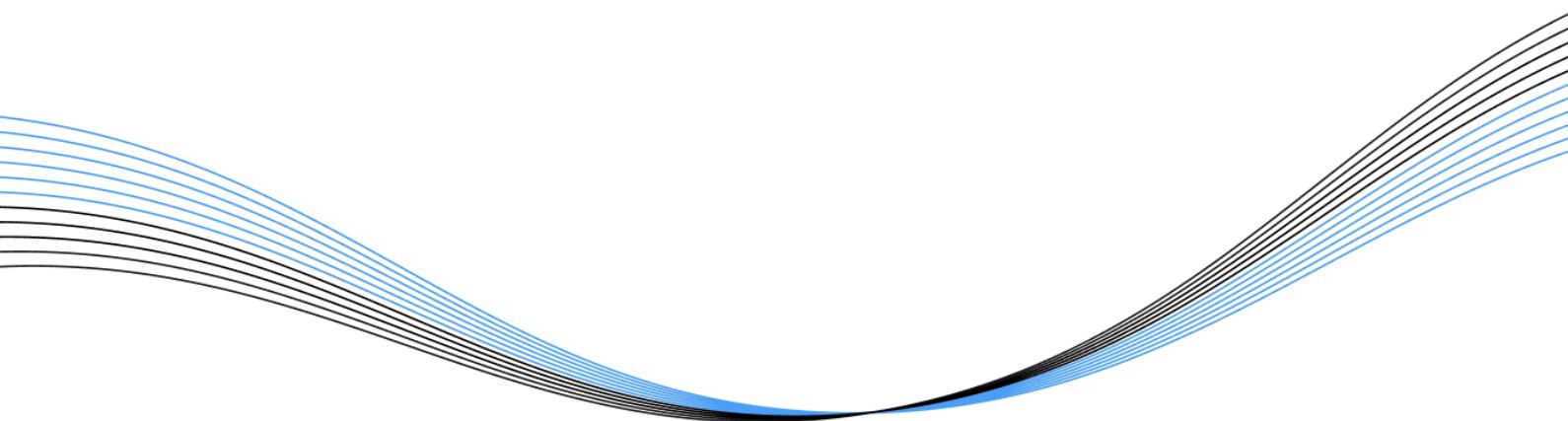


© Hexlant Inc.  
340 Gangnam-daero  
Seoul,  
Republic of Korea 06242  
Hexlant.com

# ORT

# SMART CONTRACT

# AUDIT REPORT



**Audit Date**  
21 FEB 2022

**Category**  
Token Contract

**Auditor**  
Hexlant Audit Team

This audit report specifies that the Hexlant Technical Team validated and notified that it has no technical defects.

# AUDIT

# OVERVIEW

---

## PUBLISHED INFORMATION

---

REPORT NUMBER	ERC20220221
DATE	2022/02/21
PUBLISHER	Eun /eun@hexlant.com

---

## PROJECT INFORMATION

---

TITLE	ORT		
SYMBOL	ORT		
PLATFORM	ETHEREUM	TOKEN TYPE	ERC-20
TOTAL SUPPLY	500,000,000 ORT		
CONTRACT ADDRESS	0x51f3E0Db1d24264230F2FdfDfC88F6D558D2171e		

---

## 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	YES	Ability to block token transfers for a period of time (Administrators can set lockout periods for investors, team members, advisors, etc.)
BURN	NO	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 키 관리, 블록체인 지갑 시스템 구축 등 블록체인 기술 전반의 서비스를 제공받을 수 있습니다. 현재 2000여개의 고객사가 Hexlant의 서비스를 바탕으로 블록체인 사업을 시작, 운영했으며 누적으로 관리하는 자산은 12조를 달성했습니다.

Initials for identification purposes:

  
For identification purposes  
**Hexlant.**

# CONTENTS

## **1. Analysis Purpose**

## **2. Function Summary**

- Variable
- Modifier
- Function

## **2. Test Result**

## **3. Vulnerability Analysis**

- Critical Severity
- High Severity
- Medium Severity
- Low Severity

## **4. Conclusion**

# ANALYSIS PURPOSE

본 리포트는 발행된 컨트랙트 코드가 요구사항을 충분히 만족하는지, 그리고 보안의 취약점과 실제 운영하면서 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 수정되어야 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.

---

## GONI 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.

## - **Pausable**

컨트랙트 정지에 관련된 기능을 제공합니다. 컨트랙트가 정지 상태일 경우, 모든 토큰 전송이 이뤄질 수 없도록 상태를 제한할 수 있습니다.

## - **ORT**

ORT의 메인 컨트랙트입니다. 락업, 동결, 업그레이드와 같은 생태계에 필수적인 기능을 추가 제공합니다.

## Function 1. Contract

상태 변수와 함수를 포함하여 컨테이너 형태의 계약을 표현하기 위해 사용

Contract	Description
Ownable	컨트랙트 오너쉽 관련 기능
PauserRole	컨트랙트 정지관리자 관련 기능
Pausable	컨트랙트 정지 상태 관련 기능
ERC20	ERC20 표준 인터페이스 관련 기능
ERC20Pausable	컨트랙트 정지에 대한 토큰 전송 관련 기능
ERC20Detailed	토큰 기본 정보 제공 기능
ORT	ORT 메인 기능

## Function 2. Interface

컨트랙트 내 구현하고자 하는 표준함수를 정의하기 위해 사용

Interface	Description
IERC20	ERC20 표준 인터페이스

## Function 3. Library

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

Library	Description
SafeMath	산술연산 제어
Roles	컨트랙트 내 권한 제어

## Function 4. Variable

컨트랙트의 상태를 표현하는 변수들로 컨트랙트에 필요한 정보들을 저장하기 위해 사용

Variable	Description
owner	컨트랙트 오너 주소
newOwner	컨트랙트 새로운 오너 주소
_pausers	정지관리자 주소 해시 테이블
_paused	컨트랙트 정지 상태
_balances	특정 주소의 토큰 잔액 해시 테이블
_allowed	특정 주소에게 출금이 위임된 토큰 잔액 해시 테이블
_totalSupply	토큰 총 발행량
_name	토큰 이름
_symbol	토큰 심볼
_decimals	토큰 최대 표현 가능한 소수점 자리수

implementation	업그레이드 컨트랙트 주소
timelockList	특정 주소의 작업 정보 리스트 테이블
frozenAccount	특정 주소의 동결 여부 해시 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
onlyNewOwner	컨트랙트의 새로운 오너만 실행 가능
onlyPauser	컨트랙트의 정지 관리자만 실행 가능
whenNotPaused	컨트랙트가 정지 상태가 아닐 경우 실행 가능
whenPaused	컨트랙트가 정지 상태일 경우 실행 가능
notFrozen	특정 주소가 동결 상태가 아닐 경우 실행 가능

#### 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
PauserAdded	컨트랙트 정지 관리자 권한 부여 시 이벤트 발생
PauserRemoved	컨트랙트 정지 관리자 권한 제거 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
Lock	락업 시 이벤트 발생
Unlock	언락 시 이벤트 발생

---

## Function 7. Function

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

Event	Description
isOwner	컨트랙트 오너인지 여부 확인
transferOwnership	컨트랙트 오너 권한 이전
acceptOwnership	컨트랙트 오너 이전 수락
isPauser	컨트랙트 정지 관리자인지 여부 확인
addPauser	컨트랙트 정지 관리자 권한 부여
removePauser	컨트랙트 정지 관리자 권한 제거
renouncePauser	컨트랙트 정지 관리자 권한 포기
_addPauser	컨트랙트 정지 관리자 권한 추가
_removePauser	컨트랙트 정지 관리자 권한 제거
paused	컨트랙트 정지 상태 여부 확인
pause	컨트랙트 정지 상태로 전환
unpause	컨트랙트 비정지 상태로 전환
totalSupply	토큰 총 발행량 확인
balanceOf	특정 주소의 토큰 잔액 확인
allowance	특정 주소에게 출금 위임된 토큰 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
_mint	토큰 발행
_burn	토큰 소각
_burnFrom	출금 위임된 토큰 소각
name	토큰 이름 확인
symbol	토큰 심볼 확인
decimals	토큰 최대 표현 가능한 소수점 자리수 확인
freezeAccount	특정 주소 동결
unfreezeAccount	특정 주소 동결 해제
lock	특정 주소의 보유 잔액 락업
transferWithLock	특정 주소에게 락업된 토큰 전송
unlock	특정 주소의 락업된 토큰 언락
upgradeTo	업그레이드 컨트랙트 주소
_lock	특정 주소의 보유 잔액 락업
_unlock	특정 주소의 락업된 토큰 언락
_autoUnlock	락업 된 토큰 중 만료기간이 지난 토큰 언락
_setImplementation	업그레이드 컨트랙트 주소 삽입

# TEST RESULT

## Code Coverage

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

GONI 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
GONI.sol	100% (128/128)	100% (54/54)	100% (135/135)

# TEST CASE

실제 적용한 테스트케이스 목록입니다.

Test Case	Result	
토큰 이름은 지정한 이름과 일치한다.	PASS	FAIL
토큰 심볼은 지정한 심볼과 일치한다.	PASS	FAIL
토큰 데시멀은 지정한 데시멀과 일치한다.	PASS	FAIL
지정한 초기 발행량이 총 발행량으로 할당된다.	PASS	FAIL
지정한 초기 발행량이 컨트랙트의 오너(배포 주소)에게 할당된다.	PASS	FAIL
배포 후 오너 외 주소들의 토큰 잔액은 0이다.	PASS	FAIL
토큰 전송 시 받는 주소가 0x0 일 경우 예외처리가 되는가?	PASS	FAIL
토큰 전송 시 보내는 수량이 음수 일 경우 예외처리가 되는가?	PASS	FAIL
토큰 전송 시 보유한 수량을 초과한 경우 예외처리가 되는가?	PASS	FAIL
특정 주소에게 출금 위임 시 해당 주소의 출금 위임 잔액이 증액하는가? P	PASS	FAIL
특정 주소에게 출금 위임된 토큰 잔액을 증액 혹은 감액할 수 있는가?	PASS	FAIL
출금 위임받은 토큰 전송이 가능한가?	PASS	FAIL
출금 위임받은 토큰 전송 시 관련 주소들의 토큰 잔액이 올바르게 업데이트 되는가?	PASS	FAIL
출금 위임받은 토큰 전송 시 받는 주소가 0x0일 경우 예외처리가 되는가?	PASS	FAIL
출금 위임받은 토큰 잔액을 초과한 수량을 전송 시 예외처리가 되는가?	PASS	FAIL
출금을 위임한 주소의 토큰 보유 잔액이 부족할 경우 예외처리가 되는가?	PASS	FAIL
컨트랙트 오너 여부를 확인할 수 있는가?	PASS	FAIL
컨트랙트 오너 외 주소로부터 오너 권한 이전을 제안 시 예외처리가 되는가?	PASS	FAIL
컨트랙트 오너는 자신의 오너 권한을 타 주소에게 이전을 제안하는 것이 가능한가?	PASS	FAIL
컨트랙트 오너 권한 이전을 제안받은 주소는 수락 가능한가?	PASS	FAIL
컨트랙트 오너 권한 이전 완료 후 새로운 오너의 주소는 0x0이 되는가?	PASS	FAIL
컨트랙트 정지관리자 외 주소로부터 락업된 토큰을 해제 시 예외처리가	PASS	FAIL

Test Case	Result	
되는가?		
컨트랙트 정지관리자는 특정 주소의 보유 토큰을 락업 가능한가?	PASS	FAIL
컨트랙트 정지관리자는 특정 주소에게 락업된 토큰을 전송 가능한가?	PASS	FAIL
컨트랙트 정지관리자는 특정 주소의 락업된 토큰을 해제 가능한가?	PASS	FAIL
만료기간이 지나지 않은 토큰 전송 시 예외처리가 되는가?	PASS	FAIL
만료기간이 지나지 않은 토큰에 대해 출금 위임을 통한 토큰 전송 시 예외처리가 되는가?	PASS	FAIL
컨트랙트 정지관리자 외 주소로부터 특정 주소 동결 시 예외처리가 되는가?	PASS	FAIL
컨트랙트 정지관리자 외 주소로부터 동결된 주소를 해제 시 예외처리가 되는가?	PASS	FAIL
컨트랙트 정지관리자는 특정 주소를 동결 가능한가?	PASS	FAIL
컨트랙트 정지 관리자는 특정 주소의 동결 상태를 해제 가능한가?	PASS	FAIL
동결된 주소는 토큰 전송 시 예외처리가 되는가?	PASS	FAIL
동결된 주소로 부터 출금 위임받은 토큰 전송 시 예외처리가 되는가?	PASS	FAIL
컨트랙트 정지관리자 외 주소로부터 특정 주소에 대해 정지관리자 권한 부여 시 예외처리 가 되는가?	PASS	FAIL
컨트랙트 정지관리자 외 주소로부터 특정 주소의 정지관리자 권한 제거 시 예외처리가 되는가?	PASS	FAIL
컨트랙트 정지관리자는 특정 주소에게 정지관리자 권한을 부여할 수 있는가?	PASS	FAIL
컨트랙트 정지관리자는 특정 주소의 정지관리자 권한을 박탈 가능한가?	PASS	FAIL
컨트랙트 정지관리자는 자신의 권한을 포기 가능한가?	PASS	FAIL
컨트랙트 배포 시 토큰 전송 이벤트가 발생하는가?	PASS	FAIL
토큰 전송 시 이벤트가 발생하는가?	PASS	FAIL
출금 위임 시 이벤트가 발생하는가?	PASS	FAIL
출금 위임 토큰 잔액 증액 및 감액 시 이벤트가 발생하는가?	PASS	FAIL
출금 위임된 토큰 전송 시 이벤트가 발생하는가?	PASS	FAIL
컨트랙트 오너 권한 이전 시 이벤트가 발생하는가?	PASS	FAIL
컨트랙트 정지관리자 권한 부여, 박탈 및 포기 시 이벤트가 발생하는가?	PASS	FAIL

# VULNERABILITY ANALYSIS

---

## GONI CONTRACT VULNERABILITY ANALYSIS

---

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

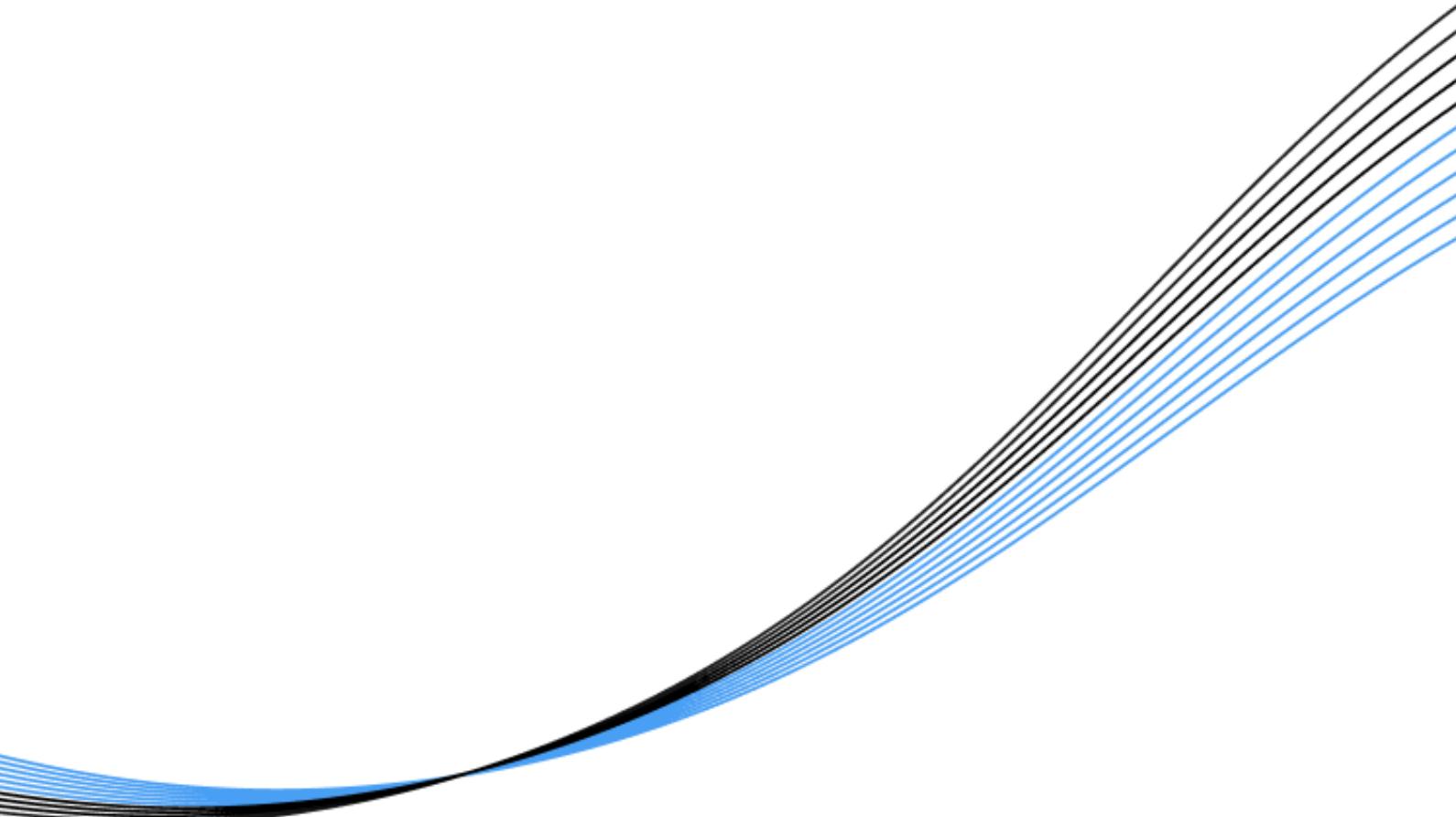
---

# CONCLUSION

ORT 컨트랙트는 ERC-20 인터페이스 기능과 더불어 락업, 동결, 업그레이드 기능을 추가로 구현한 컨트랙트입니다. 토큰 유통량에 영향을 줄 수 있는 추가 발행 및 소각은 불가능한 상태이며, 컨트랙트의 정지 관리자 권한을 통해 전체 생태계의 토큰 전송을 제제할 수 있을 뿐 아니라 특정 주소에 한해서만 동결도 가능합니다. 컨트랙트 구현 로직이 검증된 코드로 작성되었기 때문에 보안적 이슈를 발견하지 못하였습니다.

## 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](mailto:contact@hexlant.com)  
[www.hexlant.com](http://www.hexlant.com)