DIGITAL ASSET COMPLIANCE & SECURITY AUDIT SERVICES

SECURITY AUDIT REPORT

venrai

1 June 2021

info@Venrai.com

Venrai.com

venrai

CONTENTS

venrai

AUDIT SCOPE

The scope of this audit was to identify and report on potential security issues in the code of the provisioned smart contracts. Contracts were analysed for security deficiencies using automated methods.

The analysis did not identify any critical vulnerabilities.

During the audit Venrai aimed to confirm that each smart contract:

- Implements and adheres to existing BEP-20 standards;
- Uses methods safe from re-entrance attacks;
- Is not affected by critical vulnerabilities.

It should be noted that this audit is not an endorsement of the reliability or effectiveness of the smart contracts and should instead be viewed as an assessment of the logic and implementation of the smart contracts. To ensure secure contract code we at Venrai recommend that the team puts in place a bug bounty programme to encourage further and active analysis of the smart contracts.

venrai

SECURITY ISSUE RATINGS

Minor issues are generally subjective in nature or potentially deal with topics such as "best practice" or "readability". Minor issues will in general not indicate an actual problem or bug in code. Owner of the project should use their own judgment as to whether addressing these issues improves the codebase.

Medium issues are generally objective in nature but do not represent actual bugs or security problems. These issues should be addressed unless there is a clear reason not to.

Major issues include bugs and security vulnerabilities. These issues may not be directly exploitable or may require a certain condition to arise in order to be exploited. Left unaddressed, these issues are likely to cause problems with the operation of the contract or to lead to a situation that allows for exploitation.

Critical issues are directly exploitable bugs or security vulnerabilities. Left unaddressed, these issues are highly likely or guaranteed to cause major problems or potentially a full failure in the operations of the contract.

venrai

SECURITY AUDIT RESULTS

The following results pertain to our security audit of SAFUYIELD smart contracts, which can be accessed via the following link.

https://bscscan.com/address/0xc74cd0042c837ce59210857504ebb0859e06aa22#code

Evaluation of Address - PASS

This contract meets modern security requirements, with no issues observed.

Vulnerability Checklist:

Integer Underflow	-	PASS
Integer Overflow	-	PASS
Parity Multisig Bug	-	PASS
Callstack Depth Attack	-	PASS
Transaction-Ordering Dependency	-	PASS
Timestamp Dependency	-	PASS
Re-Entrancy	-	PASS

Evaluation of Context - PASS

This contract meets modern security requirements, with no issues observed.

Vulnerability Checklist:

Integer Underflow	-	PASS
Integer Overflow	-	PASS
Parity Multisig Bug	-	PASS
Callstack Depth Attack	-	PASS
Transaction-Ordering Dependency	-	PASS
Timestamp Dependency	-	PASS
Re-Entrancy	-	PASS

venrai

Evaluation of Ownable - PASS

This contract meets modern security requirements, with no issues observed.

Vulnerability Checklist:

Integer Underflow	-	PASS
Integer Overflow	-	PASS
Parity Multisig Bug	-	PASS
Callstack Depth Attack	-	PASS
Transaction-Ordering Dependency	-	PASS
Timestamp Dependency	-	PASS
Re-Entrancy	-	PASS

Evaluation of SafuYield - PASS

This contract meets modern security requirements, with no issues observed.

Vulnerability Checklist:

Integer Underflow	-	PASS
Integer Overflow	-	PASS
Parity Multisig Bug	-	PASS
Callstack Depth Attack	-	PASS
Transaction-Ordering Dependency	-	PASS
Timestamp Dependency	-	PASS
Re-Entrancy	-	PASS

CONCLUSION

Serious vulnerabilities were not detected. The contracts are well written and follow proper BEP-20 specification. All reviewed contracts have passed the Venrai auditing process.

venrai

AUDIT TOOLS

Venrai security audits of smart contract code leverages a number of tools, some of which are listed below.

Remix IDE (http://remix.ethereum.org)

Mythrill (https://github.com/ConsenSys/mythril-classic)

solidity-coverage (https://github.com/sc-forks/solidity-coverage)

eth-gas-reporter (https://github.com/cgewecke/eth-gas-reporter)

Anchain.ai (https://sandbox.anchainai.com)

solium (https://github.com/duaraghav8/Solium)

solhint (https://github.com/protofire/solhint)

DISCLAIMER

The statements made in this document should not be interpreted as investment or legal advice, nor should its authors be held accountable for decisions made based on them.

We recommend that the team put in place a bug bounty program to encourage further analysis of the smart contract by other third parties.

CONTACT US
+44 (0) 7445 869246
info@Venrai.com
www.Venrai.com

venrai