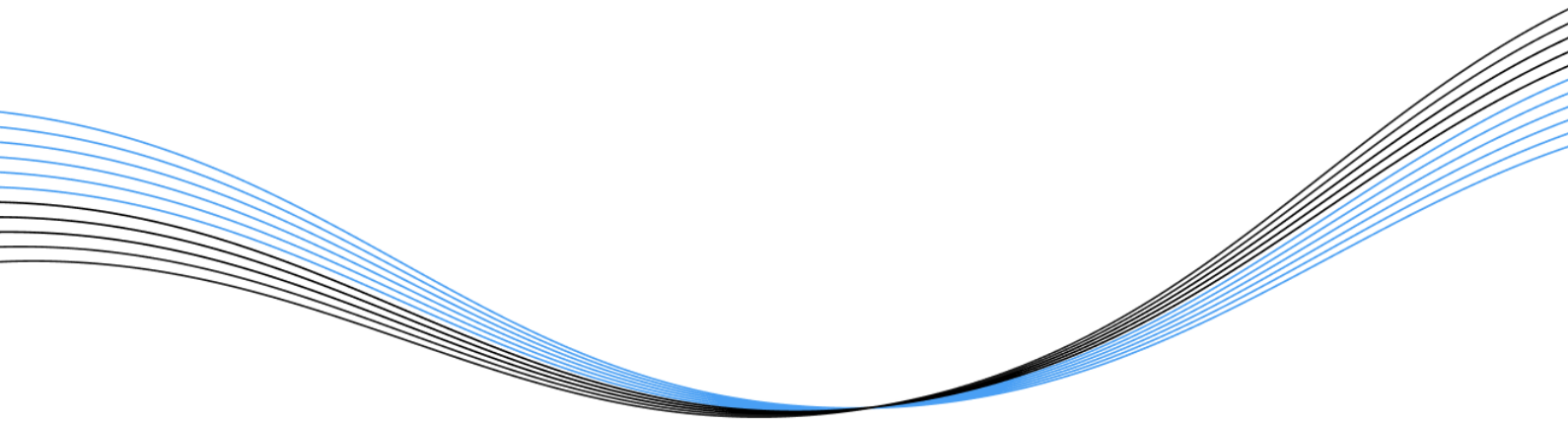
© Hexlant Inc.
Gangnam-daero 340
Seoul,
Republic of Korea 06242
Hexlant.com

1ECO SMART CONTRACT AUDIT REPORT



Audit Date
18 NOV 2021

Category
Token Contract

Auditor
Hexlant Audit Team

This contract specifies that it has been validated by the Hexlant Technical Team and notifies that it has not any technical defects.

AUDIT OVERVIEW

PUBLISHED INFORMATION	
REPORT NUMBER	ERC20211118pz
DATE	2021/11/18
PUBLISHER	Henry / henry@hexlant.com

PROJECT INFORMATION			
TITLE	1eco coin		
SYMBOL	1ECO		
PLATFORM	ETHEREUM	**TOKEN TYPE**	ERC-20
TOTAL SUPPLY	500,000,000 1ECO		
CONTRACT ADDRESS	0x1af2eaeaf2b1d9dda800861268e6bbb3995a6c3b		

VULNERABILITY ANALYSIS		
CRITICAL	0	No relevant provision
HIGH	0	No relevant provision
MEDIUM	0	No relevant provision
LOW	0	No relevant provision

CENTRALIZED FUNCTION		
FREEZE	YES	Ability to freeze tokens in accounts. (The administrator can freeze the hacker's account in case of hacking.)
PAUSE	YES	Ability to pause functions related to token transmission in a contract. (This is used when the administrator needs to prevent the movement of assets due to token swaps or hacking.)
LOCKUP	NO	Ability to block token transfers for a period of time (Administrators can use to set lockout periods for investors, team members, advisors, etc.)
BURN	YES	Ability to reduce total supply by burning tokens
MINT	NO	Ability to increase total supply by minting tokens

COMPANY PROPOSAL

Hexlant는 2018년에 설립한 블록체인 기술 기업입니다. 삼성전자 출신의 보안·네트워크·소프트웨어 전문가가 스마트 컨트랙트와 블록체인 프로토콜의 보안 결함을 발견하고 블록체인 생태계의 기술 안정성을 입증하기 위해 설립하였습니다.

Hexlant는 블록체인 동작 환경을 파악하기 위해 20개 이상의 블록체인 메인넷을 직접 구축하고 있습니다. 나아가 키 보안 알고리즘 및 메인넷 모니터링 기술을 개발했습니다. 이 방식은 비트코인, 이더리움, 폴카닷, 에이다 등 헥슬란트가 보유한 모든 메인넷 플랫폼에서 적용되고 운영됩니다.

Hexlant는 위와 같은 기술 운영 경험을 바탕으로 스마트 컨트랙트 기술을 검증합니다. 스마트 컨트랙트 내 버그를 발견하는 오류 테스트 뿐만 아니라 메인넷 상황에서의 문제점을 탐지하며 서비스 관점에서 지속적으로 운영할 수 있는 블록체인 기술 가이드를 제공합니다.

Hexlant의 고객사는 컨트랙트에 대한 취약성 감사부터 오너 키 관리, 블록체인 지갑 시스템 구축 등 블록체인 기술 전반의 서비스를 제공받을 수 있습니다. 현재 200여개의 고객사가 Hexlant의 서비스를 바탕으로 블록체인 사업을 시작, 운영했으며 누적으로 관리하는 자산은 12조를 달성했습니다.

Initials for identification purposes:

CONTENTS

ANALYSIS PURPOSE

본 리포트는 발행된 컨트랙트 코드가 요구사항을 충분히 만족하는지, 그리고 보안의 취약점과 실제 운영 하면서 발생 할 수 있는 문제들을 파악하고 해결방안을 찾기위해 분석을 수행하고 그 결과를 정리하였습니다. 이번 코드 분석은 다음과 같은 요소들을 검증하기위해 진행하였습니다.

- 구현된 기능의 정상 작동 여부
- 기능 수행 중 보안 위험성
- Off Chain에서 발생하는 문제에 대한 대비
- 컨트랙트 코드의 가독성 및 코드 완성도

VULNERABILITY CLASSIFICATION

본 취약성 검증은 오류 위험도를 아래와 같이 분류, 평가합니다.

● Critical Severity

심각성 치명적 단계는 큰 보안 결함을 뜻하며 자산 탈취 및 동결, 추가 발행 등 치명적인 문제를 야기합니다. 본 결함은 반드시 수정되야 합니다.

● High Severity

심각성 높은 단계는 특수 조건에 의해 보안 결함이 발생할 수 있는 항목이며 수정을 강력하게 권고합니다.

● Medium Severity

심각성 중간 단계는 보안 결함은 아니나 비효율적인 컨트랙트 동작을 야기합니다. 컨트랙트를 효율적으로 동작하도록 수정을 권유하는 항목입니다.

● Low Severity

심각성 낮음 단계는 보안에는 문제가 없으나 컨트랙트 구조 개선을 위해 수정을 권유하는 항목입니다.

1ECO CONTRACT VULNERABILITY ANALYSIS		
● **CRITICAL**	0	No relevant provision
● **HIGH**	0	No relevant provision
● **MEDIUM**	0	No relevant provision
● **LOW**	0	No relevant provision

FUNCTION SUMMARY

- **Ownable**

  컨트랙트 오너쉽에 관련된 기능을 제공합니다. onlyOwner Modifier를 통해 기능 실행에 대한 권한을 특정 주소로 한정할 수 있습니다.

- **ERC20Burnable**

  컨트랙트 토큰 소각과 관련된 기능을 제공합니다. 토큰 홀더의 잔액 또는 출금 위임된 토큰 잔액에 한하여 소각을 진행할 수 있습니다.

- **ECO1**

  1ECO 의 메인 컨트랙트입니다. 소각, 동결과 같은 생태계에 필수적인 기능을 추가 제공합니다.

Function 1. Contract

상태 변수와 함수를 포함하여 컨테이너 형태의 계약을 표현하기 위해 사용

Contract	Description
Context	컨트랙트 Context
Ownable	컨트랙트 오너쉽 관련 기능
Pausable	컨트랙트 정지 상태 관련 기능
Freezable	컨트랙트 동결 상태 관련 기능
ERC20	ERC20 표준 인터페이스 관련 기능
ERC20Burnable	토큰 소각과 관련된 기능
ECO1	1ECO 메인 기능

Function 2. Interface

컨트랙트 내 구현하고자 하는 표준함수를 정의하기 위해 사용

Interface	Description
IERC20	ERC20 표준 인터페이스
IERC20Metadata	ERC20 정보 인터페이스

Function 3. Library

상태 변수를 가질 수 없고 상속을 지원하지 않는 컨트랙트 라이브러리. 라이브러리 함수가 호출되며 호출한 컨트랙트의 컨택스트에서 실행

Library	Description

Function 4. Variable

컨트랙트의 상태를 표현하는 변수들로 컨트랙트에 필요한 정보들을 저장하기 위해 사용

Variable	Description
_owner	컨트랙트 오너 주소
_paused	컨트랙트 정지 상태
_balances	특정 주소의 토큰 잔액 테이블
_allowances	특정 주소에게 출금이 위임된 토큰 잔액 테이블
_totalSupply	토큰 총 발행량
_name	토큰 이름
_symbol	토큰 심볼
_frozenAccount	특정 주소의 동결 여부 테이블

Function 5. Modifier

함수의 한정요소로 특정 기능을 수행할 때 한정된 조건에서만 실행될 수 있도록 하기 위해 사용

Modifier	Description
onlyOwner	컨트랙트의 오너만 실행 가능
whenNotPaused	컨트랙트가 정지 상태가 아닐 경우 실행가능
whenPaused	컨트랙트가 정지 상태일 경우 실행가능
whenNotFrozen	특정 주소가 동결 상태가 아닐 경우 실행가능

Function 6. Event

컨트랙트 함수 실행에 따른 로그 이벤트로 추후 애플리케이션 적용에 있어 컨트랙트 상황을 보다 쉽게 대응하기 위해 사용

Event	Description
OwnershipTransferred	컨트랙트 오너 주소 이전 시 이벤트 발생
Paused	컨트랙트 정지 시 이벤트 발생
Unpaused	컨트랙트 정지 상태 해제 시 이벤트 발생
Transfer	토큰 전송 시 이벤트 발생
Approval	출금 위임 시 이벤트 발생
Freeze	주소 동결 시 이벤트 발생
Unfreeze	주소 동결 상태 해제 시 이벤트 발생

Function 7. Function

컨트랙트의 함수들로써 컨트랙트에 필요한 특정 로직을 담아 기능 실행을 하기 위해 사용

Event	Description
name	토큰 이름 확인
symbol	토큰 심볼 확인

decimals	토큰 최대 표현 가능한 소수점 자리수 확인
totalSupply	토큰 총 발행량 확인
balanceOf	특정 주소의 토큰 잔액 확인
allowance	특정 주소 출금 위임 잔액 확인
transfer	토큰 전송
approve	출금 위임
transferFrom	출금 위임된 토큰 전송
increaseAllowance	출금 위임된 토큰 잔액 증액
decreaseAllowance	출금 위임된 토큰 잔액 감액
_transfer	토큰 전송 이너 함수
_mint	토큰 발행 이너 함수
burn	토큰 소각
_burn	토큰 소각 이너 함수
burnFrom	출금 위임된 토큰 소각
_burnFrom	출금 위임된 토큰 소각 이너 함수
_approve	출금 위임 이너 함수
transferOwnership	컨트랙트 오너 권한 이전
renounceOwnership	컨트랙트 오너 권한 포기
pause	컨트랙트 정지 상태로 전환
unpause	컨트랙트 정지 상태 해제
isFrozen	특정 주소 동경 상태 확인
freezeAccount	특정 주소 동결
unfreezeAccount	특정 주소 동결 해제
_msgSender	트랜잭션 발신자 반환
_msgData	트랜잭션 호출 데이터 반환
_beforeTokenTransfer	토큰 전송 전 배리데이션 체크 함수

TEST RESULT

Code Coverage

코드 커버리지는 작성한 테스트가 얼마만큼 컨트랙트 코드의 기능을 테스트 했는지 알 수 있는 정량적인 지표입니다.

1ECO 컨트랙트는 라이브러리와 일부 컨트랙트에 구현된 기능에 대해 추가적인 호출이 진행되지 않은 경우가 존재합니다.

아래의 Coverage 지표는 위 사항을 반영한 결과입니다.

File Name	Statements	Functions	Lines
ECO1.sol	100% (82/83)	100% (41/42)	100% (91/93)

TEST CASE

실제 적용한 테스트케이스 목록입니다.

Test Case	Result	
배포 시 지정한 토큰의 이름과 일치하는가?	PASS	FAIL
배포 시 지정한 토큰의 심볼과 일치하는가?	PASS	FAIL
배포 시 지정한 토큰의 데시멀과 일치하는가?	PASS	FAIL
배포 시 지정한 토큰의 초기 발행량과 일치하는가?	PASS	FAIL
배포 시 지정한 초기 발행량이 컨트랙트 배포자에게 할당되는가?	PASS	FAIL
배포 후 오너의 주소 이외의 토큰 잔액은 0인가?	PASS	FAIL
기본적인 토큰 전송은 잘 동작하는가?	PASS	FAIL
특정 주소들의 올바른 토큰 잔액을 반환한다.	PASS	FAIL
보유 토큰 잔액을 초과하여 토큰 전송 시 예외처리가 되는가?	PASS	FAIL
받는 주소가 0x0의 주소일 경우, 예외처리가 되는가?	PASS	FAIL
토큰에 대한 출금을 위임할 수 있는가?	PASS	FAIL
출금 위임된 토큰의 잔액을 확인 가능한가?	PASS	FAIL
출금 위임된 토큰의 잔액을 증액 가능한가?	PASS	FAIL
출금 위임된 토큰의 잔액을 감액 가능한가?	PASS	FAIL
출금 위임된 토큰을 전송 가능한가?	PASS	FAIL
출금 위임된 토큰을 전송 시 받는 주소가 0x0일 경우 예외처리가 되는가?	PASS	FAIL
출금 위임된 토큰을 전송 시 위임자의 잔액이 부족할 경우 예외처리가 되는가?	PASS	FAIL
출금 위임된 토큰을 전송 시 위임된 잔액을 초과하여 전송 시 예외처리가 되는가?	PASS	FAIL
컨트랙트의 오너 주소를 올바르게 반환한다.	PASS	FAIL
컨트랙트 오너 외 주소로부터 오너 권한 이전 시 예외처리가 되는가?	PASS	FAIL
컨트랙트 오너 로부터 오너 권한 이전 신청이 가능한가?	PASS	FAIL
컨트랙트의 오너는 오너권한을 포기할 수 있는가?	PASS	FAIL
컨트랙트 오너 외 주소가 오너권한 포기 시 예외처리가 되는가?	PASS	FAIL
컨트랙트의 오너를 0x0에게 위임 시 예외처리가 되는가?	PASS	FAIL
토큰 소각 기능은 잘 동작하는가?	PASS	FAIL

토큰 소각 시 보유 잔액이 부족하면 예외처리가 되는가?	PASS	FAIL
토큰 소각 시 토큰 총 발행량도 함께 감액하는가?	PASS	FAIL
출금 위임받은 토큰에 대한 소각이 가능한가?	PASS	FAIL
출금 위임받은 토큰 잔액이 부족할 경우 소각 시 예외처리가 되는가?	PASS	FAIL
출금 위임받은 토큰 소각 시 위임자의 잔액이 부족하면 예외처리가 되는가?	PASS	FAIL
컨트랙트 오너 외 주소로부터 특정 주소 동결 시 예외처리가 되는가?	PASS	FAIL
컨트랙트 오너 외 주소로부터 동결된 주소의 동결 해제시 예외처리가 되는가?	PASS	FAIL
컨트랙트 오너는 특정 주소를 동결할 수 있는가?	PASS	FAIL
컨트랙트 오너는 특정 주소의 동결 상태를 해제 가능한가?	PASS	FAIL
동결된 주소는 토큰 전송 시 예외처리가 되는가?	PASS	FAIL
동결된 주소는 출금 위임된 토큰 전송 시 예외처리가 되는가?	PASS	FAIL
동결된 주소의 동결 상태를 해제 시 토큰 전송이 가능한가?	PASS	FAIL
동결된 주소의 동결 상태 해제시 출금 위임된 토큰 전송이 가능한가?	PASS	FAIL
동결된 주소를 다시 동결 시 예외처리가 되는가?	PASS	FAIL
동결 되지 않은 주소를 해제 시 예외처리가 되는가?	PASS	FAIL
컨트랙트 정지 상태를 확인가능하다.	PASS	FAIL
컨트랙트 오너는 컨트랙트를 정지시킬 수 있다.	PASS	FAIL
컨트랙트 오너 외 주소로부터 컨트랙트 정지 시도 시 예외처리가 되는가?	PASS	FAIL
컨트랙트 오너는 컨트랙트 정지 상태를 해제 할 수 있다.	PASS	FAIL
컨트랙트 오너 외 주소로부터 컨트랙트 정지 상태 해제 시 예외처리가 되는가?	PASS	FAIL
컨트랙트가 정지 상태 일 때 토큰 전송 시 예외처리가 되는가?	PASS	FAIL
컨트랙트가 정지 상태 일 때 출금 권한을 부여받은 토큰을 전송하면 예외처리가 되는가?	PASS	FAIL
컨트랙트가 정지 상태가 아닐 시 정지 해제 하면 예외처리가 되는가?	PASS	FAIL

VULNERABILITY ANALYSIS

본 컨트랙트의 수정이 필요한 사항은 없습니다.

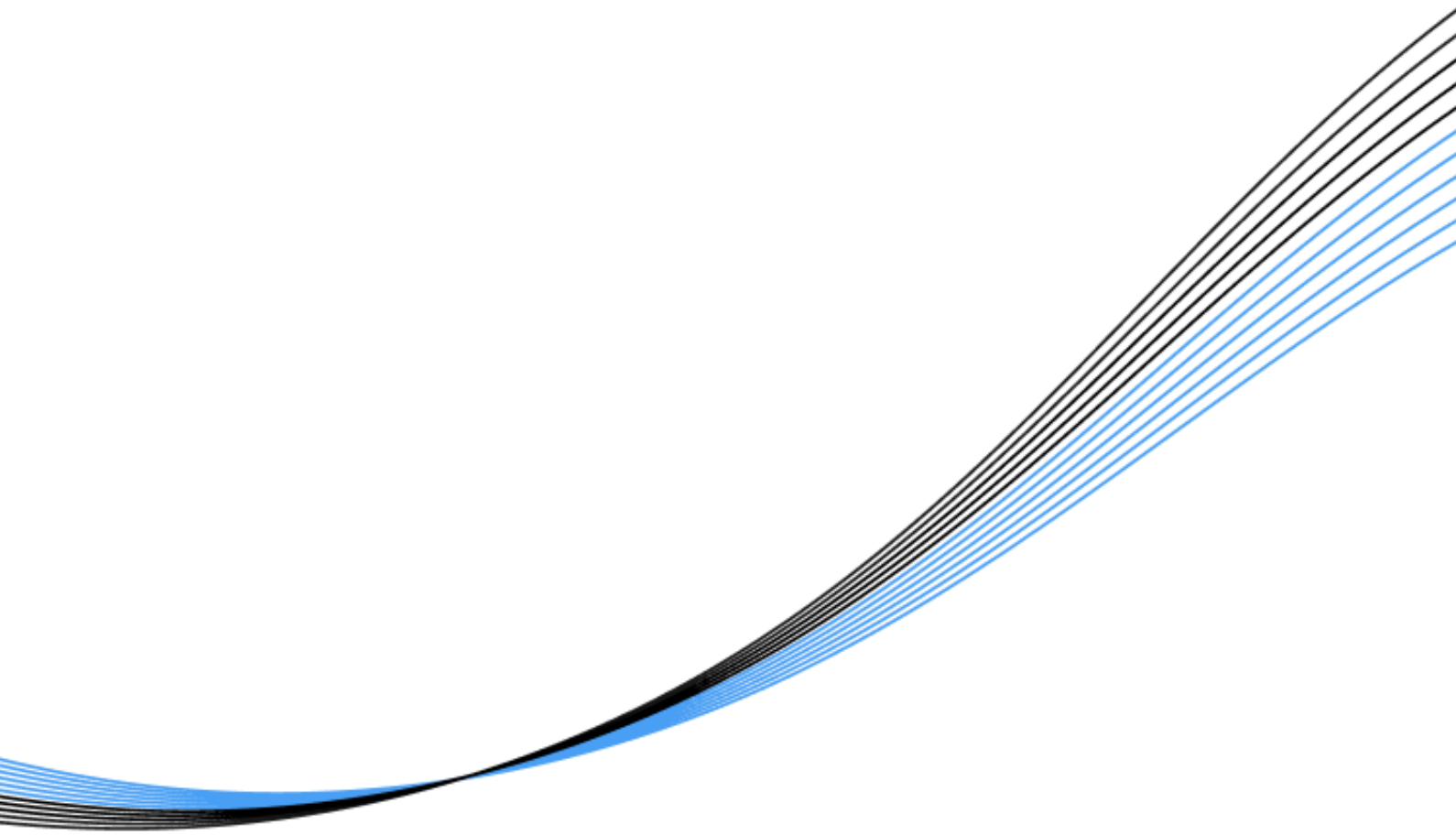
1ECO CONTRACT VULNERABILITY ANALYSIS		
● **CRITICAL**	0	No relevant provision
● **HIGH**	0	No relevant provision
● **MEDIUM**	0	No relevant provision
● **LOW**	0	No relevant provision

CONCLUSION

1ECO 컨트랙트는 ERC-20 표준 기능 외 동결과 더불어 정지 기능을 포함한 컨트랙트입니다. 컨트랙트 오너권한을 두어 전체 생태계의 토큰 전송을 제재할 수 있을 뿐 아니라 특정 주소를 동결하여 출금을 정지시킬 수 있습니다. 토큰 유통량에 관여될 수 있는 토큰 소각 기능이 추가되어 있으며 해당 기능은 토큰 홀더 본인의 토큰을 소각을 하거나 출금 위임된 토큰 잔액에 한에서 소각을 진행할 수 있습니다. 정지 기능은 스왑이나 토큰 생태계의 특수상황 시 전체 컨트랙트의 기능을 멈출 수 있는 기능입니다.

Declare

해당 리포트는 Hexlant의 스마트 컨트랙트 보안 감사 결과를 바탕으로 작성되었습니다. 해당 리포트는 비즈니스 모델의 적합성과 법적 규제, 투자에 대한 의견을 보증하지 않습니다. 리포트에 기술한 문제점 이외에 메인넷 기술 또는 가상머신을 비롯하여 발견되지 않은 문제점이 있을 수 있습니다. 해당 리포트는 논의 목적으로만 사용됩니다.



Hexlant.

-

contact@hexlant.com
www.hexlant.com