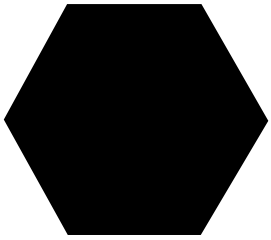
29 MAR 2021

MPLE SMART CONTRACT AUDIT REPORT

Hexlant.



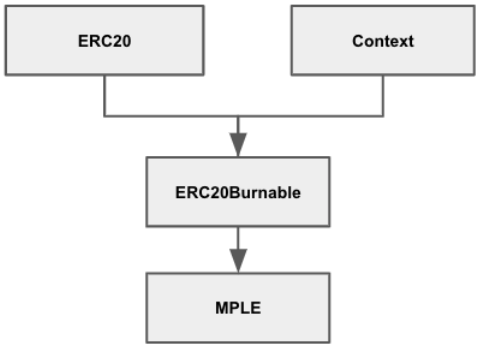
Analysis Purpose

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 정상작동 여부
- 기능 수행 중 보안 위험성
- **Off Chain**에서 발생하는 문제에 대한 대비
- 컨트랙트 코드의 가독성 및 코드 완성도

Function Summary

MPLE 컨트랙트는 다음과 같은 컨트랙트를 통해 **MPLE**의 기능을 구현하였습니다.



- **ERC20Burnable**
  토큰 소각과 관련된 기능을 제공합니다.

- **ERC20**
  ERC20 표준 기능을 제공합니다.

- **MPLE**
  MPLE 의 메인 컨트랙트입니다. 스테이킹 및 컨트랙트 정지 등의 기능을 제공합니다.

Contract

상태 변수와 함수를 포함하여 컨테이너 형태의 계약을 표현하기 위해 사용

Contract	Description
Context	실행 컨텍스트 관련 기능을 포함한 컨트랙트
ERC20	ERC20 표준 기능을 포함한 컨트랙트
ERC20Burnable	토큰 소각 기능을 포함한 컨트랙트
MPLE	메인 컨트랙트

Interface

컨트랙트 내 구현하고자 하는 표준함수를 정의하기 위해 사용

Interface	Description
IERC20	ERC20 인터페이스
ISTAKING	스테이킹 컨트랙트 인터페이스

Library

상태 변수를 갖을 수 없고 상속을 지원하지 않는 컨트랙트 라이브러리로, 라이브러리 내 함수가 호출되며 호출한 컨트랙트의 컨텍스트에서 실행

Library	Description
SafeMath	산술 연산 관련 기능을 포함한 라이브러리
Address	주소 관련 기능을 포함한 라이브러리

Variable

컨트랙트의 상태를 표현하는 변수들로, 컨트랙트에 필요한 정보들을 저장하기위해 사용

Variable	Description
_balances	특정 주소의 토큰 잔액 테이블
_allowances	특정 주소의 출금 위임된 토큰 잔액 테이블
_totalSupply	토큰 총 발행량
_name	토큰 이름
_symbol	토큰 심볼
_decimals	토큰 데시멀
INITAL_SUPPLY	초기 공급량
stakingContract	스테이킹 컨트랙트 주소
_paused	컨트랙트 정지 상태
_owner	컨트랙트 관리자 주소
stakingFinished	스테이킹 종료 여부
stakingLocked	스테이킹 락업 여부
stakingManagers	스테이킹 관리자 테이블

Modifier

함수의 한정요소로, 특정 기능을 수행할 때 한정된 조건에서만 실행 될 수 있도록 하기 위해 사용

Modifier	Description
onlyOwner	컨트랙트 관리자만 실행 가능
onlyManager	컨트랙트 매니저만 실행 가능
canStaking	스테이킹 종료 상태가 아닐 경우 실행 가능
canWithdraw	스테이킹 락업 상태가 아닐 경우 실행 가능
onlyContract	컨트랙트 주소 일 경우 만 실행 가능
whenNotPaused	컨트랙트 정지 상태가 아닐 경우 실행 가능
whenPaused	컨트랙트 정지 상태일 경우 실행 가능

Event

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

Event	Description
Transfer	토큰 전송 시 이벤트 발생
Approval	출금 위임 시 이벤트 발생
OwnershipTransferred	컨트랙트 관리자 권한 이전 시 이벤트 발생
Staking	스테이킹 시 이벤트 발생
Withdraw	스테이킹 해제 시 이벤트 발생
StaikngOpen	스테이킹 오픈 시 이벤트 발생
StakingFinished	스테이킹 종료 시 이벤트 발생
StakingContractChanged	스테이킹 컨트랙트 변경 시 이벤트 발생
ManagerChanged	컨트랙트 매니저 변경 시 이벤트 발생
WithdrowErc20Token	컨트랙트에 입금된 ERC20 출금 시 이벤트 발생
Paused	컨트랙트 정지 시 이벤트 발생
Unpaused	컨트랙트 정지 상태 해제 시 이벤트 발생
OwnershipTransferred	컨트랙트 관리자 권한 이전 시 이벤트 발생

Function

컨트랙트의 함수들 로서 컨트랙트에 필요한 특정 로직을 담아 기능 실행을 하기 위해 사용

Function	Description
totalSupply	토큰 총 발행량 확인
balanceOf	특정 주소의 토큰 잔액 확인
transfer	특정 주소에게 토큰 전송
allowance	특정 주소에게 출금 위임된 토큰 잔액 확인
approve	특정 주소에게 출금 위임
tranferFrom	특정 주소에게 출금 위임된 토큰 전송
name	토큰 이름
symbol	토큰 심볼
decimals	토큰 데시멀
increaseAllowance	특정 주소에게 출금 위임된 토큰 잔액 증액
decreaseAllowance	특정 주소에게 출금 위임된 토큰 잔액 감액
_transfer	특정 주소에게 토큰 전송
_mint	토큰 추가 발행
_burn	토큰 소각

_approve	특정 주소에게 출금 위임
_setupDecimals	토큰 데시멀 설정
_beforeTokenTransfer	토큰 전송 전 검증
burn	토큰 소각
burnFrom	출금 위임된 토큰 소각
owner	컨트랙트 관리자 주소
transferOwnership	컨트랙트 관리자 권한 이전
paused	컨트랙트 정지 상태 확인
pause	컨트랙트 정지
unpause	컨트랙트 정지 상태 해제
setManager	매니저 권한 이전
setStakingContract	스테이킹 컨트랙트 주소 지정
openStaking	스테이킹 시작
closeStaking	스테이킹 종료
staking	스테이킹 컨트랙트로 토큰 전송
withdraw	스테이킹 컨트랙트로부터 토큰 출금
withdrawErc20	ERC20 출금
mint	토큰 추가 발행

Test Result

Code Coverage

코드 커버리지는 작성한 테스트가 얼마만큼 컨트랙트 코드의 기능들을 테스트 했는지 알 수있는 정량적인 지표입니다.

MPLE 컨트랙트는 라이브러리와 일부 컨트랙트에 구현된 기능에 대해 추가적인 호출이 진행되지않은 경우가 존재합니다.

아래의 **Coverage** 지표는 위 사항을 반영한 결과입니다.

File Name	Statements	Functions	Lines
MPLE.sol	64.34 % (92/143)	64.71 % (44/68)	67.81 % (99/146)

Test cases

Test case	Result
배포 시 지정한 토큰의 이름을 반환한다.	PASS
배포 시 지정한 토큰의 심볼을 반환한다.	PASS
배포 시 지정한 토큰의 데시멀을 반환한다.	PASS
배포 시 지정한 초기 발행량을 반환한다.	PASS
배포 시 지정한 초기 발행량은 컨트랙트 관리자에게 할당된다.	PASS
올바른 토큰 잔액을 반환한다.	PASS
보유 토큰 잔액을 초과하여 토큰 전송 시 예외처리가 된다.	PASS
0x0의 주소로 토큰 전송 시 예외처리가 된다.	PASS
특정 주소에게 출금 권한을 위임할 수 있다.	PASS
출금 권한을 위임받은 토큰 잔액을 올바르게 반환한다.	PASS
출금 권한을 위임받은 토큰 잔액을 증액 혹은 감액 가능하다.	PASS
출금 권한을 위임받은 토큰 잔액을 초과하여 토큰 전송 시 예외처리가 된다.	PASS
출금 권한을 위임받은 토큰을 0x0의 주소로 토큰 전송 시 예외처리가 된다.	PASS
컨트랙트의 관리자 주소를 올바르게 반환하다.	PASS
컨트랙트 관리자 외 주소로부터 관리자 권한 이전 시 예외처리가 된다.	PASS
컨트랙트 관리자는 관리자 권한을 이전 가능하다.	PASS
보유 토큰 잔액 이내에서 토큰 소각이 가능하다.	PASS
보유 토큰 잔액을 초과하여 토큰 소각 시 예외처리가 된다.	PASS

Test case	Result
출금 위임받은 토큰 잔액 이내에서 토큰 소각이 가능하다.	PASS
출금 위임받은 토큰 잔액을 초과하여 토큰 소각 시 예외처리가 된다.	PASS
컨트랙트의 관리자 외 주소로부터 컨트랙트 동결 시 예외처리가 된다.	PASS
컨트랙트가 동결 상태일 경우 토큰 전송 시 예외처리가 된다.	PASS
컨트랙트가 동결 상태일 경우 출금 위임된 토큰 전송 시 예외처리가 된다.	PASS
컨트랙트 관리자 외 주소로부터 토큰 추가 발행 시 예외처리가 된다.	PASS
컨트랙트 관리자는 토큰 추가 발행이 가능하다.	PASS
초기 발행량을 초과하여 토큰 추가발행 시 예외처리가 된다.	PASS
컨트랙트 관리자는 스테이킹 매니저 권한을 추가 변경이 가능하다.	PASS
컨트랙트 관리자 외 주소로부터 스테이킹 매니저 권한을 추가 변경 시 예외처리가 된다.	PASS
컨트랙트 스테이킹 매니저 외 주소로부터 스테이킹 시작 가능 상태 전환 시 예외처리가 된다.	PASS
컨트랙트 스테이킹 매니저는 스테이킹 시작 가능 상태로 전환이 가능하다.	PASS
컨트랙트 관리자는 스테이킹 컨트랙트를 지정 및 수정 가능하다.	PASS
컨트랙트 관리자 외 주소로부터 스테이킹 컨트랙트 지정 및 수정 시 예외처리가 된다.	PASS
스테이킹 시 스테이킹 컨트랙트로 지정 수량이 전달된다.	PASS
컨트랙트 관리자는 컨트랙트로 입금된 ERC20 토큰을 출금 가능하다.	PASS

Vulnerability Analysis

Critical Severity

심각성 치명적 단계는 일반적인 상황에서 보안 또는 큰 문제를 야기 할 수 있는 오류로 반드시 수정해야 하는 항목입니다

해당 항목 없음

High Severity

심각성 높음 단계는 일반적인 상황에서 발생하는 문제는 아니지만, 특수한 조건이나 예외상황에 의해서 문제가 발생 할 수 있는 항목입니다. 추가적인 예외처리나, 코너케이스에 대하여 분석하고 오류를 막을 수 있도록 수정이 필요한 항목입니다.

해당 항목 없음

Medium Severity

심각성 중간단계는 크게 문제가 되는 항목은 아니지만, 좀더 효율적으로 동작 할 수 있도록 수정을 권유하는 항목입니다

해당 항목 없음

Low Severity

낮은 위험도는 성능이나 보안에는 문제는 없지만, 코드 가독성, 컨트랙트 구조 개선을 위해 수정을 권유하는 항목입니다.

해당 항목 없음

Conclusion

MPLE 컨트랙트는 **ERC20** 표준 규격을 지킨 토큰 컨트랙트입니다.
컨트랙트 내 적용되는 모든 산술 연산에 대해 오버플로우/언더플로우 방지를 가능하도록 **SafeMath** 라이브러리를 적용하였습니다. 또한 일반적인 기능에 대해서는 검증된 **Openzepplin** 컨트랙트가 참조되었습니다.

주요 사항으로는 스테이킹 관련 기본 기능이 구현되어있어 이후 스테이킹 동작을 실현 가능합니다. 스테이킹에 대한 권한 분리를 하여 컨트랙트 관리자 외 매니저 권한을 통해 스테이킹을 시작 및 종료 할 수 있도록 하였습니다. 토큰 유통량에 직접적 영향을 줄 수 있는 토큰 소각 및 발행이 모두 구현되어있으나 토큰 추가발행의 경우, 초기 지정한 발행량을 초과할 수 없도록 하였습니다.

컨트랙트에 보안적 이슈를 발견하지 못하였습니다.

Declare

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

HEXLANT CONTRACT CERTIFICATION

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

PUBLISHIED INFORMATION

REPORT NUMBER	ERC20210329
DATE	2021/03/29
PUBLISHIER	SEONGEUN CHO eun@hexlant.com

TOKEN INFORMATION

TOKEN NAME	MPLE		
SYMBOL	MPLE		
PLATFORM	ETHEREUM	**TOKEN TYPE**	ERC-20
TOTAL SUPPLY	1,000,000,000 MPLE		
CONTRACT ADDRESS	0xC0c25245DCb2ee51594C4fA908b18DC4eDc0fa6E		

VULNERABLILLITY ANALYSIS

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

CENTRALIZED FUNCTIONS

FREEZE	NO	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	YES	Ability to increase total supply by minting tokens

Certified by Hexlant.

Hexlant.
Blockchain Lab
-
contact@hexlant.com
www.hexlant.com