mload(returndata)
      revert(add(32, returndata), returndata_size)
      })
   c. Severity : Medium

9. **Use of return in constructor :** Checked (None)

10. **HardCoded Address** : Line number 308 & 720 (Check for issuance)

11. **Pure-functions should not read/change state** : Checked (None)

12. **Constant functions** : Consider using view for functions and constant for state variables. (Checked/ None)

13. **DoS by external Contract** : A conditional statement (if, for, while) should not depend on an external call: the callee may permanently fail (e.g. with throw; or revert();), preventing the caller from completing the execution.
    a. Line number 405 (if (returndata.length > 0) {assembly {
    let returndata_size := mload(returndata)
    revert(add(32, returndata), returndata_size)})
    b. Severity : Low

14. **Reentrancy** : Any interaction from a contract (A) with another contract (B) and any transfer of Ether hands over control to that contract (B). This makes it possible for B to call back into A before this interaction is completed. (Checked/None)

15. **Cross-function Reentrancy :** Checked/None

16. **Style guide violation :** Checked/None

17. **Unchecked math :** Checked/None

18. **Strict comparison with block.timestamp or now :** now can be manipulated by the miner so that he/she will always win.
    a. Line number 743 (start=now;)
    b. Severity : Low

19. **Overflow and Underflow :** Checked/None

20. **Using the approve function of the ERC-20 token standard :** Check with the necessity of approve methods inside the contract. (warning)

21. **Replace multiple return values with a struct :** Checked/None

22. **Replace multiple return values with a struct :** Cross Checked (Used canonical form

Code is of *Excellent* build quality and has been checked and gone through 37 failure cases and has found no module withsevere risks. Code is approved for Deployment.