오리고
탈중앙화 어플리케이션을 위한
프라이버시 보호 플랫폼

오리고 파운데이션
support@origo.network

0.2 판

최종 업데이트: 2019 년 1 월 28 일

법적 고지: 본 문서는 기술개요의 목적으로 작성되었으며, 종합 혹은 최종 설계가 아닙니다. 본 문서는 핵심적이지 않은 요소는 다루지 않고 있습니다.

중요

본 백서를 읽기 전 부록의 법적 고지와 위험 요소 항목 전문을 반드시 읽으십시오

목차

1. 소개 **1**

1.1. 프라이버시 문제 1

1.2. 개발 내용 2

2. 개요 **3**

2.1. 프라이버시 목표의 범위 3

3. 오리고 프로토콜 **4**

3.1. 프라이버시 목표의 범위 4

3.2. 현재 솔루션의 한계 5

3.3. 프로토콜 개요 7

4. 기술 설계 **9**

4.1. 프로토콜 역할 9

4.2. 프로토콜 단계 9

4.2.1. 초기화 단계 10

4.2.2. 커밋 단계 10

4.2.3. 실행 단계 10

4.2.4. 결제 단계 11

4.3. 영지식증명 **12**

4.3.1. 오리고의 영지식증명 14

4.3.2. 신뢰설정 15
4.3.3. 안전 다중참여자연산과의 비교 16
4.3.4. 결론 16
5. 인프라 **18**
5.1. 이더리움 호환성 18
5.2. 비밀 트랜잭션 18
6. 향후 개선책 **20**
6.1. 합의 프로토콜 20
6.2. 샤딩 23
6.2.1. 연산 샤딩 23
6.2.2. 상태 샤딩 23
6.3. 가상 머신 24
7. 어플리케이션 **26**
7.1. 오리고가 가능케 한 어플리케이션들 26
7.1.1. 대중에 대한 프라이버시 26
7.1.2. 참여 당사자에 대한 프라이버시 28
7.2. 프라이버시 보호 어플리케이션 플랫폼 (PPAP) 28
7.3. 예시 28
8. 보안 **31**
8.1. 공정성 보장 31
8.2. 실행 완전성 - 당사자 31
8.3. 실행 완전성 – 실행자 32
9. 암호경제학 설계 **33**

9.1. 설계 원칙 33

9.2. 인센티브 및 역할 34

10. 로드맵 **37**

11. 커뮤니티 **38**

11.1. 주요 기여자 38

11.2. 기술 기여자 39

참고 문헌 **40**

A. 법적 고지 **43**

B. 위험 요소 **57**

제 1 장

소개

이더리움 (Ethereum) [1]은 코드 한 줄로 디지털 자산을 직접 컨트롤할 수 있도록 하여 보다 복잡한 어플리케이션 [2]에 대한 가능성을 열어준 스마트컨트랙트를 통해 비트코인 (Bitcoin) [3]을 한 단계 더 발전시켰습니다. 하지만, 현재의 스마트컨트랙트에는 프라이버시가 없습니다. 스마트컨트랙트에 입력되는 데이터와 그 실행 결과가 네트워크 전체에 공개되기 때문에, 프라이버시를 중시하는 현실의 많은 기업 및 개인이 스마트컨트랙트를 채택하고 사용하는 것을 꺼리고 있습니다 [4]. 블록체인의 강력한 기술들이 무신뢰한 당사자들이 안전하고 정확하게 상호작용할 수 있는 단초를 제공하긴 했지만, 오리고 (Origo)는 안전성과 정확성뿐만 아니라 프라이버시가 블록체인이 더욱 널리 퍼지게 해줄 열쇠라고 믿고 있습니다. 제로캐시 (Zerocash) [5]와 같은 블록체인의 진보는 비공개 트랜잭션을 가능케 했지만, 오리고는 거래 당사자들이 개인의 입출력 내역을 공개하지 않고도 스마트컨트랙트를 생성하고 실행할 수 있도록 함으로써 이러한 호크 (Hawk) [6]와 불렛프루프 (Bulletproof) [7] 등에 기반한 프라이버시 관련 작업에 한 단계 더 진보를 이루고자 합니다.

1.1. 프라이버시 문제

실제 세계의 정부와 중앙화된 사기업은 점점 더 어디에서나 시민과 고객들을 감시하고 있습니다. 머지않아 시민들과 고객들은 프라이버시에 대한 보다 근본적인 인권을 요구하게 될 것입니다. 전세계적으로 프라이버시에 대한 우려와 관심이 증가하자, 미디어는 계속해서 프라이버시에 관련된 사건사고에 대한 논란들을 다루고 있습니다. 이러한 예시로

는 정부의 감시 [8], 참가자들도 모르게 명시적인 통보 없지 진행되었다고 알려진 페이스북 (Facebook)의 대규모 과학 실험 등이 있습니다 [9].

공개된 블록체인에서 모든 프라이버시가 제한 없이 공개될 경우 지적 재산에 대한 소유권 및 권리 문제, 데이터 오남용, 적대적 행위 등의 문제를 일으킬 수 있기에 기업과 개인들은 이러한 노출에 대한 우려를 품고 있습니다.

계약에 있어 계약 당사자들은 계약금, 성능/치수 등의 중요 데이터, 계약의 선행조건 등 민감한 데이터와 내용에 대해 심대한 우려를 품고 있습니다. 이더리움 등의 전통적인 스마트컨트랙트는 이러한 민감한 계약 정보들을 보호하는데 실패하였고, 결과적으로 스마트컨트랙트의 산업적, 개인적 사용을 제한하였습니다.

1.2. 개발 내용

- **프라이버시 보호 어플리케이션 플랫폼**: 오리고의 프라이버시 보호 어플리케이션 플랫폼 (Privacy Preserving Application Platform, PPAP)은 혁신적인 프라이버시 프로토콜과 효율적인 영지식증명 (Zero Knowledge Proof, ZKP) 프레임워크를 결합함으로써 탈중앙화 어플리케이션 상의 입출력 데이터와 트랜잭션의 프라이버시를 보호합니다.

- **오프체인 (Off-Chain) 계산**: 오리고는 탈중앙화 어플리케이션의 오프체인 실행을 지원함으로써 어플리케이션 실행의 프라이버시를 보호할 뿐만 아니라 온체인 (On-Chain) 성능을 눈에 띄게 개선합니다.

- **향후 작업**: 향후 버전에서는 향상된 합의 프로토콜, 최첨단 샤딩 기술, 스테이트리스 클라이언트, 개선된 어플리케이션 런타임 환경 (가상 머신) 등의 성능 개선에 중점을 둔 수많은 유망 기술을 통해 프라이버시 보호 어플리케이션의 크로스체인 (Cross Chain) 지원, 신뢰설정 없는 영지식증명 프레임워크, 탈중앙화 어플리케이션을 위한 형식검증 도구, 고확장성 아키텍처 도입 등의 다양한 흥미로운 요소들이 도입될 것입니다.

제 2 장

개요

2.1. 프라이버시 목표의 범위

모네로 (Monero) [10], Z캐시 (ZCash) 등의 최근 프로젝트들은 새로운 비공개 암호화폐를 만들어냄으로써 프라이버시 문제를 해결하기 위해 노력하였지만, 이러한 프로젝트들은 영지식증명과 기타 기초적 암호법을 통해 트랜잭션의 기밀성을 보장하고자 했습니다. 오리고는 트랜잭션의 기밀성만을 보장할 뿐만 아니라 스마트컨트랙트 내에 작성된 탈중앙화 어플리케이션의 입출력 데이터의 프라이버시를 보장함으로써 보다 나은 프라이버시 보호를 제공하고자 합니다. 따라서 오리고는 상기 프로젝트들에 비해 유연성을 보이게 됩니다. 아래는 위에서 말한 트랜잭션의 기밀성에 집중한 프로젝트들과 오리고의 프라이버시 목표의 범위를 비교한 것입니다.

표 2.1에서 나타난 것처럼, 모네로/Z캐시/밈블윔블 (MimbleWimble) 등이 비공개 트랜잭션을 지원하는 비트코인의 포크라면, 오리고는 어플리케이션의 입출력 데이터 프라이버시를 보호하는 이더리움과 비슷한 개선된 탈중앙화 어플리케이션 플랫폼입니다.

모네로/Z캐시	**오리고**
송신자 주소	송신자 주소
트랜잭션 금액	트랜잭션 금액
수신자 주소	수신자 주소
-	어플리케이션 입력
-	어플리케이션 출력

표 2.1.: 오리고와 모네로/Z캐시의 프라이버시 범위 비교

제 3 장

오리고 프로토콜

3.1. 프라이버시 목표의 범위

프라이버시 보호 어플리케이션 플랫폼은 단순한 비공개 트랜잭션보다는 많은 기능을 제공합니다. 비공개 트랜잭션은 거래되는 금액과 함께 송신자와 수신자의 정보를 보호한다는 뜻입니다. 프라이버시 보호 어플리케이션은 비공개 트랜잭션의 기능뿐만 아니라 입출력 데이터의 프라이버시에 대한 보호 능력도 갖추고 있어야 합니다.

거래 당사자들은 자신들의 입력 데이터 (예를 들어, 갬블링의 선택 등)와 화폐 단위 (예를 들어, 경매의 입찰)를 시스템에 제공합니다. 시스템은 이러한 입력값을 수신한 뒤 오프체인으로 어플리케이션을 실행하고 거래 당사자들에게 배당된 지불금을 암호화하여 출력합니다. 시스템은 입력값의 프라이버시와 실행의 공정성을 보장할 필요가 있습니다.

- **입/출력의 프라이버시**: 어플리케이션의 입출력 (데이터 및 화폐량 포함)은 보호되어 공개되어서는 안됩니다. 즉, 입출력 내용은 암호화되어 공개되어서는 안됩니다. 이를 위해서는 블록체인을 오가는 모든 정보는 암호화되어야 하며 컨트랙트 실행을 보장하기 위해 영지식증명이 사용되어야 합니다.

- **실행의 공정성**: 탈중앙화 어플리케이션, 특히 다수의 당사자가 존재하는 경우에 대해서는 프라이버시를 일반 대중으로부터 보호하는 것만으로는 부족합니다. 거래 당사자들이 자신의 이익을 극대화하기 위한 이기적인 존재라고 가정했을 때, 그들은 실행 이전에 트랜잭션을 중단할 수도 있습니다. 따라서 시스템은 거래 당사자들 간의 공정성도 보장할 필요가 있습니다.

오리고는 탈중앙화 어플리케이션을 비공개로 안전하게 실행할 수 있는 솔루션을 제안합니다. 입출력 데이터 프라이버시를 보호하기 위해 오리고는 탈중앙화 어플리케이션을 오프체인 환경에서 실행합니다. 오프체인 실행의 증명은 올바른 계산에 대한 검증을 위해 온체인으로 제출되어야 합니다.

어플리케이션 개발자들은 암호법에 대해 알 필요는 없습니다. 오리고의 프라이버시 보호 어플리케이션 플랫폼 (Privacy-Preserving Application Platform, PPAP)에서 개발자들이 원래 하던 방식대로 어플리케이션을 작성하면 오리고 PPAP가 입출력 데이터의 유출 없이 어플리케이션을 컴파일하고 실행합니다. PPAP는 개발자들이 쉽고 편하게 프라이버시 보호 어플리케이션을 구출할 수 있도록 해줍니다.

효율성과 프라이버시를 보장하기 위해 오리고는 온체인 및 오프체인 계산을 모두 지원합니다. 프라이버시가 요구되는 어플리케이션의 실행 및 정당성 검증은 오프체인으로 실행됩니다. 프라이버시 보호 어플리케이션의 계산 검증과 일반 어플리케이션의 실행은 온체인으로 진행됩니다. 저희는 어플리케이션의 오프체인 실행의 세부사항은 보호하는 동시에 그 실행의 정당성에 대해서는 공개 블록체인이 정당성을 입증할 수 있도록 영지식증명을 사용합니다. 또한 오리고는 악의를 지닌 당사자가 컨트랙트를 중단하지 못하도록 하는 적절한 경제적 메커니즘을 제안합니다.

3.2. 현재 솔루션의 한계

현존하는 블록체인 기술을 통해 튜링 완전한 프라이버시 보호 어플리케이션을 적용할 수 있는 간단한 방법은 존재하지 않습니다.

이더리움은 튜링 완전한 어플리케이션을 지원하는 무허가형 공개 블록체인입니다. 이더리움은 그 어떠한 트랜잭션 상의 프라이버시도 제공하지 않습니다. 컨트랙트가 올바르게 실행되었나 검증하기 위해서는 각 노드가 컨트랙트를 실행해야 합니다. 따라서, 각 컨트랙트의 입력, 중간 상태, 출력 데이터는 이더리움의 모든 노드에 대해 공개됩니다.

이더리움의 특정 어플리케이션에 대해서 일정 수준의 프라이버시를 보호할 수 있는 테크닉이 있습니다. 예를 들어, 두 거래 당사자가 이더리움 스마트컨트랙트를 이용해서 가위바위보를 할 때 한 쪽이 컨트랙트에 직접 패를 게시하게 되면 다른 한 쪽은 첫 번째

당사자의 선택을 읽고 유리한 패를 제시함으로써 이득을 취할 수 있습니다. 이러한 방식 대신, 두 당사자는 컨트랙트의 자신의 선택의 해쉬값과 무작위한 스트링을 게시하고, 두 당사자 모두가 입력을 커밋하고 나면 컨트랙트에 무작위 스트링에 대응하는 자신의 선택을 공개하여 입력값을 공개하는 방식을 사용할 수도 있습니다. 그러면 컨트랙트는 각 거래 당사자가 주장하는 입력값과 무작위 스트링을 조합한 것이 제출된 해쉬값과 일치하는지 검사함으로써 각 당사자의 입력값을 구할 수 있습니다. 코드 3.1은 위에 설명한 솔루션을 보여주고 있습니다. 이러한 테크닉은 두 당사자가 한쪽이 상대방의 선택을 보고 그에 맞는 선택지를 제시할 수도 있다는 우려를 할 필요 없이 게임을 진행할 수 있도록 해줍니다. 하지만 이러한 게임의 결과는 여전히 공개된 상태입니다. 누구나 누가 게임을 이겼으며 승자에게 얼마가 지급되었는지 열람할 수 있습니다.

```
def commit(party, choice, random_string):
    commitment = HASH_FUNC(choice, random_string)
    party.send(commitment)

def reveal(party, choice, random_string):
    WAIT_UNTIL(len(commitments) == 2, TIMEOUT(T))
    expected_commitment = HASH_FUNC(choice, random_string)
    received_commitment = commitments[party]
    if expected_commitment == received_commitment:
        return (party, choice)
    return (party, NULL_CHOICE)

def execute(parties, party_choices):
    if winner(party_choices) == parties[0]:
        transfer_all_fund_to(parties[0])
    elif winner(party_choices) == parties[1]:
        transfer_all_fund_to(parties[1])
    else:
        refund_all_parties(parties)
```

리스팅 3.1.: 가위바위보 게임을 하기 위한 이더리움 상의 스마트컨트랙트의 의사코드

Z캐시 및 모네로와 같은 암호화폐는 비공개 트랜잭션을 지원함으로써 이러한 문제를 해결했지만 스마트컨트랙트를 지원하지는 않습니다. 오리고는 탈중앙화 어플리케이션에 대해 비공개 트랜잭션과 스마트컨트랙트를 모두 지원할 것입니다. 또한 프라이버시 보호 어플리케이션의 입출력 데이터가 공개되는 것을 방지하기 위해 해당 어플리케이션은 오프체인으로 실행될 것입니다. 해당 어플리케이션의 실행은 여전히 검증을 받아야 하긴

하지만 영지식증명을 통해 실제 결과를 공개하지 않고도 검증이 진행됩니다. 모든 적절한 프로토콜은 거래 당사자들이 규칙에 따라 행동하도록 유인을 제공하게 설계되었습니다.

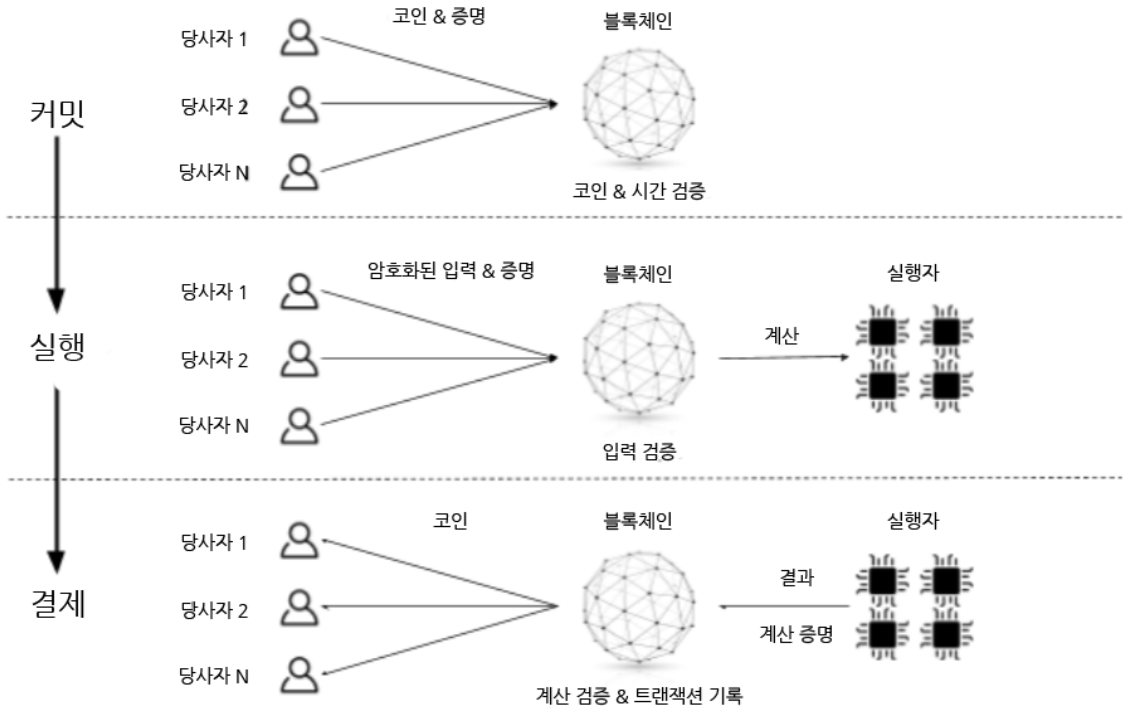


그림 3.1.: 프로토콜 도해

3.3. 프로토콜 개요

상기 한계점들을 해결하기 위해 오리고는 비공개 트랜잭션과 스마트컨트랙트를 모두 지원합니다. 호크 [6]로부터 영감을 받아 저희는 온체인 계산과 오프체인 계산을 결합하여 스마트컨트랙트 실행 시의 프라이버시를 지키는 프로토콜을 소개합니다.

그림 3.1.에 나타난 것처럼, 저희 프로토콜에는 **초기화**, **커밋**, **실행**, **결제**의 네 단계가 있습니다. 아래는 이 네 단계에 대한 간략한 설명입니다. 좀 더 자세한 설명은 다음 장에서 다루도록 하겠습니다.

커밋 단계에서 각 당사자는 자신의 코인을 컨트랙트에 동결시키고 자신의 비공개 입력값과 코인을 포함하고 있는 커밋먼트를 제출합니다. 커밋먼트 스킴을 이용함으로써 입력 데이터와 코인은 비공개가 되지만 제출 당사자는 커밋먼트 이후에 해당 내용을 바꾸지 못합니다. 모든 당사자가 커밋먼트를 제출하거나 단계의 타임아웃이 도래하면 예치금이 검증됩니다. 이는 다음 단계로 넘어갑니다.

실행 단계에서 각 당사자는 자신의 비공개 입력 데이터를 오프라인 실행자에게 공개합니다. 실행자는 스마트컨트랙트를 오프라인으로 실행함으로써 입력 데이터와 실행 결과가 공개되지 않도록 합니다.

컨트랙트가 실행된 뒤, 실행자는 컨트랙트가 올바르게 실행되었는지에 대해 영지식증명을 생성합니다. 블록체인이 정당성을 검증하고 나면 실행 결과에 따라 자금이 당사자들에게 분배됩니다.

이러한 프로토콜을 사용함으로써 사용자 입력값, 트랜잭션 금액, 컨트랙트 실행 정보 등이 비공개로 유지됩니다. 하지만 여전히 누구나 컨트랙트가 올바르게 실행되었는지 검증할 수 있습니다.

제 4 장

기술 설계

4.1. 프로토콜 역할

오리고 프로토콜은 스마트컨트랙트 실행의 한 주기 동안 크게 세 가지 역할을 맡습니다:

- **당사자**: P_1, …, P_N, 스마트컨트랙트 SC에 참여하는 일련의 사용자들.
  당사자들은 비공개 입력값 I^{priv}_1, …, I^{priv}_N, 공개 입력값 I^{pub}_1, …, I^{pub}_N, 그리고
  코인 C_1, …, C_N을 제출합니다.

- **블록체인**: B, 당사자자들 간의 트랜잭션을 효율적으로, 그리고 검증 가능하고
  영구적인 방식으로 기록하는 공개된 분산 원장입니다.

- **실행자**: PE, 오리고의 스마트컨트랙트의 실행을 가능케 하는 특수한 당사자.
  실행자는 각 당사자에게 결과값 O_1, …, O_N을 출력합니다.

4.2. 프로토콜 단계

오리고 프로토콜은 *초기화, 커밋, 실행, 결제*의 네 단계로 이루어져 있습니다. 이러한 네 단계는 T_1과 T_2, 두 타임아웃으로 엄격하게 경계 지어져 있으며, $T_{commit} < T_1$이고 $T_1 \leq T_{execute} < T_2$입니다. 아래는 각 단계에 대한 기술적 세부사항입니다.

4.2.1. 초기화 단계

당사자들은 블록체인 B의 노드 N_i를 실행자 P_E로 선출하고 P_E의 공개키 K_E가 모든 당사자들에게 공유됩니다.

4.2.2. 커밋 단계

각 당사자 P_i ($i \in [N]$)는 스마트컨트랙트에 예치하고자 하는 만큼의 코인 C_i ($i \in [N]$)를 자신의 월렛으로부터 동결합니다. 각 당사자는 동결된 코인 C_i에 대한 커밋먼트 $cm = comm(C_i \| I^{priv}_i)$과 영지식증명 $Proof_{ci}$ ($i \in [N]$)를 계산합니다. 커밋먼트 cm과 $Proof_{Ci}$,는 T_1 이전에 블록체인 B로 보내져야 하며, 만약 그렇지 못할 경우 당사자는 컨트랙트의 참가자로 인정받지 못합니다.

블록체인 B는 각 당사자가 보낸 $Proof_{Ci}$를 검증하고 T_1이후에 그 어떠한 새로운 당사자도 추가되지 않도록 할 의무가 있습니다. 만약 모든 의무 당사자가 입력값과 코인을 커밋 했다면 컨트랙트는 실행 단계로 진행됩니다. 만약 그렇지 않았다면 컨트랙트는 중지되고 모든 커밋 된 코인은 각 당사자들에게 환급될 것입니다.

이 단계의 목적은 각 당사자가 자신의 입력값과 코인을 비공개로 제출하는 것입니다. 그 누구도 (심지어는 실행자도) 이 단계에서는 다른 당사자의 입력값이나 코인을 알 수 없습니다. 이 단계 이후에는 당사자들의 입력값과 스마트컨트랙트에 예치된 코인은 불변합니다. 그 누구도 다른 당사자의 입력값을 알게 된 이후에 자신의 입력값이나 코인을 변경함으로써 이들을 취할 수 없습니다.

4.2.3. 실행 단계

각 당사자 P_i ($i \in [N]$)는 자신의 비공개 입력값 I^{priv}_i와 코인 C_i ($i \in [N]$)에 대한 정보를 실행자 P_E의 공개키 K_E로 암호화합니다. 또한 영지식증명 $Proof_{Ei}$ ($i \in [N]$)를 구축해 암호화된 값이 자신의 커밋먼트 cm과 일치함을 증명합니다. 암호화된 데이터 $ENC(I^{priv}_i \| C_i)$와 그에 따른 증명 $Proof_E$는 블록체인으로 송신됩니다.

일단 블록체인이 암호화된 데이터와 증명을 각 당사자로부터 수신하면, B는 각 당사자들의 암호화 데이터 $ENC(I^{priv}_i \| C_i)$가 커밋 단계에서 제출된 커밋먼트 cm = comm (Ciǁ Iprivi)과 일치하는지 검증합니다. 이는 다른 당사자가 암호화된 데이터를 제출한 이후에 어느 누군가가 자신의 입력 데이터를 변경하는 것을 방지합니다. B가 성공적으로 $Proof_{Ei}$를 검증하였고 현재 시간이 $T_1 \leqq T < T_2$임이 확인되었다면 B는 암호화된 데이터를 실행자 P_E에게 송신합니다.

검증된 암호화 데이터를 블록체인 B로부터 수신하고 나면 실행자 P_E는 자신의 개인키 PK_E를 통해 각 당사자의 I^{priv}_i와 C_i를 해독하고 스마트컨트랙트를 실행합니다.

T_2 이전에 어떠한 당사자라도 암호화된 데이터와 증명을 블록체인에 송신하는 것에 실패하거나 증명이 올바르지 않다면 해당 당사자는 컨트랙트를 중단하는 것으로 간주됩니다. 컨트랙트의 요건에 따라 해당 당사자의 예치금에 대해 적절한 제제가 가해질 것입니다.

만약 실행자가 타임아웃 이전에 출력값과 증명을 블록체인에 송신하지 못한다면 실행자는 컨트랙트를 중단한 것으로 간주됩니다. 악의적인 실행자가 특정 당사자에게 유리하지 않은 실행 결과가 나타날 경우 컨트랙트를 의도적으로 중단할 수도 있기 때문에, 이를 방지하기 위해 저희는 실행자가 일정 금액의 예치금을 지불할 것을 요구하고 있습니다. 실행자가 결과 혹은 증명을 제출하지 못한다면 해당 실행자는 예치금을 잃게 됩니다.

실행자가 실행 이후에 각 당사자의 입력값 및 출력값을 공개하지 않도록 하기 위해 실행을 Intel SGX [11] 등의 신뢰할 수 있는 하드웨어에서 하는 것도 좋은 아이디어입니다.

4.2.4. 결제 단계

일단 실행자 P_E가 실행을 끝마치고 나면 각 당사자 P_i ($i \in [N]$)에 대한 출력값 $O_1, \ldots, O_N$이 생성됩니다. P_E는 출력값이 각 당사자들의 입력값과 스마트컨트랙트에 따라 올바르게 계산되었음을 증명하기 위해 증명 $Proof_E$를 생성하고 출력값 $O_1, \ldots, O_N$을 각 당사자들의 공개키 KP_i ($i \in [N]$)를 통해 $ENC(O_1), \ldots, ENC(O_N)$으로 암호화합니다. 그리고 P_E는 $Proof_E$

와 $ENC(O_1)$, …, $ENC(O_N)$를 블록체인 B로 송신합니다.

B는 컨트랙트가 올바르게 실행되었는지를 확인하기 위해 $Proof_E$를 검증하고 실행 결과에 따라 각 당사자에게 코인을 분배합니다.

마지막으로 각 당사자는 결과값을 해독합니다. 만약 당사자가 컨트랙트로부터 코인을 얻었다면 해당 당사자는 비공개 트랜잭션을 통해 코인을 월렛에 넣을 수 있습니다.

4.3. 영지식증명

영지식증명 (Zero Knowledge Proof, ZKP)는 오리고가 스마트컨트랙트를 올바르고 완전하게 실행하면서도 프라이버시를 보장할 수 있게 해주는 핵심 기술입니다. 영지식증명은 잘 구축된 암호법적 방법입니다. 영지식증명에서, 두 당사자가 있다고 가정할 때 한 당사자, 즉 증명자 (prover)는 다른 한 당사자, 즉 검증자 (verifier)에게 어떠한 정보도 공유하지 않고도 어떠한 명제가 왜 사실인지 증명할 수 있습니다. 영지식증명 프로토콜은 아래의 속성을 반드시 만족해야 합니다.

- **완전성**: 증명자와 검증자가 정직하다고 가정할 때 영지식증명 프로토콜은 압도적인 확률로 성공합니다.

- **건전성**: 비밀을 알지 못하는 그 누구도 무시할 수 없는 확률로 검증자를 확신시킬 수 없습니다.

- **영지식**: 증명 과정에서 그 어떠한 추가적인 정보도 유출되지 않습니다.

영지식증명 프로토콜을 생성하는 매우 직관적인 방법으로는 대화식 영지식증명 (Interactive Zero Knowledge Proof, IZKP)라고 불리는, 검증자와 증명자 간의 상호작용 및 의사소통이 허용되는 방식이 있습니다. 검증자는 증명자가 비밀 정보를 알고 있고 증명자가 비밀 정보를 알고 있다면 질문에 대답할 수 있다는 전제 하에 증명자에게 어떠한 질문이라도 (심지어 무작위로도) 할 수 있으며, 물론 증명자의 이전 답변에 기반하여 질문을 생성하는 것도 허용됩니다.

어떠한 대화식 영지식증명도 (만약 검증자가 공개된 코인 검증자일 경우, 예를 들어 검증자에 의한 무작위 선택이 공개적으로 이루어지는 등) 피아트-샤미르 휴리스틱을 사용하는 랜덤 오라클 모델 하에서 안전하고 영지식적인 비대화식 영지식증명으로 전환될 수 있습니다 [12]. 모든 무작위 질문은 해쉬값으로 대체됩니다. 더 자세히 말하자면, 비대화식 영지식증명 (Non-Interactive Zero Knowledge Proof, NIZK)은 사용자의 입력값을 노출하지 않는 스마트컨트랙트를 가능케 하기 위한 도구로서 학계에서 제안된 것입니다 [6, 13, 14]. 하지만 비대화식 영지식증명은 스마트컨트랙트를 갖춘 블록체인을 통한 의사소통의 비용이 비싸고 스마트컨트랙트 자체의 계산 능력이 매우 제한적이기 때문에 스마트컨트랙트에서의 실제적 사용에 있어서 한계를 지니고 있습니다. 심지어 현재 널리 사용되는 SNARK {15}에서도 스마트컨트랙트에 대한 중립적인 선택은 복잡한 신뢰설정이 필요합니다. 신뢰설정의 핵심인 공통참조스트링 (Common Reference String, CRS)은 일반적으로 길뿐더러 개별 스마트컨트랙트에 특정되어 있고 잠재적인 트랩도어로 인해 스킴을 신뢰할 수 없도록 만듭니다.

모든 디지털 회로의 핵심인 연산회로 (Arithmetic Circuit, AC)는 어떠한 수학적 표상을 형성하는 데에든 사용될 수 있습니다. 연산회로는 덧셈, 뺄셈, 곱셈, 나눗셈 등 작은 논리적 작업의 조합입니다. 예를 들어, 그림 **4.1.**은 (a+b)×c/d를 계산하기 위한 연산회로 형식을 나타내고 있습니다.

(a) 모든 계산 조건이 참, 거짓으로 나뉘는 불값으로 이루어진 입출력값을 취하는 연산회로로 표현될 수 있으며, 그리고 (b) 형식적으로 특정된 언어 내에서 튜링 완전한 스마트컨트랙트는 연산적 조건의 복잡한 집합체 및 상호작용으로 볼 수도 있다는 사실을 고려할 때, 스마트컨트랙트를 연산회로로 옮기는 것은 놀라운 일이 아닙니다. 임의의 연산회로에 대해 효율적인 영지식증명을 생성하기 위한 다양한 방법들이 제시되었습니다 [7, 16]. 예를 들자면 증명자가 연산회로를 만족시키거나 연산회로의 출력값을 참으로 만드는 특정 입력값을 가지고 있음을 증명할 수 있게 하는 방법이 제시되었습니다. 따라서 컨트랙트에 대한 데이터나 정보의 공유 없이도 컨트랙트 실행의 정당성을 증명하는 것이 가능해졌습니다.

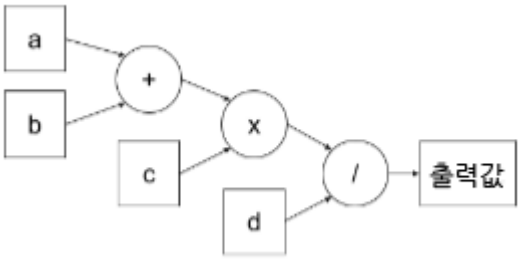


그림 4.1.: 연산회로의 예시

4.3.1. 오리고의 영지식증명

오리고에서 영지식증명은 트랜잭션 정보 (송신자 및 수신자 주소, 트랜잭션 금액)와 스마트컨트랙트의 입출력값을 보호하기 위해 사용됩니다. 섹션 3.3.의 내용을 기반으로, 비공개 스마트 컨트랙트를 실행할 때, 다수의 단계에서 당사자 P_i (i∈[N])와 실행자 P_E의 커밋먼트를 증명하고 검증하기 위해 영지식증명을 요구합니다.

- **커밋 단계**: 당사자 P_i (i∈[N])는 스마트컨트랙트 SC에 자신이 충분한 코인 C_i (i∈[N])를 예치했음을 증명해야 합니다.
  - $statement := NIZK.Prove(P_i, (C_i||K_i), witness) \quad (i \in [N])$
  - $NIZK.Verify(P_i, statement)$

- **계산 단계**: 당사자 P_i (i∈[N])는 스마트컨트랙트 SC에 대한 비공개 입력값 I^{priv}_i (i∈[N])이 실행자의 공개키 K_E로 올바르게 암호화되었음을 증명해야 합니다.
  - $I_i^{priv} := ENC(I_i, K_E) \quad (i[N])$(Off-chain)
  - $statement := NIZK.Prove(P_i, I_i^{priv}, witness) \quad (i \in [N])$
  - $NIZK.Verify(P_i, statement)$

- **결제 단계**: 실행자 P_E는 자신이 성공적으로 스마트컨트랙트 SC를 실행시켜 정당한 결과값 O_i (i∈[N])를 냈음을 증명해야 합니다.
  - $statement := NIZK.Prove(P_i, I_i^{priv}, witness) \quad (i \in [N])$
  - $statement := NIZK.Prove(P_i, O_i, witness) \quad (i \in [N])$

증명 시스템	zk-SNARK	zk-STARK	불렛프루프
증명 크기	짧음	중간에서 짧음	짧음
증명자 시간	FFT	FFT (높은 메모리 소비)	선형적
검증자 시간	효율적	효율적	선형적
신뢰설정	필요	불필요	불필요
실용성	예	아니오	예

표 4.1: 영지식증명 시스템간 비교

위에서 설명한 오리고의 모든 증명 과정은 오프체인으로 진행되고 완료까지 수 초에서 수 분까지 걸릴 수 있습니다. 각각의 비대화식 영지식증명 시스템은 온체인 검증 동안 서로 다른 성능을 보입니다. 검증 성능의 차이는 신뢰설정 과정과 증명/검증 크기 간의 제로섬입니다.

4.3.2. 신뢰설정

위에서 설명한 바와 같이 현재 기술의 대부분은 각 어플리케이션에 대한 신뢰설정 단계가 필요하고, 신뢰할 수 있는 제 3자 혹은 다중참여자연산 (Multi-Party Computation, MPC)이 사용되어야 합니다. 하지만 오리고는 프라이버시 보호 스마트컨트랙트를 지원하도록 설계되었으므로 고유의 공통참조스트링을 생성하기 위해 각각의 스마트컨트랙트가 신뢰설정을 필요로 합니다. 어떠한 신뢰설정 과정을 거치든지, 신뢰설정은 프라이버시 보호 스마트컨트랙트를 무겁고 유연성이 떨어지게 만듭니다. 따라서, 프라이버시 보호 스마트컨트랙트 측면에 있어서 신뢰설정을 생략하는 것은 오리고를 실용적으로 만드는데 필수불가결한 부분입니다. 비공개 트랜잭션에 대해서는 신뢰설정 과정이 한 번만 이루어지므로 이 경우에는 감수할 수 있으며 이미 업계에서는 유효한 설정식에 대한 쇼케이스를 진행하였음에 유의하여 주십시오.

저희는 신뢰설정이 없는 유효한 영지식증명 프로토콜을 제공하기 위해 몇 가지 새로운 기술들을 조사하였고 [7, 15], 표 4.1.에 나타난 것처럼, 현재 실용성이 있는 신뢰증명이 불필요한 증명 시스템은 보다 떨어지는 검증자 효율성을 가지고 있었습니다. 높은 검증자 비용은 검증이 온체인으로 이루어질 경우 합의 속도를 더욱 떨어트립니다. 신뢰

설정이 없는 새로운 증명 시스템으로 인해 발생하는 이러한 결점을 최소화하기 위해 오프체인 검증이 필요합니다.

기능	안전 다중참여자연산 (Secure Multi-Party Computation)	오리고
성능	나쁨	준수
출력값의 프라이버시	아니오	예
동기화	필요	불필요

표 4.2.: 안전 다중참여자연산과 오리고의 비교

4.3.3. 안전 다중참여자연산과의 비교

저희는 영지식증명 외에도 동형암호 (homomorphic encryption)과 안전 다중참여자연산 등 기타 프라이버시 보호 기술에 대한 연구도 진행하였습니다. 안전 다중참여자연산은 당사자들이 입력값은 비공개로 유지하면서도 자신들의 입력값에 대한 함수는 공동으로 계산하도록 해줍니다. 스마트컨트랙트에 이러한 기술을 적용했을 때, 안전 다중참여자연산은 당사자들이 입력값은 비공개로 유지하면서도 스마트컨트랙트 실행의 출력값을 공동으로 연산할 수 있도록 해줍니다.

하지만 다중참여자연산은 당사자 간의 다회에 걸친 상호작용을 필요로 하지만 비대화식 영지식증명은 증명자와 검증자 간의 상호작용을 요구하지 않습니다. 또한 모든 참여 당사자들이 실행 결과를 비공개로 유지하게 할 실행 접근법이 없습니다. 가장 중요한 것은, 다중참여자연산의 계산 복잡성은 영지식증명의 그것보다 월등히 높으며, 다중참여자연산은 제한적인 범위의 실제 어플리케이션에만 적용 가능합니다. 따라서, 저희는 영지식증명이 프라이버시 보호 어플리케이션 플랫폼의 구축에 더 어울린다고 생각합니다.

4.3.4. 결론

영지식증명이 보다 효율적인 검증 시간을 나타내며 검증이 블록체인 상에서 이루어질 수도 있으므로, 비공개 트랜잭션의 효율성을 보장하기 위해 저희는 비공개 트랜잭션 검증

에 신뢰설정이 필요한 영지식증명을 적용하는 것을 선호합니다. 또한 각 프라이버시 보호 스마트컨트랙트가 개별적인 신뢰설정을 실행하는 것은 실용적이지 못하므로 저희는 컨트랙트 실행을 검증하는데 신뢰설정을 필요로 하지 않는 영지식증명 기술을 적용하였습니다.

제 5 장

인프라

5.1. 이더리움 호환성

현재 오리고의 체인 인프라는 작업증명 합의, EVM, 솔리디티 등, 이더리움의 기능에 호환됩니다. 최초에 저희들은 저희의 플랫폼을 이더리움의 비잔티움 포크 기분으로 개발하였습니다. 저희가 첫 번째 단계로 이더리움 호환 인프라를 선택한 이유는 이더리움 커뮤니티가 활동 중인 개발자들이 가장 많은 커뮤니티이므로 저희가 프라이버시 기술의 최적화에 더욱 많은 자원을 투자할 수 있었기 때문입니다. 프라이버시 보호 기능은 추가적인 연산 자원을 요구하기 때문에 저희의 현재 플랫폼의 블록 가스 한도는 현재 이더리움의 한도보다 높게 설계되었습니다. 하지만 이더리움 호환 인프라는 몇 가지 확장성 문제를 가지고 있으며, 저희는 오리고 플랫폼의 향후 버전에서 이러한 문제를 해결하고자 합니다.

5.2. 비밀 트랜잭션

비밀 트랜잭션의 목표는 트랜잭션 내의 데이터가 비공개로 남는 것입니다. Z캐시와 비슷하게, 비밀 트랜잭션 역시 비공개 주소를 사용합니다. 두 비공개 주소 간의 트랜잭션은 송신자, 수신자, 트랜잭션 금액 등의 정보를 제 3자에게 전혀 유출하지 않습니다. 사용자는 공개 주소에서 비공개 주소로 토큰을 옮길 수도, 그 반대로 할 수도 있습니다. 저희는 영지식증명 시스템 zkSnark를 사용해 트랜잭션 데이터를 비공개로 유지합니다. 하지

만 여전히 비밀 트랜잭션의 정당성 (예를 들어 송신자가 비공개 주소의 토큰을 사용하기 위한 비밀을 알고 있는지, 투입 토큰의 총량이 배출 토큰의 총량과 같은지 등)은 공공에 의해 검증될 수 있습니다.

제 6 장

향후 개선책

이더리움과 유사한 인프라로는 플랫폼을 극단적으로 효율적으로 만드는 데 있어 몇몇 확장성 한계를 겪고 있습니다. 따라서, 저희의 향후 플랫폼 개선책은 주로 보다 나은 확장성을 확보하는데 주안점을 두고 있습니다.

- **최적화된 합의** – 트랜잭션 처리량을 개선하기 위한 하이브리드 합의 프로토콜
- **샤딩** – 오리고를 선형적으로 확장 가능하게 하기 위한 최첨단 샤딩 프로토콜
- **향상된 가상 머신** – 스마트컨트랙트의 실행 속도를 개선하기 위한 새로운 가상 머신 표준

본 백서에서 아래 섹션은 이러한 기술들을 간략히 설명합니다. 일단 저희가 이러한 잠재적 기술들에 대한 보다 구체적인 설계안을 만들게 되면 보다 자세한 문서를 발행할 것입니다.

6.1. 합의 프로토콜

합의 프로토콜은 네트워크 상의 노드들이 어떻게 값에 대한 합의에 도달하는지를 특정합니다. 합의 프로토콜은 노드의 불이행, 네트워크 파티션, 오류/손상 메시지, 메시지 지연 등에 대해 탄력적이어야 합니다. 이기적인 노드 혹은 악의를 품은 노드는 합의를 망치거

나 잘못된 상태로 이끌 수도 있습니다. 합의에는 i) 정상적인 노드들은 결과적으로 출력 값을 내놓아야 한다 (라이브니스); 및 ii) 합의에 참여하는 모든 노드는 동일하고 유효한 출력값을 내놓는다 (일관성)는 두 가지 핵심 속성이 있습니다. 합의는 새로운 문제가 아닙니다. 학계는 수십 년 간 이에 대해 광범위하게 연구하였으며 악의적인 노드를 견뎌낼 수 있는 수많은 실용성을 지닌 솔루션을 개발해냈습니다 [17, 18]. 하지만 이러한 솔루션은 폐쇄적이고 허가 받은, 대기시간이 짧은 네트워크에 초점을 맞춘 것입니다.

	전통적 합의	블록체인 합의
예시	pBFT, Paxos	작업증명, 지분증명, 권한증명
트랜잭션 처리량	높음	낮음에서 중간
네트워크 크기	작음	큼
개방성	허가	무허가

표 6.1.: 전통적 합의와 블록체인 중심 합의의 비교

비트코인의 근본적인 혁신은 개방된 무허가형 탈중앙화 네트워크에서 합의를 가능케 했다는 것입니다. 이는 모든 참가자들은 수학적 퍼즐을 풀려 하고 가장 먼저 퍼즐을 푼 참가자는 다음 블록을 추가할 권리를 얻는다는 작업증명이라는 리더 선출 절차에 의해 가능했습니다. 작업증명은 무허가 네트워크의 보안에 대해 매우 강력한 보장을 제공해 주었지만 근본적 재설계가 없이는 낮은 성능에 시달리게 되며 [19] 엄청난 양의 에너지를 소모합니다. 블록체인 산업의 급격한 성장으로 인해 위 문제를 해결하기 위한 수많은 제안들이 제시되었습니다 [20]. 일부 연구는 에너지 소모의 감소에 중점을 두었고 (지분증명 [21]), 일부는 원래의 작업증명보다 나은 성능을 발휘하도록 하는데 중점을 두었습니다 [22]. 허가 네트워크의 전통적인 합의 프로토콜과 비교했을 때 이러한 프로토콜의 성능은 현실의 어플리케이션에 블록체인을 도입하는 데에는 별로 이상적이지 않습니다. 표 6.1.은 전통적 합의와 블록체인 중심의 합의를 비교한 것입니다.

전통적 합의와 블록체인 중심 합의 모두가 현재의 블록체인 환경에 대규모로 적용하기에는 모두 그다지 적절하지 않다는 점을 고려했을 때, 저희는 전통적 합의 프로토콜의 성능을 가지면서도 허가 설정을 요구하지 않는 하이브리드 합의 프로토콜이 장기적으로 저희 플랫폼에 적용될 합의 엔진으로서 고려되어야 한다고 생각합니다. 그림 6.1.은 오리고 합의 프로토콜이 향후 사용하게 될 잠재적 아키텍처를 보여줍니다.

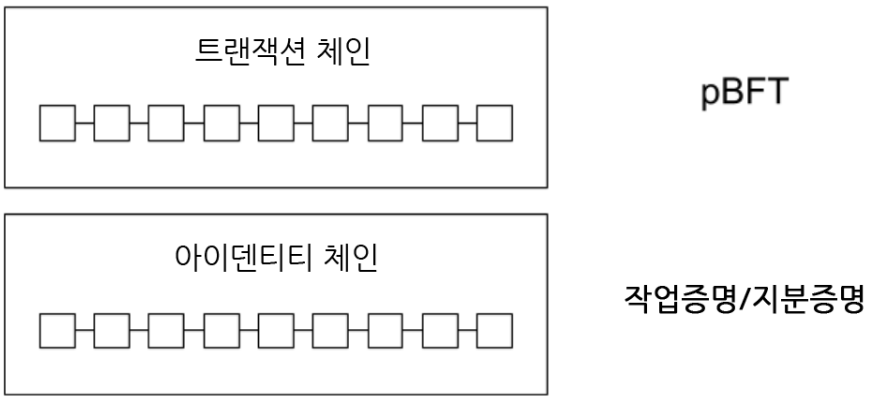


그림 6.1.: 오리고 합의 아키텍처

- pBFT의 노드 인식 요구를 해결하기 위해서는 아이덴티티 체인이 필요합니다. 아이덴티티 체인은 현재 널리 사용되는 작업증명이나 지분증명 등의 블록체인 중심의 합의나, 시빌공격에 탄력적인 다른 모든 합의 방식이라도 사용합니다 [23]. 아이덴티티 체인은 *아이덴티티 블록*으로 구성된 체인으로 각 블록은 트랜잭션 체인 검증자 (validator)가 될 자격을 갖춘 노드들의 목록을 담고 있습니다.

- pBFT는 트랜잭션 체인의 합의 프로토콜로 사용되어야 합니다. pBFT는 비교적 작은 (약 수백 개 정도의 노드) 네트워크에서 최고의 성능을 내기 때문에 주기적인 검증자 선출이 적용되어 고정되었지만 설정으로 변경 가능한 수의 검증자들이 아이덴티티 체인에 기록된 노드 중에서 선출되어 pBFT 합의를 수행합니다.

- BLS 서명 [24] 기반의 무작위 비콘 이 분산된 무작위성의 안전한 소스로서 적용되어야 합니다. 무작위성은 후보자들로부터 검증자를 선출하는 데에 필요하며 네트워크를 샤딩하는 데에도 사용됩니다.

오리고의 하이브리드 합의 프로토콜의 설계와 구현에 대한 더욱 자세한 내용은 향후에 발간될 문서에서 더욱 자세히 다루겠습니다.

6.2. 샤딩

가장 최신의 블록체인 설계에서 각 노드는 모든 온체인 데이터를 담고 모든 트랜잭션을 처리합니다. 이러한 메커니즘이 보안 전반을 강화하기는 하지만 성능을 크게 희생합니다. 이더리움이나 비트코인과 같은 블록체인은 초당 수십 건 미만의 트랜잭션만을 처리할 수 있습니다. 이러한 문제를 해결하기 위해 저희는 연산 샤딩과 상태 샤딩이라는 두 가지 종류의 샤딩 메커니즘이 필요하다는 결론을 내렸습니다.

6.2.1. 연산 샤딩

연산 샤딩은 노드들이 여러 그룹으로 나뉘고 각 그룹이 트랜잭션의 하위 집합을 처리하는 방식입니다. 따라서 네트워크는 그룹의 수가 늘어날수록 선형적으로 확장성을 띄게 된다 하지만 안전한 난수 발생기는 양수인 보안에 필수적입니다. 안전한 난수 발생기 없이는 샤딩 작업은 축소됩니다. 단일 샤드를 공격하는 것이 전체 네트워크를 공격하는 것보다 훨씬 쉽기 때문에 축소된 샤딩 작업은 보안성을 크게 낮춥니다. 6.1.에서 언급한 바와 같이, 사전에 선출된 검증자를 통해 난수를 만들기 위해서는 BLS 서명 [24]이 필요합니다. 샤딩 작업은 *아이덴티티 블록*에 기록되며 클라이언트는 트랜잭션을 그에 맞는 샤드에 보내기 위해 이러한 정보를 사용합니다. 트랜잭션의 송신자 주소를 샤딩의 기준으로 삼는 것은 같은 계정의 모든 트랜잭션이 같은 샤드에서 진행되어 샤드 간 커뮤니케이션의 필요성을 낮출 수 있도록 해줄 것입니다.

6.2.2. 상태 샤딩

확장성을 보다 개선하기 위해서는 상태 샤딩 역시 도입되어야 합니다. 상태 샤딩이란 노드들이 부분적인 블록 데이터를 저장하기 위해 샤딩되는 것을 의미합니다. 연산 샤딩과 비교했을 때, 상태 샤딩은 더 많은 어려움을 안고 있습니다. i) 안전성을 위해서는 더욱 광범위한 작업이 필요하고 ii) 단일 트랜잭션이 다수 샤드에 걸친 정보를 포함하기에 샤드 간 커뮤니케이션이 자주 필요하지만, 이러한 샤드 간 커뮤니케이션은 전체적인 처리량을 저하시킵니다.

6.3. 가상 머신

가상 머신은 스마트컨트랙트의 런타임 환경이며 블록체인이 스마트컨트랙트를 지원하기 위해 필요한 가장 중요한 요소입니다. 미래의 오리고 가상 머신은 새롭게 대두중인 휴대 가능하고 크기와 로드타임이 효율적인 새로운 형식인 웹어셈블리 (WebAssembly, 줄여서 WASM)에 기반할 것입니다. 웹어셈블리는 W3C Community Group에 의해 공개 표준으로서 개발되고 있습니다. 웹어셈블리는 효율적일 뿐만 아니라 성능도 뛰어나지만 컴파일 백엔드로 다수의 프로그래밍 언어를 지원하는 LLVM의 지원을 받고 있습니다. 장기적으로, 미래의 오리고 가상머신은 파이썬이나 자바와 같은 더 많은 개발자 친화적 언어를 지원할 것입니다. 그림 6.2.는 스마트컨트랙트 컴파일과 실행의 과정을 나타내고 있습니다.

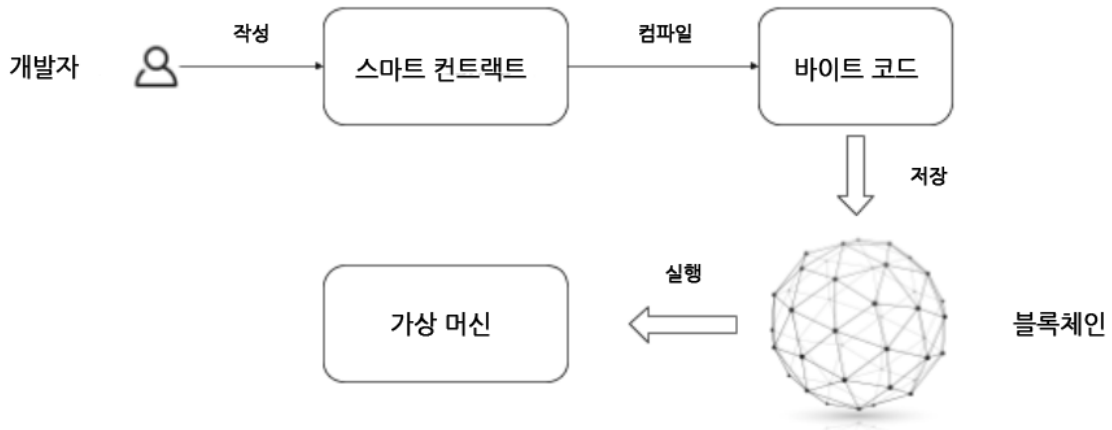


그림 6.2.: 이더리움의 스마트컨트랙트 컴파일 및 실행 프로세스

프라이버시 보호 스마트컨트랙트의 실행의 증명 및 검증에 있어 영지식증명에 의존하는 오리고의 프라이버시 보호 스마트컨트랙트는 영지식증명 시스템과 통합된 컴파일러와 가상 머신이 필요합니다. 프라이버시 보호 스마트컨트랙트는 영지식증명 시스템에서 증명 가능한 프로그램으로서 연산회로 내에 컴파일 되어야 합니다. 가상 머신은 증명을 생성하고 검증하기 위해 회로를 실행시킬 수 있어야 합니다. 오리고는 공개 스마트컨트랙트와 프라이버시 보호 스마트컨트랙트를 모두 지원하기 때문에 오리고의 가상 머신 인스턴스 역시 공개 스마트컨트랙트와 프라이버시 보호 스마트컨트랙트 모두를 실행할 수 있도록 설계되었습니다. 따라서 단순히 스마트컨트랙트를 컴파일하고 실행하는 일반적인 파이프라인은 저희의 요구사항에 맞지 않습니다. 장기적으로, 그림 6.3.과 같

이 공개 스마트컨트랙트와 프라이버시 보호 스마트컨트랙트 모두와 호환되는 파이프라인이 필요합니다.

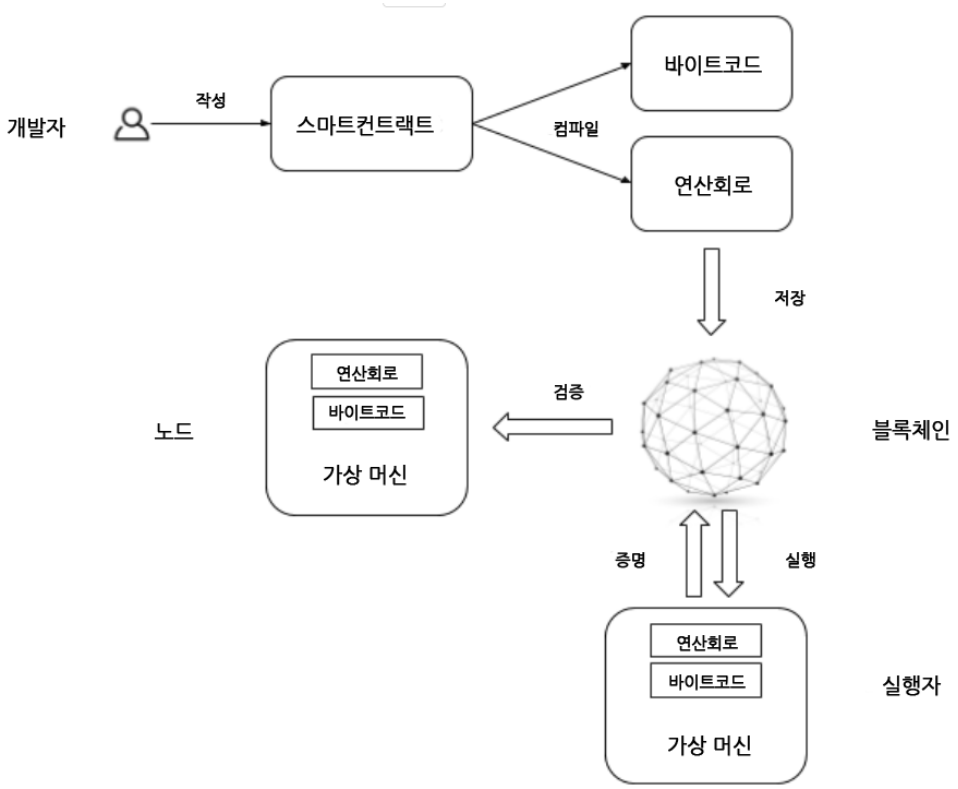


그림 6.3.: 오리고의 스마트컨트랙트 컴파일 및 실행 프로세스

현재 오리고의 가상 머신은 연산회로를 통한 영지식증명의 증명 및 검증을 지원하기 위해 확장연산자와 호환되는 EVM입니다. 또한, 오리고의 프라이버시 보호 스마트컨트랙트 언어는 보다 나은 성능을 달성하기 위해 특정 작업으로 엄격하게 제한된 솔리디티입니다. 오리고의 공개 스마트컨트랙트는 완전한 솔리디티임에 유의하십시오. 이더리움에서 오리고로 스마트컨트랙트를 이전하는데 최소한의 노력만 들이고자, 저희는 솔리디티를 오리고 DSL로 사용하고자 합니다.

제 7 장

어플리케이션

7.1. 오리고가 가능케 한 어플리케이션들

오리고의 프라이버시 보호 프로토콜은 프라이버시가 필요한 탈중앙화 어플리케이션의 광범위한 도입을 가능케 했습니다. 섹션 2,1,에서 언급한 바와 같이, 저희는 그러한 어플리케이션을 두 분류로 나눕니다.

7.1.1. 대중에 대한 프라이버시

이 분류에서 참가자들은 입력값과 출력값을 대중에게 공개하지 않기를 원하지만 참가자들 간에 정보를 나누는 것은 허용합니다. 아래는 이러한 어플리케이션의 분야별 예시입니다.

금융:

- 개인 거래
- 신용등급
- 온라인 여신

- 보험
- 옵션 및 선물

기업:

- 급여/보너스 계약
- 스톡옵션
- 공급사슬 계약
- 기업 컴플라이언스

보건:

- 맞춤형 의료
- 진단
- 의료 기록

기타:

- 사물인터넷

급여대상자명단 등 이러한 분류에 속한 어플리케이션에 대해 당해 고용주와 고용인은 대중으로부터만 급여를 비공개하고 싶어합니다. 이러한 경우 고용인 혹은 고용주는 컨트랙트를 로컬로 처리하고 영지식증명을 블록체인으로 제출합니다. 따라서 오리고 프로토콜은 이러한 어플리케이션의 효율성을 개선하는데 최적화되어 있습니다.

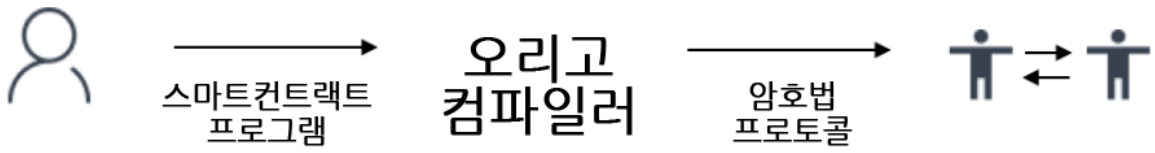
7.1.2. 참여 당사자에 대한 프라이버시

이 분류에서 각 참가자들은 입력값과 출력값을 아무에게도 공개하지 않기를 원합니다. 따라서 프라이버시 요구사항을 충족시키기 위해 오리고 프로토콜 전체가 적용됩니다. 아래는 이러한 어플리케이션의 분야별 예시입니다.

- 모금 (예를 들어, 토큰 모금)
- 경매
- 투표

7.2. 프라이버시 보호 어플리케이션 플랫폼 (PPAP)

오리고 프라이버시 보호 어플리케이션 플랫폼은 영지식증명과 같은 암호법의 기초요소들을 사용해 자동적으로 암호법 프로토콜을 생성하는 컴파일러를 제공함으로써 개발자들이 프라이버시 보호 어플리케이션을 암호법에 대한 지식 없이도 구축할 수 있도록 해줍니다.



7.3. 예시

아래는 오리고 어플리케이션 플랫폼을 사용하는 급여명단의 의사코드입니다.

```
# Employer offchain
def commit(rate, coin):
  cm = commitment(rate, coin.value)
  proof = ZKP.prove(coin is valid)
  # interact with blockchain
  BlockChain._commit(proof, coin, cm)

def execute(rate, coin):
  encrypted_input = encrypt(executor.epk, [rate, coin.value])
  proof = ZKP.prove(encrypted_input correctly encrypted)
  # interact with blockchain
  BlockChain._execute(proof, encrypted_input)

#BlockChain
def _commit(proof, coin, cm):
  ZKP.verify(proof, coin is valid)
  check(not_spend(coin))
  freeze_coin_to_contract(coin)

def _execute(proof, encrypted_input):
  ZKP.verify(proof, encrypted_input correctly encrypted)
  #send encrypted_input to executor.
  call Executor.execute(encrypted_input)

def _settle(output, [coin_employee, coin_employer], proofs):
  ZKP.verify(proofs, contract is correctly executed and [coin_employee,
    coin_employer] are valid)
  _send(coin_employee, employee)
  freeze_coin_to_contract(coin_employer) # for later use

# Executor offchain
def execute(encrypted_input):
  rate, coin_value = decrypt(encrypted_input)
  salary = rate * hour
  balance = coin_value - salary
  output = encrypt({balance}, employer.enc_key)
  if balance > 0:
    coin_employee = coin(salary)
    coin_employer = coin(balance)
  else:
    handle_error("not enough balance")
    coin_employee = coin(coin_value)
    coin_employer = coin(0)

  proofs = [ZKP.prove(contract is correctly executed), ZKP.prove([
    coin_employee, coin_employer] are valid)]
  # interact with blockchain
  BlockChain._settle(output, [coin_employee, coin_employer], proofs)
```

리스팅 7.1..: 급여명단을 실행하기 위한 오리고 스마트컨트랙트의 의사코드

고용주의 오프체인 부분은 자동 생성되었으면 코드의 블록체인 부분은 오리고가 구축한 것입니다. 개발자들은 실행자 부분의 로직만 구현하면 됩니다. 이는 이더리움의 스마트컨트랙트 작성과 매우 유사합니다.

제 8 장

보안

8.1. 공정성 보장

스마트컨트랙트 실행의 공정성을 보장하기 위해 입력과 실행이 두 단계로 나뉘어 있습니다. 모든 컨트랙트의 참여자들은 실행 이전에 (돈을 포함한) 자신의 암호화된 입력값을 준비하고 커밋 해야 합니다. 이러한 모든 커밋은 암호화 되어 있기 때문에 참여자들이 다른 당사자들에게 자신의 커밋을 공개하지 않기를 원한다면 모든 입력값은 서로에게 감춰집니다. 커밋 단계가 끝나면 당사자 중 누구도 입력값을 변경할 수 없습니다. 커밋 단계가 끝나면 당사자들은 자신들의 입력값을 실행자에게 공개해 실행자가 스마트컨트랙트를 처리할 수 있도록 합니다. 커밋 이후에는 모든 입력값이 변경 불가능하여 당사자가 더 이상 입력값을 변경할 수 없기 때문에 이 단계에서는 임의의 당사자조차도 타인의 입력값을 알 수 있습니다. 이러한 설계를 통해 당사자 중 누구도 실행의 결과에 영향을 끼칠 수 없습니다.

8.2. 실행 완전성 - 당사자

프로토콜의 설계가 모든 참가자가 실행 결과를 변경하지 못하게 함으로써 참가자 간의 공정성을 보장하기 때문에 임의의 당사자가 타인의 입력값을 알고 결과를 예측할 수 있을 때 해당 당사자가 할 수 있는 유일한 개입은 손실을 방지하기 위해 컨트랙트를 중지하는 것입니다 (예를 들어, 도박 등). 이러한 사태를 방지하기 위해 예치금 메커니즘이

적용됩니다. 이탈을 막을 필요가 있는 컨트랙트 (예를 들어, 도박 등)에 대해 오리고는 컨트랙트 설계자에게 모든 당사자가 참가 이전에 예치금을 거치하게 하는 예치금 프레임워크를 제공합니다. 따라서, 만약 어떠한 당사자든 컨트랙트를 중단하게 된다면 해당 당사자의 예치금은 다른 참가자들이 나누어 가지게 됩니다. 이러한 방식을 통해 당사자들은 컨트랙트를 중단할 동기를 잃게 됩니다.

8.3. 실행 완전성 – 실행자

당사자의 경우와는 다르게 실행자의 경우에는 예치금만으로는 중단을 막기에 충분치 않습니다. 기본적으로 실행자는 컨트랙트를 실행하기 위해 예치금을 거치합니다. 실행자가 컨트랙트를 실행하지 않으면 예치금은 모든 당사자들에게 분배됩니다. 높은 효용성 요건을 가진 컨트랙트를 위해 백업 실행자 메커니즘이 설계되었습니다. 다른 실행자/그룹이 같은 컨트랙트를 실행하고 검증자가 됩니다. 일반적으로 이는 메인 실행자의 결과에 대해 검증만 실행하지만 실행자가 컨트랙트를 중단하게 된다면 해당 검증자가 백업 실행자가 됩니다.

제 9 장

암호경제학 설계

9.1. 설계 원칙

토렌트 플랫폼과 같은 과거의 탈중앙화 시스템은 사용자들이 다른 사용자가 파일을 다운로드할 수 있도록 네트워크에 파일의 시드를 유지하는 등의 규칙에 따르게 할 경제적 유인의 부족으로 인해 실패하였습니다. 비트코인은 적절한 암호경제학 메커니즘을 구축함으로써 사용자들이 규칙을 따르게 할 뿐만 아니라 비잔틴 장군의 문제를 극복하여 완벽한 합의 시스템을 만들어내 이러한 탈중앙화 시스템을 한층 더 발전시켰습니다.

오리고 플랫폼에서 규칙 (본 장의 뒤를 참조하십시오)은 주로 프라이버시에 집중함으로써 오리고의 각 역할이 정보 누출이나 프라이버시 보호 컨트랙트 실행의 중단 등의 스마트컨트랙트 프라이버시에 관련된 의도하거나 의도치 않은 행위를 실행하지 않도록 합니다. 작업증명이나 지분증명 등의 합의 알고리즘에서 처벌 (음성 인센티브) 메커니즘의 부족으로 인해 “이중지불”이나 “지분없음” 등의 문제가 발생하는 등, 오리고의 규칙에 기반한 합의에 이르도록 하기 위해 인센티브 메커니즘만으로는 부족합니다. 따라서, 오리고는 BFT 합의 프로토콜과 지분 기반 블록체인 합의를 결합한 하이브리드 합의 알고리즘을 적용합니다.

9.2. 인센티브 및 역할

먼저, 오리고 합의 프로토콜은 표 9.1.에 묘사된 두 가지 인센티브 조합으로 구성되어 있습니다.

인센티브 조합 #1 – 기본 조합	
오리고 토큰	오리고 토큰은 이더리움의 ETH와 마찬가지로 “gas fee”의 기능을 합니다. 적극적으로 참여하고 블록체인에 기여하는 역할은 자신의 노력에 대해 암호화폐를 배당 받음으로써 보상받습니다.
특권	역할들은 오리고 토큰을 오리고 생태계 내에서 다양한 목적으로 사용할 수 있습니다.
인센티브 조합 #2 – 고급 조합	
예치금	실행자 역할에 입찰하는 등 특정 작업에는 오리고 토큰이 예치금으로 요구됩니다.
지불	참가자들은 트랜잭션 수수료 등 특정 활동에 참여하기 위해 일정 금액의 오리고 토큰을 지불합니다.
보상	오리고 내의 우수한 참여자들은 그 행동에 토큰으로 보상을 받습니다.
처벌	악성 참가자들은 규칙에 어긋나는 행위를 한 대가로 예치금의 일부 혹은 전체를 잃거나 특정 권리를 박탈당합니다.

표 9.1.: 인센티브 조합

오리고는 향후의 논의를 위해 인센티브에 대한 단어들에 대해 이러한 정의를 내립니다.

- **토큰 보상**: n번째 당사자의 $R_1, \ldots, R_n$

- **지불**: n번째 당사자의 $P_1, \ldots, P_n$
- **예치금**: n번째 당사자의 $D_1, \ldots, D_n$
- **처벌**: n번째 당사자의 $Pun_1, \ldots, Pun_n$

추가적으로, 오리고는 플랫폼 내의 네 가지 역할에 대해 아래와 같이 정의합니다.

- **검증자**: $V_i \in V$, 플랫폼이 증명 검증 및 블록 검증 등 다양한 작업을 수행할 수 있도록 연산력을 제공하는 역할입니다. V_i는 블록을 채굴하거나 특정 작업을 연산한 후에 R_{Vi}를 받습니다
- **사용자**: $U_i \in U$, 플랫폼 상의 컨트랙트 및 DApp을 사용하는 역할입니다. Ui는 스마트컨트랙트와 DApp을 통해 서비스 및 상품에 대해 예치금 D_{Ui}를 거치하고 지불 P_{Ui}를 지급합니다. U_i는 개발자가 해당 메커니즘을 구현해두었을 경우 컨트랙트 및 DApp을 통해 보상 R_{Ui}를 얻을 수도 있습니다.
- **컨트랙트/DAPP 개발자**: $Dev_i \in Dev$, 프라이버시 보호 스마트컨트랙트와 DApp을 만드는 역할입니다. Dev_i는 연산 자원을 사용하고 지불 P_{Devi}를 지급하거나 스마트컨트랙트 및 DApp을 만들고 보상 R_{Devi}을 받습니다.
- **실행자**: $E_i \in E$, 영지식증명에서 프라이버시 관련 작업을 수행하는 역할입니다. E_i는 규칙위반행위를 막기 위한 목적으로 오리고에 의해 예치금 D_{ei}를 거치하도록 강제되며, 만약 이를 이행하지 않을 경우 처벌 Pun_{Ei}를 받게 됩니다. E_i는 또한 프라이버시 관련 작업을 완료한 후 보상 R_{Ei}를 받을 수도 있습니다.

아래는 각 역할에 대해 인센티브 조합을 생성하기 위한 필수적인 프로토콜입니다.

1. 오리고 플랫폼 상의 어떠한 활동 i에 대하여,
   항상 $D_{Ui}, P_{Ui}, P_{Devi}, D_{Ei}, R_{Mi}, R_{Ui}, R_{Devi}, Pun_{Ei}, R_{Ei} \geqq 0$일 경우,

$$D_{Ui} + P_{Ui} + P_{Devi} + D_{Ei} \geqq R_{Mi} + R_{Ui} + R_{Devi} + Pun_{Ei} + R_{Ei}$$

가 항상 적용됩니다.

2. 오리고가 플랫폼에서 D_{Ui}, P_{Ui}, P_{Devi}, D_{Ei}, R_{Vi}, R_{Ui}, R_{Devi}, Pun_{Ei}, R_{Ei}의 정확한 금액을 수요와 공급의 법칙이 결정하도록 둘 경우,

$$\sum D_{Ui} + P_{Ui} + P_{Devi} + D_{Ei} \geqq \sum R_{Vi} + R_{Ui} + R_{Devi} + Pun_{Ei} + R_{Ei}$$

가 항상 유지되어 플랫폼의 지속가능성이 유지됩니다.

제 10 장

로드맵

- **2018년 12월**: *Originis*: 비밀 트랜잭션을 갖춘 테스트넷 공개
- **2019년 9월**: *Medietas*: 메인넷 공개
- **2019년 12월**: *Adscensus*: 자체 프라이버시 보호 스마트 계약가능
- **2020년 6월**: *Infinitas*: 개발자들이 자체적으로 프라이버시 보호, 보안성 확보 및 증명 가능한 스마트 계약 생성 가능

제 11 장

커뮤니티

11.1. 주요 기여자

프랭크 팽(Frank Fang)
미 카네기 멜론 대학교에서 컴퓨터 공학 석사 및 칭화대학교 컴퓨터 공학 학사를 취득하였으며, 전 Pinterest 본사 선임 아키텍트 및 Pinterest 사의 전반적인 아키텍트를 담당함. 분배체계, 암호화 알고리즘 및 신뢰 컴퓨팅 분야에서 폭넓은 경력을 자랑함.

이지아 장(Yijia Zhang)
미 카네기 멜론 대학교 컴퓨터 공학 석사 및 칭화대학교 컴퓨터 공학 학사 취득. 전 구글어시스턴트 창립 멤버 및 기술 선임자. 과거 구글애드, 서치, 안드로이드 오토, 지메일 등 여러 사업분야에 관여.

배론 공(Baron Gong)
미 콜럼비아 대학교 경영과학 및 공학 석사 취득. ICM Outstanding Winner 수상., 7억 위안 + 펀드 관리 경험.

웨이란리우 박사 (Dr. Weiran Liu)
북경항공항천대학 암호학 박사. 중국 Zhihu사에서 암호학 핵심 구성원으로 유명 (Zhihu 사는 중국내 가장 규모가 큰 문답식(question and answer) 웹사이트로써, 사용자 커뮤니티에서 직접 질문 및 답변을 생성, 수정 및 조직할 수 있도록 함) 암호학계에서 15,000 명 이상의 팔로워들을 보유하고 있음.

홍차이(Hong Chai)
중국 내 동영상 플랫폼인 Youku 초기 100명 직원 중 한 명으로, PPS뿐 아니라 나스닥(NASDAQ)에 상장된 Sohu(SOHU: NASDAQ)및 다른 인터넷 회사 마케팅 부서 책임으로 근무 함. CNR Media 및 Charm Media Group의 부회장으로 디지털 마케팅 분야를 담당. 15년 이상의 마케팅 경력.

소니아 왕(Sonia Wang)
15년 이상 금융, 미디어, 보험 및 인터넷 분야에서의 경력을 쌓음. 중국 내 가장 큰 주간지인 The Economic Observer, 다국적 대기업인 CK Hutchinson Holdings 예하의 TOM Group Limited(2383 HKG) 및 HNA Group에서 근무함. AVIVACHina에서 브랜딩 및 커뮤니케이션 부서를 관리하였으며, 중국 내 순위권 온라인 커뮤니티인 Babytree 커뮤니티에서 일일사용자 약 6백만 명을 관리함.

11.2. 기술 기여자

지카이 웬(Zikai Wen)
Hawk 저자이며, 미 코넬대학교에서 박사학위 취득. 분산화된 프라이버시 보호 스마트 계약에 대한 최초 논문 작성

신 우 (Xin Wu)
미 카네기 멜론 대학교에서 컴퓨터공학 석사 및 칭화대학교 컴퓨터공학 학사를 취득하였으며, Google 시니어 소프트웨어 엔지니어 및 Anti-fraud팀 기술선임역임. Google Search, Youtube behavior analysis 경험. 블록체인에 폭넓은 경험을 가진 베테랑으로, 독자적으로 arbitrage system 개발함; 빅데이터 프로세싱 및 데이터보안, 프라이버시, 사용자행동분석, 및 anti-fraud에 폭넓은 경력 및 경험을 자랑.

개빈 왕(Gavin Wang)
미 카네기 멜론 대학교에서 컴퓨터 공학 석사 및 칭화대학교 컴퓨터 공학 학사를 취득하였으며, Google 시니어 소프트웨어 엔지니어. 구글서치, 웹 Answer 및 다른 프로젝트를 진행함; 퀀트트레이딩 체계 자체 개발 경험; 머신 러닝, 인공 지능, 딥 러닝 및 퀀트트레이딩에 폭넓은 경험.

참고 문헌

[1] G. Wood, Ethereum Project Yellow Paper 151, 1 (2014).

[2] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, 2009.

[3] V. Buterin, (2014).

[4] T. Macheel, Banks's Privacy Concerns Shaping Blockchain Vendors' Strategies, https://www.americanbanker.com/news/banks-privacy-concerns-shaping-blockchain-vendors-strategies, 2016, [Online; accessed 15-March-2018].

[5] E. B. Sassonet al., Zerocash: Decentralized anonymous payments from bitcoin, inSecurity and Privacy (SP), 2014 IEEE Symposium on, pp. 459–474, IEEE, 2014.

[6] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, Hawk: The blockchain model of cryptography and privacy-preserving smart contracts, in Security and Privacy (SP), 2016 IEEE Symposium on, pp. 839–858, IEEE, 2016.

[7] B. BÃijnzet al., Bulletproofs: Short proofs for confidential transactions and more, Cryptology ePrint Archive, Report 2017/1066, 2017, https://eprint.iacr.org/2017/1066.

[8] J. Ball, NSA's Prism surveillance program: how it works and what it can do, https://www.theguardian.com/world/2013/jun/08/nsa-prism-server-collection-facebook-google, 2013, [Online; accessed 15-March-2018].

[9] V. Goel, Facebook Tinkers WithUsers'Emotions in News Feed Experiment, Stirring Outcry, http://nyti.ms/2eFHePr, 2014, [Online; accessed 15-March-2018].

[10] N. van Saberhagen, Crypto Note v2.0, howpublished = "https://github.com/monero-project/research-lab/blob/master/whitepaper/whitepaper.pdf", year = 2016, note = "[online; accessed 15-march-2018]".

[11] Intel, Intel Software Guard Extensions, https://software.intel.com/en-us/sgx, 2017, [Online; accessed 15-March-2018].

[12] M. Bellare and P. Rogaway, Random oracles are practical: A paradigm for designing efficient protocols, in CCS ’93, Proceedings of the 1st ACM Conference on Computer and Communications Security, Fairfax, Virginia, USA, November 3-5, 1993., pp. 62–73, 1993.

[13] P. McCorry, S. F. Shahandashti, and F. Hao, A smart contract for boardroom voting with maximum voter privacy, in Financial Cryptography and Data Security - 21st International Conference, FC 2017, Sliema, Malta, April 3-7, 2017, Revised Selected Papers, pp. 357–375, 2017.

[14] M. Campanelli, R. Gennaro, S. Goldfeder, and L. Nizzardo, Zero-knowledge contingent payments revisited: Attacks and payments for services, Cryptology ePrint Archive, Report 2017/566, 2017, https://eprint.iacr.org/2017/566.

[15] E. Ben-Sasson, A. Chiesa, E. Tromer, and M. Virza, Succinct non-interactive zero knowledge for a von neumann architecture, in Proceedings of the 23rd USENIX Conference on Security Symposium, SEC’14, pp. 781–

796, Berkeley, CA, USA, 2014, USENIX Association.

[16] J. Bootle and J. Groth, Efficient batch zero-knowledge arguments for low degree polynomials, Cryptology ePrint Archive, Report 2018/045, 2018, https://eprint.iacr.org/2018/045.

[17] L. Lamport, ACM Transactions on Computer Systems (TOCS) 16, 133 (1998).

[18] M. Castro et al., Practical byzantine fault tolerance, in OSDI Vol. 99, pp. 173–186, 1999.

[19] K. Croman et al., On scaling decentralized blockchains, in International Conference on Financial Cryptography and Data Security, pp. 106–125, Springer, 2016.

[20] S. Bano, M. Al-Bassam, and G. Danezis, USENIX; login: magazine (2017).

[21] S. King and S. Nadal, self-published paper, August 19 (2012).

[22] A. Gervais et al., On the security and performance of proof of work blockchains, inProceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pp. 3–16, ACM, 2016.

[23] Wikipedia, Sybil attack — Wikipedia, the free encyclopedia, http://en.wikipedia.org/w/index.php?title=Sybil%20attack&oldid=833940724, 2018, [Online; accessed 05-May-2018].

[24] D. Boneh, B. Lynn, and H. Shacham, Short signatures from the weil pairing, in International Conference on the Theory and Application of Cryptology and Information Security, pp. 514–532, Springer, 2001.

부록 A.

법적 고지

본 백서 (이하 "백서") 상에 명시된 바와 같이 Origo 플랫폼 내 참여자용 교환수단인 Origo 토큰 (이하 "Origo 토큰")의 판매 (이하 "토큰 판매")는 특정 개인들만을 대상으로 합니다. 본 백서는 투자안내서 또는 공매문서가 아니며, 관할권 내에서 유가증권, 사업신탁 단위, 집합증권투자 단위 또는 기타 다른 형태의 투자 제안이나 투자 권유를 의도하고 있지 않습니다. 규제 당국은 본 백서상 명시된 어떠한 정보도 조사하거나 승인한 바 없습니다. 본 백서는 관할권 내 규제당국에 등록되지 않았습니다. 본 백서에 담긴 정보 전부 또는 (경우에 따라) 일부에 접근성을 가지거나 해당 정보의 소유를 수락함으로써, 귀하는 Origo Foundation (싱가포르 재단등록번호 201808339D) (이하 "프로젝트 회사") 및 Next Innovation Limited (BVI 법인번호 1737837) (이하 "토큰발행인") 측에 다음에 관하여 진술하고 보장합니다:

• (a) 귀하는 중국에 소재하고 있지 않으며, 중국 시민 (세금 또는 기타) 또는 거주자가 아니며, 중국에 살고 있지 않습니다;

• (b) 귀하는 (본 백서상 정의하는) 미국 적격자가 아닌 이상, 미국에 소재하고 있지 않고 미국의 시민권자, 거주자 (세금 또는 기타) 또는 영주권소지자가

아니며 미국에 살고 있지 않습니다;

• (c) 귀하는 어떤 형태 또는 방법으로든 법률이나 규제요건, 규칙 등으로 인하여 토큰판매가 전면 또는 부분적으로 금지, 제한 또는 비 승인된 관할지에 소재하고 있지 않습니다;

• (d) 귀하는 본 고시에 명시된 한계 및 제한사항 구속됨에 동의합니다;

• (e) 귀하는 본 백서가 귀하에게 송달되어 귀하의 Origo 토큰구매 여부에 관한 의사결정을 도와줄 수 있도록 준비되어 있음을 인지하고 있습니다.

주요 고지

현 형태의 본 백서는 투자자들의 피드백을 얻기 위해 현재 구상된 바와 같이 오직 Origo 플랫폼에만 일반 정보 전달용으로 유포되고, 토큰발행인 및/또는 프로젝트 회사의 관리자, 고문 또는 법률 자문인에 의하여 검토 및 변경될 수 있습니다. 이러한 고지사항을 동반하지 않고는 본 백서의 어느 부분도 복제 또는 배포되지 않도록 하십시오. 본 백서의 어느 부분도 백서 수령인과의 법률 관계를 형성하거나, 구속력이 있거나, 토큰발행인 및/또는 프로젝트 회사에 대한 백서 수령인의 강제력을 발생시키지 않습니다. 본 백서의 최신 버전은 적절한 때에 토큰발행인 및/또는 프로젝트 회사가 결정, 공지하는 일자에 발표될 수 있습니다.

본 섹션을 비롯하여 '법적 책임 고지' '진술 및 보장 없음' '귀하의 진술 및 보장' '전향적 진술에 대한 주의 사항' '제3자 정보 및 기타 당사자의 비동의' '사용용어' '조언 없음' '자세한 정보 및 업데이트 의무 없음' '배포 및 유포 제한' '투자 및 등기 제안 금지'와 '위험성 및 불확실성'으로 명명된 다음 섹션을 정독해주십시오.

귀하가 취해야 할 조치에 관해 확신이 없을 경우, 귀하의 법률, 금융, 조세 및 기타 전문영역 담당 자문인과 협의하십시오.

본 Origo 토큰은 어느 사법관할에서든 유가증권 이나 사업신탁 단위, 집합증권투자 단위 또는 기타 다른 형태의 투자를 제안하거나 유도할 의도가 없습니다. 본 백서는 투자안내서 또는 공매문서가 아니며, 관할권 내에서 유가증권, 사업신탁 단위, 집합증권투자 단위 또는 기타 다른 형태의 투자 제안이나 투자 권유를 의도하고 있지 않습니다.

본 백서는 Origo 토큰을 확보, 판매하라는 의견이나 조언, 또는 프로젝트 회사나 토큰발행인의 Origo 토큰확보 제안에 대한 회유를 하고 있지 않으며, 본 백서의 전체 또는 그 일부와 더불어 백서를 제공한 사실이 계약 또는 투자 결정의 근거로 작용하거나 그와 관련하여 신뢰의 대상이 되지 아니합니다. .

Origo 토큰 판매 수익은 현재 진행중인 Origo 플랫폼의 개발 및 성장, 사업 개발, 파트너쉽 및 지역 지원활동 지원에 쓰일 예정입니다.

어느 누구도 계약이나 구속력 있는 법률 약정을 맺을 의무를 가지지 않고, 본 백서에 의거하여 암호화폐 또는 기타 형태의 대금결제는 인정되지 않습니다.

토큰발행인과 토큰판매의 참여자인 귀하 사이에 Origo 토큰 구입과 관련하여 맺는 모든 계약은 해당 계약의 조건 (이하 "토큰판매 조건")을 담은 별도의 문서에 의해서만 규율 됩니다. 토큰판매 조건과 본 백서 사이에 모순된 내용이 있는 경우, 토큰판매 조건이 우선하여 적용됩니다.

(A) 토큰발행인은 귀하에게 제안 또는 판매를 하고 있지 않으며, 귀하는

다음 사항에 해당할 경우 토큰판매 시에 Origo 토큰을 구매할 자격이 없습니다: (A) 귀하가 중국에 소재하거나, 중국 시민 (세금 또는 기타) 또는 거주자이거나, 중국에 살고 있는 경우; (B) 귀하가 미국 적격자가 아닌 이상, 미국에 소재하고 있거나 미국의 시민권자, 거주자 (세금 또는 기타) 혹은 영주권소지자 이거나 미국에 살고 있는 경우; 및 (C) 귀하가 의도한 구매가 이루어지는 때 또는 토큰판매 시기에 Origo 토큰 구매가 이루어지는 때에, 해당 토큰판매가 귀하가 소재한 관할지에서 법률이나 규제사항, 규칙 등에 의해 전면 또는 부분적으로 금지, 제한 또는 비 승인된 경우.

규제 당국은 본 백서에 명시된 어느 정보도 조사하거나 승인한 바 없습니다. 해당 행위는 관할지 내의 법률, 규제사항 또는 규칙에 따라 취해진 적 없고 취해질 계획이 없습니다. 본 백서의 발행, 배포 또는 유포가 준거법, 규제사항 또는 규칙을 준수하고 있다는 의미를 내포하지 않습니다.

프로젝트 회사 및 토큰발행인과 그들의 사업운영, Origo 토큰, 토큰판매, Origo 플랫폼과 관련하여 위험성 및 불확실성이 존재합니다. 본 백서 말미에 명시된 '위험 및 정보공개' 섹션을 참고하십시오.

본 백서의 배포 및 유포가 금지되거나 제한된 국가에는 본 백서 일부 및 부본이 송달되거나 전송될 수 없습니다.

본 백서의 어느 부분도 본 섹션 및 다음에 오게 될 '법적 책임 고지' '진술 및 보장 없음' '귀하의 진술 및 보장' '전향적 진술에 관한 주의사항' '제3자 정보 및 기타 당사자의 비동의' '사용용어' '조언 없음' '자세한 정보 및 업데이트 의무 없음' '배포 및 유포 제한' '투자 및 등기 제안 금지'와 '위험성 및 불확실성' 섹션을 포함하지 않고는 재생산, 배포 또는 유포될 수 없습니다.

법적 책임 부인

귀하가 본 백서 및 그 일부를 수락하거나 본 백서를 신뢰함과 관련하여 불법행위 상, 계약 상 또는 기타로 인해 발생한 간접적, 특수적, 부수적, 결과적 또는 기타 모든 종류의 손실 (수익, 수입, 이윤 손실, 데이터 손실 또는 사용 불가 등을 포함하며 이에 국한되지 않음)에 토큰발행인은 준거법, 규제 및 규칙상 허락된 최대 범위까지 책임을 지지 아니합니다.

진술 및 보장 없음

프로젝트 회사 및 토큰발행인은 본 백서에 담긴 정보의 진실성, 정확성 및 완전성과 관련하여 어느 기업 또는 개인에게도 법적 고지, 진술, 보장 또는 약속을 제공하거나 제공할 목적이 있지 아니합니다

귀하의 진술 및 보장

본 백서 전체 또는 (경우에 따라) 일부에 포함된 정보에 대한 접근 및/또는 소유 승인을 통해, 귀하는 프로젝트 회사 및 토큰발행인에게 다음과 같이 진술하고 보장합니다:

(a) 귀하는 Origo 토큰이 관할권 내에서 유가증권, 사업신탁 단위, 집합증권투자 단위 또는 기타 다른 형태의 투자를 이루고 있지 않음에 동의하고 이를 인정합니다;

(b) 귀하는:

• (i) 중국에 소재하고 있지 않으며, 중국의 시민 또는 거주자 (세금 또는 기타)가 아니고, 중국에 살고 있지 않습니다;

• (ii) (본 백서에서 정의된 바) 미국 적격자가 아닌 이상, 미국에 소재하고 있지

않으며 미국의 시민권자, 거주자 (세금 또는 기타) 또는 영주권소지자가 아니며, 미국에 살고 있지 않습니다; 또는

• (iii) 토큰판매가 어떤 형태 또는 방법으로든, 전부 또는 부분적으로 해당 관할권 내에서 법률, 규제요건 또는 규칙상 금지, 제한 또는 비 승인된 관할권에 소재하고 있지 않습니다;

(c) 귀하가 미국에 소재하거나 그 시민권자, 거주자 (세금 또는 기타) 또는 영주권소지자 또는 상주자인 경우, 귀하는 때에 따라 수정, 개정 또는 보충이 가능한 1933년도 미국 증권법의 규정 D, 통칙 501(a) 상에서 규정하고 있는 공인투자자인 미국 적격자 (개인 또는 법인격 여부를 불문하며 정부당국을 포함하되 이에 국한되지 아니함) 입니다;

(d) 귀하는 본 백서가 투자안내서 또는 공매문서가 아니며, 관할권 내에서 유가증권, 사업신탁 단위, 집합증권투자 단위 또는 기타 다른 형태의 투자 제안이나 투자 권유를 의도하고 있지 않음에 동의하고 이를 인정합니다. 또한 귀하는 계약 또는 구속력 있는 법적 약정을 맺어야 할 의무가 없음과 본 백서에 의거하여 암호화폐 또는 기타 형태의 대금결제가 인정되지 않음에 동의하고 이를 인정합니다;

(e) 귀하는 Origo 토큰이 토큰소지자로 하여금 Origo 토큰과 관련하여 발생하는 이익, 수입, 기타 대금이나 수익, 또는 토큰판매로 인한 수익금 등을 취하거나 수령하도록 하는 매개 또는 그러한 이익, 수입 또는 기타 대금이나 수익에서 지불되는 합계금액을 수령하는 것을 가능하게 하거나 그러한 기회를 부여하는 매개로 해석, 이해, 분류 또는 취급되지 않음을 인정하고 이해합니다;

(f) 귀하는 어떠한 규제당국도 본 백서에 명시된 정보를 조사하거나 승인한 바가

없음을, 관할권 내의 법률, 규제요건 또는 규칙상 어떠한 조치도 취해지거나 취해질 예정이 없음을, 귀하에게 본 백서를 발행, 분배 또는 유포하는 것이 준거법, 규제요건 또는 규칙을 준수한다는 의미를 내포하고 있지 않음에 동의하고 이를 인정합니다;

(g) 귀하는 본 백서와 토큰판매 약속 및/또는 이행, 또는 향후 암호화폐 거래소에서의 Origo 토큰 거래가 프로젝트 회사, 토큰발행인, Origo 토큰, 토큰판매 및 Origo 플랫폼의 장점을 암시하는 것으로 해석, 이해 또는 간주되지 않음에 동의하고 이를 인정합니다;

.

(h) 본 백서 전체/일부 및 부본의 배포 및 유포, 또는 귀하의 백서 취득이 귀하의 관할권 내에서 적용되는 준거법, 규정 또는 규칙에 의하여 금지 또는 제한되지 않고, 소유와 관련하여 제한사항이 적용되는 경우, 귀하는 프로젝트 회사 및/또는 토큰발행인에게 법적 책임을 발생시키지 않고 귀하의 비용으로 해당 제한사항을 준수하고 따랐습니다;

(i) 귀하가 Origo 토큰을 취득하기를 희망하는 경우, 귀하는 Origo 토큰이 다음과 같이 이해, 해석, 분류 또는 취급되지 않음에 동의하고 이를 인정합니다:

- (i) 암호화폐 이외의 모든 통화;
- (ii) 개인 또는 법인이 발행하는 무담보사채, 채권 또는 주식;
- (iii) 해당 무담보사채, 채권 또는 주식과 관련한 권리, 옵션 또는 파생상품;
- (iv) 차액정산계약 또는 그 목적 또는 표면상 목적이 이윤 확보이거나 손실 방지인 기타 계약상의 권리;
- (v) 집합증권투자의 단위;
- (vi) 사업신탁의 단위;
- (vii) 사업신탁 단위의 파생상품; 또는

• (viii) 모든 형태의 투자

(j) 귀하는 토큰 판매와 더불어 Origo 토큰의 보유 및 사용 등 토큰 판매에 참여하는 것과 관련된 모든 행위를 하도록 법적으로 허용되었습니다;

(k) 귀하가 Origo 토큰을 취득하기 위해 사용하는 금액은 자금세탁방지법 등 관할권 내의 법률에 위배되는 행위에 의해 직, 간접적으로 파생된 적 없으며 현재에도 마찬가지입니다;

(l) 귀하가 자연인인 경우, 귀하는 귀하가 거주하는 관할지 및 귀하가 토큰판매에 시민으로서 참여하는 관할지의 준거법상 충분한 연령에 해당하고 충분한 능력을 갖추고 있습니다;

(m) 귀하는 불법적인 목적으로 Origo 토큰을 취득하거나 서용하고 있지 않습니다;

(n) 귀하는 암호화폐, 블록체인 기반 소프트웨어 시스템, 암호화폐 월렛 또는 기타 관련 토큰저장방식, 블록체인 기술 및 스마트 계약 기술의 작동, 기능, 사용, 저장, 전송 매커니즘과 그 외 주요한 특징에 관하여 기초적인 이해를 하고 있습니다;

(o) 귀하는, 귀하가 Origo 토큰 구매를 희망하는 경우에 프로젝트 회사와 토큰발행인, 그들의 사업운영, Origo 토큰, 토큰판매, 토큰 플랫폼과 관련한 위험성이 있음을 전적으로 인식하고 이해하고 있습니다;

(p) 귀하는 Origo 토큰 구매와 관련한 세금부과 건에 대해 결정할 단독 책임을 가지고, 그로 인해 발생하거나 그와 관련된 모든 조세채무에 대해 프로젝트 회사,

토큰발행인 및/또는 토큰판매 관련자가 책임지지 않도록 함에 동의합니다;

(q) 귀하는 본 백서 또는 그 일부를 수락하거나 그에 신뢰함으로써 불법행위 상, 계약 상 또는 기타 이유로 발생하는 모든 직접적, 간접적, 특수적, 부수적, 인과적 또는 기타의 모든 성격의 손실 (수입, 소득 또는 수익, 사용불가 또는 데이터 손상 등을 포함하되 이에 국한되지 않음) 에 대해 프로젝트 회사 및 토큰발행인이 책임지지 않음에 동의하고 이를 인정합니다;

(r) 귀하는 프로젝트 회사, 토큰발행인 및/또는 토큰판매나 Origo 토큰의 생성과 분배와 관련 있는 자를 상대로 하는 집단 소송 또는 집단 중재에 참여할 권리를 포기합니다; 그리고

(s) 위 진술 및 보장사항 모두는 본 백서 또는 (상황에 따라) 본 백서 일부분에 대한 귀하의 접근 및/또는 소지 수락 시점부터 진실하고 완전하며 정확하고 오해의 소지가 없습니다.

전향적 진술에 관한 주의사항

본 백서상 포함된 진술 중 보도자료나 대중의 접근이 가능한 곳에 발표되고, 프로젝트 회사나 프로젝트 회사 및/또는 (상황에 따라) 토큰발행인을 대리하는 이사진, 간부진 또는 직원에 의해 만들어질 수 있는 진술이며, 역사적 사실이 아닌 진술은 모두 "전향적 진술"이 됩니다. 이러한 진술 일부는 "~목적으로 하다", "목표하다", "기대하다", "생각하다", "~수 있다", "추정하다", "예상하다", "만약", "의도하다", "~일 수도다", "계획하다", "가능성이 있다", "~할 개연성이 있다", "계획하다", "해야 한다", "~것이다" 또는 기타 유사 단어 등의 전향적 용어로 감별할 수 있습니다. 그러나 이러한 용어들이 전향적 전술을 확인하는 유일한 수단은 아닙니다. 프로젝트 회사 및/또는 토큰발행인의

사업전략, 계획과 전망 및 프로젝트 회사 및/또는 토큰발행인이 활동하는 산업의 미래 전망과 관련한 모든 진술은 전향적 진술입니다. 프로젝트 회사 및/또는 토큰발행인과 관련하여 본 백서에서 논의된 이러한 전향적 진술은 프로젝트 회사/및 토큰발행인의 전망, 미래 계획, 기타 산업 예측 동향 및 기타 사항들을 포함하되 이게 국한되지 아니하며 역사적 사실이 아니라 예측에 불과합니다.

이러한 전향적 진술은 알려지거나 알려지지 않은 위험성, 불확실성 및 기타 요인과 더불어, 프로젝트 회사 및/또는 토큰발행인의 실제 미래의 결과, 성과 또는 성취가, 전향적 진술에 의해 예상되고 명시적 또는 암시적으로 표현된 미래의 결과, 성과 또는 성취와 실질적으로 차이가 있도록 하는 요인들을 포함합니다. 해당 요인들에는 다음이 포함됩니다:

• (a) 정치, 사회, 경제 및 주식/암호화폐 시장의 상황 및 프로젝트 회사 및/또는 토큰발행인이 사업운영을 수행하고 있는 국가의 규제환경 변동;

• (b) 프로젝트 회사가 사업전략 및 미래계획을 수행 또는 시행할 수 없게 되는 위험성;

• (c) 이자율과 신용화폐 및 암호화폐의 환율변동;

• (d) 프로젝트 회사 및 Origo 플랫폼의 기대성장 전략 및 내부성장 예측의 변동;

• (e) 사업운용과 관련한 효용성 및 이와 관련하여 프로젝트 회사에 지불하는 요금 또는 Origo 플랫폼 상의 변동;

• (f) 사업운용을 위해 프로젝트 회사 및/또는 토큰발행인이 고용한 직원의 효용성 및 임금 상의 변동;

• (g) Origo 플랫폼 사용자의 선호도 변화;

• (h) 프로젝트 회사가 사업을 영위하고 있는 경쟁 환경 및 프로젝트 회사가 해당 환경에서 가지는 경쟁력의 변화;

• (i) 프로젝트 회사의 추후 자금 수요와 해당 자금 수요에 대한 조달 가능성 및 자금 상의 변동;

• (j) 전쟁 또는 국내외 테러 활동;
• (k) 프로젝트 회사 및/또는 토큰발행인의 사업 및/또는 영업활동에 영향을 미치는 재난, 자연 재해 및 불가항력 상황의 발생;
• (l) 프로젝트 회사 및/또는 토큰발행인의 통제력을 벗어난 기타 요인들; 및
• (m) 프로젝트 회사 및 토큰발행인, 그들의 사업운영, Origo 토큰, 토큰판매 및 Origo 플랫폼과 관련한 모든 위험성 및 불확실성.

프로젝트 회사, 토큰발행인 및/또는 그들을 대리하는 관계자에 의하거나 그들에서 기인하는 모든 전향적 진술은 그러한 요인들에 의해 명시적으로 자격을 갖춥니다. 위험성 및 불확실성으로 인하여 프로젝트 회사 및/또는 토큰발행인의 실제 미래결과, 성과 또는 성취가 본 백서상의 전향적 진술에 예측, 명시 또는 내포된 것과 실질적으로 차이가 나게 되는 경우를 고려할 때, 그러한 진술에 과도하게 신뢰를 하여서는 안 됩니다.

프로젝트 회사, 토큰발행인 또는 기타 모든 관계인 누구도 프로젝트 회사 및/또는 토큰발행인의 실제 미래결과, 성과 또는 성취가 전향적 진술상에서 논의될 것이라고 진술, 보장 또는 약속하지 않습니다. 프로젝트 회사 및/또는 토큰발행인의 실제 결과, 성과 또는 성취는 전향적 진술에 예측된 것과 실질적으로 차이가 날 수 있습니다.

본 백서에 포함된 내용은 어느 것도 프로젝트 회사 및/또는 토큰발행인의 미래 성과 또는 정책에 관한 약속, 진술 또는 계약으로 신뢰될 수 없습니다.

또한 새로운 정보 이용이 가능해지거나 다른 사건이 장래에 발생하더라고, 프로젝트 회사 및 토큰발행인은 장래의 국면, 사건 또는 환경을 반영하도록 전향적 진술을 업데이트하거나 그러한 전향적 진술의 개정사항을 공개적으로

발표하여야 할 책임이 없습니다.

제3자 정보 및 타인의 비동의

본 백서는 여러 제3자 정보원 (이하 "제3자 정보")으로부터 얻은 정보를 포함하고 있습니다. 제3자정보의 생산자 누구도 본 백서에 제3자정보를 포함하는 것에 동의하지 않았고, 따라서 제3자정보에 책임이 있지 아니합니다. 제3자정보를 적절한 형식과 내용으로 포함시키기 위한 합리적인 조치가 취해졌지만, 프로젝트 회사와 토큰발행인, 그들을 대리하는 이사진, 임원진 및 직원은 독립적으로 해당 제3자정보 내용의 정확성, 신뢰성, 완전성을 확인하거나 해당 제3자정보의 근본적인 전제사항을 규명하지 않았습니다. 결과적으로, 프로젝트 회사 및 토큰발행인, 그들을 대리하는 이사진, 임원진 및 직원은 누구도 그러한 정보의 정확성, 신뢰성 또는 완전성에 대해 어떠한 진술도 하지 않으며 상기 사항을 업데이트하여 제공할 의무가 없습니다.

사용용어

토큰발행인의 판매대상인 Origo 토큰과 더불어 프로젝트 회사 및 토큰발행인의 사업운영에 대한 원활한 이해를 위해, 본 백서에는 기술적 용어 및 축약을 비롯해 특정 사례에서는 그에 대한 설명이 담겨있습니다. 이러한 설명과 의미부여는 최종적인 의미로 이해돼선 안 되며, 해당 산업에서 쓰이는 표준적인 의미 또는 용례와 일치하지 않을 수 있습니다. 단수형을 쓰는 단어들은 해당하는 경우 복수형을 포함하며, 그 반대의 경우도 마찬가지입니다. 또한, 남성형 단어 역시 해당하는 경우 여성형 또는 중성적 단어를 포함하며, 그 반대의 경우도 마찬가지입니다. 개인들(persons)은 법인을 포함합니다.

조언 없음

본 백서상의 어떠한 정보도 프로젝트 회사, 토큰발행인, Origo 토큰,

토큰판매 또는 Origo 플랫폼에 관한 사업, 법률, 금융 또는 세무상 조언으로 간주되어선 안 됩니다. 귀하는 프로젝트 회사 및 토큰발행인, 그들의 사업운영, Origo 토큰, 토큰판매 및 Origo 플랫폼에 관하여 법률, 금융, 세무 또는 기타 전문 분야의 자문인과 상의하셔야 합니다. 귀하는 Origo 토큰 구매로 인해 재정적 손실 위험을 무기한 부담해야 될 수도 있음을 인지하여야 합니다.

자세한 정보 및 업데이트 의무 없음

어느 누구도 프로젝트 회사 및 토큰발행인, 그들의 사업운영, Origo 토큰, 토큰판매 또는 Origo 블록체인과 관련하여 본 백서에 담긴 정보 또는 진술을 제공해오거나 제공하도록 승인되지 않았습니다. 정보가 제공된 경우, 귀하는 프로젝트 회사 또는 토큰발행인이 자체적으로 또는 대리하여 그러한 정보에 승인을 했다고 신뢰해서는 안 됩니다. 어느 상황에서든 토큰판매는 영구적인 진술을 구성할 수 없으며, 본 백서 작성일자 이후에 변화가 없었다거나 프로젝트 회사 및/또는 토큰발행인의 상황, 조건 및 예측 또는 본 백서에 담긴 사실진술 및 정보에 주요한 변화가 있는 것으로 상당 수준 예상 가능한 성장이 없었다는 연상이나 암시를 주어서는 안 됩니다.

배포 및 유포 제한

본 백서 또는 그 일부의 배포 및 유포는 관할 법규, 규제요건 및 규칙에 의하여 금지되거나 제한될 수 있습니다. 이러한 제한이 적용되는 경우, 귀하는 귀하의 비용으로, 프로젝트 회사 및 토큰발행인의 책임 발생 없이, 본 백서 또는 (경우에 따라) 그 일부의 소유에 대해 적용되는 제한에 대해 인식하고 있어야 하며 이를 준수하여야 합니다.

본 백서의 부본이 배포 또는 유포되고 이에 대한 접근이 허락된 당사자이거나 본 백서를 기타 방법으로 소유하는 당사자는 본 백서 또는 이에

포함된 정보를 어떠한 목적으로든 타인에게 유포하거나 재생산 혹은 배포해서는 안 되며 해당 행위를 허가하거나 발생하도록 하여서는 안 됩니다.

투자 및 등기 제안 금지

본 백서는 투자안내서 또는 공매문서가 아니며, 관할권 내에서 유가증권, 사업신탁 단위, 집합증권투자 단위 또는 기타 다른 형태의 투자 제안이나 투자 권유를 의도하고 있지 않습니다. 어느 누구도 계약이나 구속력 있는 법률 약정을 맺어야 할 의무를 가지지 않고, 본 백서에 의거하여 암호화폐 또는 기타 형태의 대금결제는 인정되지 않습니다.

규제 당국은 본 백서상 명시된 어떠한 정보도 조사하거나 승인한 바 없습니다. 관할 법률, 규제요건 또는 규칙에 따라 그러한 조치는 취해진 적 없고 취해질 예정이 없습니다. 본 백서가 발행, 배포 또는 유포된다는 것이 관련 준거법, 규제요건 또는 규칙을 준수하였다는 의미를 내포하지 않습니다.

위험성 및 불확실성

Origo 토큰의 장래 구매자는 Origo 토큰 구매 전에 프로젝트 회사 및 토큰발행인, 그들의 사업운영, Origo 토큰, 토큰판매, 토큰 플랫폼, 본 백서상 명시된 모든 정보 및 토큰판매 용어와 관련한 모든 위험요소 및 불확실성을 면밀히 살펴보고 평가해야 합니다. 만약 그러한 위험요소 및 불확실성이 실제 사건으로 전개될 경우, 프로젝트 회사 및/또는 토큰발행인의 사업, 재정상태, 운영 성과 및 예측 등이 현저한 수준으로 불리해질 수 있습니다. 이 경우, 귀하는 Origo 토큰가액 전부 또는 일부를 잃을 수도 있습니다. 본 백서 후반부에 명시된 위험 요소를 참고하시기 바랍니다.

부록 B.

위험 요소

토큰판매 참여와 관련한 위험성

토큰발행인 및 프로젝트 회사와 같은 스타트업에 대한 투자는 상당한 위험성을 내포하고 있습니다.

재정상, 운영상의 위험에 직면하는 스타트업이 많고, 토큰발행인과 프로젝트 회사는 이러한 위험에 면역이 되어있지 않습니다. 그 중에서도 스타트업은 주로 제품개발, 마케팅, 자금조달 및 총괄경영 분야에서 예기치 못한 문제들을 경험하며, 이러한 문제들은 주로 해결하기가 어렵습니다.

토큰발행인 및/또는 프로젝트 회사는 사업을 중단해야 될 상황에 놓일 수도 있습니다.

암호화폐 및 신용화폐 가치의 불리한 변동, 토큰발행인 및/또는 프로젝트 회사의 Origo 플랫폼 또는 Origo 토큰 유틸리티 구축 불가, 상업 관계상의 실패, 또는 지적재산권 분쟁과 같은 여러 많은 원인들로 인해, 토큰발행인 및/또는 프로젝트 회사는 해산할 수 있고 그에 상응하는 조치를 취할 수도 있습니다.

토큰판매조건, 이에 명시된 구매자권리 및 토큰판매에 관한 세금처리는 분명하지 않으며, 장래에 특정 사건이 발생하여 구매자가 부정적인 세제영향을 받을 수 있습니다.

토큰판매조건 및 Origo 토큰에 대한 세제 특징은 불분명하며, 각 구매자들은 Origo 토큰 투자와 관련하여 세금 상담을 받아야 합니다. 토큰판매조건에 따른 투자와 Origo 토큰구매를 함으로써 구매자는 원천징수, 소득세, 세무보고요건 등 세금납부에 관한 불리한 영향을 입을 수 있습니다. 각 구매자는 토큰판매조건에 따라 Origo 토큰에 투자하는 경우, 세금 처리와 관련하여 세무 전문가와 상담하셔야 합니다.

Origo 토큰용 프리마켓은 없으며, 토큰판매가 해당 토큰에 대한 활발하고 유동성 있는 시장 환경을 보장하진 않습니다.

토큰판매 이전에 Origo 토큰을 위한 공개시장은 존재한 바 없습니다. Origo 토큰이 암호화폐 거래소에서 거래되는 경우, Origo 토큰을 위한 활발하고 유동적인 거래시장이 형성될 것이라는 보장이 없고, 만약 그러한 시장이 형성된 경우, Origo 토큰이 해당 암호화폐 거래소에서 거래된 후에 그 시장이 계속해서 유지될 것이라는 보장은 없습니다. 또한 Origo 토큰의 시장가격이 구매자가 Origo 토큰을 취득했던 구매가격 이하로 떨어지지 않을 것이란 보장이 없습니다. 그러한 구매 가격은 Origo 토큰이 암호화폐 거래소에서 거래가 가능해진 이후에 Origo 토큰의 시장가격을 반영하지 못할 수도 있습니다. Origo 토큰은 중앙은행 또는 국가기관, 초국가기관 혹은 준국가기관에서 발행되는 화폐가 아니며, 고정실물자산이나 기타 신용의 지원을 받지도 않습니다. 토큰발행인은 Origo 토큰의 시장 유통 및 거래에 대하여 책임이 없으며 그러한 행위를 추구하지도 않습니다. Origo 토큰 거래는 오로지 관련 시장 참여자들 사이의 가격 합의에 따라 달라지

며, 어느 누구도 Origo 토큰 소지자로부터 Origo 토큰을 구매해야 할 의무가 없고, 어느 누구도 Origo 토큰의 유동성 또는 시장가격에 대해 일절 보장하지 않습니다. 따라서, 토큰발행인은 Origo 토큰에 대한 수요나 시장이 존재한다는 확신을 하거나, Origo 토큰이 암호화폐 거래소에서 거래된 이후에 구매가격이 Origo 토큰의 시장가격을 반영해 준다고 확신할 수 없습니다.

장래의 Origo 토큰 판매는 Origo 토큰의 시장 가격에 중대하고 부정적인 영향을 줄 수 있습니다.

('토큰판매' 시에는 불가능했던) 장래의 Origo 토큰 판매는 시장에서 Origo 토큰의 공급 증가를 야기해 Origo 토큰의 가격하락 압력을 초래할 수 있습니다. '토큰판매' 외에 상당수의 Origo 토큰이 판매 및 분배되거나, 또는 그러한 추후 판매나 발행이 있을 수 있다는 인식이 있을 경우, Origo 토큰의 거래가격에 부정적인 영향을 줄 수 있습니다.

부정적 광고는 Origo 토큰 가격에 중대하고 부정적인 영향을 미칠 수 있습니다.

(a) 토큰발행인 및/또는 프로젝트 회사; (b) Origo 플랫폼; (c) Origo 토큰; 또는 (d) 토큰발행인 및/또는 프로젝트 회사측의 주요 직원이 관련된 부정적 광고는 해당 광고가 정당한지 여부와 관계없이, Origo 토큰에 대한 시장인식이나 시장가격에 중대하고 부정적인 영향을 줄 수 있습니다.

Origo 플랫폼의 성공에 관해 어떠한 보장도 할 수 없습니다.

Origo 토큰의 가격과 수요는 Origo 플랫폼의 성과에 의해 크게

좌우됩니다. 개시 이후에 Origo 플랫폼이 거래를 이어나가 영리적으로 성공할 것이라는 보장은 없습니다.

Origo 플랫폼은 아직 완전히 개발, 확정, 통합되지 않았고 개시 이전에 별도의 변경, 업데이트 및 조정이 있을 수 있습니다. 그러한 변경은 사용자에 대한 사전 홍보에 예기치 못한 영향을 가져다 주어 성공여부에 영향을 미칠 수 있습니다.

토큰발행자가 현실적인 예측을 하는 데 많은 노력을 기울임에도 불구하고, 토큰판매 시 조성된 암호화폐가 Origo 플랫폼의 개발 및 통합에 충분한 수준이 될 것이라는 보장이 없습니다. 상기 언급된 사항 및 기타 다른 이유로 인하여 Origo 플랫폼의 개발과 통합은 완성되지 못할 수도 있고, 개시가 될 것이라는 보장도 할 수 없습니다. 이처럼, 배분된 Origo 토큰은 가치가 거의 없을 수도 있고, 이는 토큰의 거래가격에 타격을 줄 수 있습니다.

Origo 토큰의 거래 가격은 토큰판매에 따라 변동이 있을 수 있습니다.

일반적으로 암호화폐 가격은 상대적으로 불안정한 경향이 있고, 단기간에 상당한 변동이 있을 수 있습니다. Origo 토큰에 대한 수요 및 그에 상응하는 시장 가격은 토큰발행인 및/또는 프로젝트 회사가 통제할 수 없는 요소를 포함하는 다음과 같은 사항들에 대응하여 급속한 속도로 현저히 변동할 수 있습니다:

• (a) 신규 기술 혁신;
• (b) Origo 토큰의 시장가격, 또는 토큰발행인 및/또는 프로젝트 회사의 재무 및 사업 실적에 대한 분석자의 추측, 추천 또는 예측;

• (c) Origo 토큰과 동일한 암호화폐 거래소에서 거래가 가능하도록 만들어지고, 토큰발행인 및/또는 프로젝트 회사의 사업과 비슷한 사업운용을 하는 기업체의 시장가격 및 토큰 가격상 변동;
• (d) 토큰발행인 및/또는 프로젝트 회사의 중대사 발표 (예: 파트너쉽, 스폰서쉽, 신규제품개발);
• (d) 시장 가격 및 거래소에서의 암호화폐 거래량 변동;
• (e) 토큰발행인 및/또는 프로젝트 회사 주요직원의 충원 또는 이직;
• (f) 운영 및 성장 전략 실행에 있어 토큰발행인 및/또는 프로젝트 회사의 경영 성공 또는 실패; 및
• (g) 블록체인이나 금융기술산업, 통상적 경제상황이나 시장 여론, 또는 기타 사건이나 요인.

월렛(WALLET)과 관련된 위험요소

귀하의 월렛(아래에서 정의)과 관련한 정보의 손실이나 손상은 Origo 토큰에 대한 귀하의 접근성 및 소유에 영향을 미칠 수 있습니다.

귀하가 Origo 토큰을 수령하기 위해서는, 암호화폐 월렛 (이하 "월렛")에 대한 접근성을 구축하고 유지하여야 합니다. 월렛 속 Origo 토큰에 대한 귀하의 접근성은 다른 무엇보다도 사용자 계좌정보, 주소, 개인 키(key) 및 패스워드 등 해당 월렛 정보에 대한 안전장치에 따라 달라집니다. 상기 사항이 손실되거나 손상되는 경우, 월렛에 대한 귀하의 접근은 제한될 수 있고, 이로 인해 Origo 토큰이 복구불능 또는 영구적 손상 상태가 되는 등 토큰에 대한 귀하의 접근성 및 소유에 부정적 영향이 있을 수 있습니다.

월렛 또는 월렛서비스제공자가 Origo 토큰과 기술적으로 호환이 되지 않을 수 있습니다.

월렛 또는 월렛서비스제공자가 Origo 토큰과 기술적으로 호환이 되지 않을 수 있으며 이로 인해 Origo 토큰이 전달되지 않거나 Origo 토큰에 대한 귀하의 접근에 영향이 갈 수 있습니다.

토큰발행인 및 프로젝트 회사와 관련한 위험요소

Origo 플랫폼은 토큰발행인 및/또는 프로젝트 회사에 의해 개발, 운영 및 관리되도록 계획되었습니다. 토큰발행인 및/또는 프로젝트 회사에 부정적 영향을 주는 상황이나 환경이 토큰발행인 및/또는 프로젝트 회사의 플랫폼 유지력에 영향을 주는 경우 토큰발행인 및/또는 프로젝트 회사에 상응하는 부작용을 끼칠 수 있습니다. 이에 따라, Origo 토큰의 거래가격이 영향을 받을 수 있습니다.

토큰발행인 및/또는 프로젝트 회사는 사업을 개발하고 전개하는 동안 효율적인 사업운영에 실패할 경우 중대하고 부정적인 영향을 받을 수 있고, 이는 Origo 플랫폼의 유지력에 직접적인 충격을 가하여 결과적으로 Origo 토큰의 거래가격에 영향을 미칠 수 있습니다.

금융기술 및 암호화폐 산업과 토큰발행인 및 프로젝트 회사가 활동중인 시장은 급속하게 성장해왔고 현재도 급속히 성장 중이며, 신기술발전과 변화하는 비즈니스 모델 및 기타 요인들에 대응하여 계속해서 진화하고 있습니다. 이러한 끊임없이 변화하는 환경으로 인하여, 토큰발행인 및/또는 프로젝트 회사는 변화 적응에 운영상의 어려움을 겪을 수 있고, 토큰발행인 및 프로젝트 회사의 지속가능성은 그들의 사업운용 능력, 기술발전과 시장 트렌드에 대한 적응력,

자격 있고 유능한 직원을 고용하여 적절한 트레이닝을 제공하는 확실성을 갖추었는지 여부에 의해 좌우될 것입니다.

사업 발전에 따라 토큰발행인과 프로젝트 회사는 운영 인프라 또한 확장하고 조정해야 합니다. 토큰발행인과 프로젝트 회사 각각의 사업운영은 블록체인 기반 소프트웨어 시스템, 암호화폐 월렛 또는 관련 토큰저장 매커니즘, 블록체인 기술 및 스마트계약 기술에 좌우됩니다. Origo 플랫폼에 대한 기술지원 인프라를 효율적으로 관리하기 위해서는, 토큰발행인과 프로젝트 회사가 데이터 시스템과 기타 운영상 시스템, 절차 및 제어를 지속적으로 업그레이드하고 향상시켜야 합니다. 이러한 업그레이드 및 향상은 전용자원을 필요로 하고 복잡하며, 토큰발행인 및/또는 프로젝트 회사가 통제하지 않는 제3자 호스트 컴퓨터 서비스에 점점 의존하고 있습니다. 만일 토큰발행인 및/또는 프로젝트 회사가 적시에 능률적, 비용 효율적인 방법으로 자신의 시스템과 조직을 변화하는 환경에 맞출 수 없다면, 재정상태 및 운영결과가 악화될 수 있습니다. 토큰발행인 및/또는 프로젝트 회사가 신뢰하는 제3자가 보안침입을 당하거나 토큰발행인 및/또는 프로젝트 회사가 실행하는 서비스에 영향을 주는 지장을 받게 되는 경우, 각 내부정보의 완전성 및 효용성이 손상될 수 있고 결과적으로 기밀 또는 특허정보의 손실 및 경제적 손실을 발생할 수 있습니다. 토큰발행인 및/또는 프로젝트 회사 각각의 사업, 재정 상태 및 운용에 미치는 재정, 인력 등 자원의 손실과 기타 역효과는 토큰발행인과 프로젝트 회사의 Origo 플랫폼 유지력에 직접적인 역효과를 낳습니다. Origo 플랫폼이 Origo 토큰이 결부된 주 상품이기 때문에, 이는 Origo 토큰의 거래가격에 악영향을 줄 수 있습니다.

토큰발행인 및/또는 프로젝트 회사는 자신들의 인프라 네트워크 및/또는 Origo 플랫폼에 악영향을 미칠 수 있는 시스템 장애, 예기치 못한 네트워크 또는 서비스의 중단, 하드웨어 또는 소프트웨어 결함, 보안침해 또는 기타 상황을

경험할 수 있습니다.

토큰발행인과 프로젝트 회사는 해킹, 사이버 공격, 채굴공격 (이중지출공격, 다수 채굴력 공격 및 이기적 채굴 공격 등을 포함하되 이에 국한되지 않음), 디도스 공격 또는 에러, Origo 플랫폼, Origo 토큰, 월렛 또는 이외 토큰발행인 및/또는 프로젝트 회사, Origo 플랫폼, Origo 토큰 및 월렛이 신뢰하는 기술 (스마트계약 기술을 포함하되 이에 국한되지 않음), 또는 이더리움 블록체인이나 기타 다른 블록체인상의 취약성 또는 결함이 언제 발생할 것인지 예상할 수 없습니다. 그러한 현상에는 프로그래밍이나 소스코드 결함으로 인해 착취 및 남용으로 이르게 되는 경우가 포함될 수 있습니다. 토큰발행인 또는 프로젝트 회사는 그러한 해킹, 채굴공격 (이중지출공격, 다수 채굴력 공격 및 이기적 채굴 공격 등을 포함하되 이에 국한되지 않음), 사이버 공격, 디도스 에러, 취약성 또는 결함을 제 때 감지하지 못할 수 있고, 동시다발적 또는 연달아 발생하는 여러 문제들에 효과적으로 대응할 수 있는 자원을 충분히 보유하고 있지 않을 수 있습니다. Origo 플랫폼을 포함하여 토큰발행인 및/또는 프로젝트 회사의 각 네트워크나 서비스는 자연재해, 장비고장, 네트워크 연결중지, 전력손실, 심지어 권한 없는 사용자에 의한 소프트웨어 바이러스나 공격과 같은 각 서비스의 고의적인 중단 등 토큰발행인 및/또는 프로젝트 회사의 통제영역 밖에 있는 여러 사유로 인해 지장 받을 수 있습니다. 토큰발행인과 프로젝트 회사가 Origo 플랫폼 및 각자의 서비스 유지를 위해 핵심적인 제품이나 인프라에 대한 악의적 공격에 대응하여 조치를 취하겠지만, 디도스와 같은 사이버 공격이 추후 발생하지 않을 것이란 보장은 없고, 토큰발행인과 프로젝트 회사가 강화된 보안조치를 취하더라도 효과가 있을 지 여부는 확신할 수 없습니다. 토큰발행인과 프로젝트 회사는 각자의 기술, 재무 데이터 관련 정보 또는 사용자 정보를 훔치거나 토큰발행인과 프로젝트 회사, Origo 플랫폼 사용자에 손해를 끼칠 행위를 하려는 목적으로 인프라에 가해지는 공격에 취약할 수 있습니다.

토큰발행인 및/또는 프로젝트 회사의 의도된 보안조치 또는 기타 중단이 토큰발행인 및/또는 프로젝트 회사 네트워크나 서비스 (Origo 플랫폼 포함)의 사용성, 안정성 및 보안성에 타격을 주는 중대한 위해가 발생할 경우 이는 Origo 토큰의 거래가격에 악영향을 미칠 수 있습니다.

토큰발행인 및 프로젝트 회사는 제3자의 위치 및 데이터센터 시설에 부분적으로 의존하고 있습니다.

토큰발행인 및 프로젝트 회사의 인프라 네트워크는 부분적으로 그들이 각자 제3자 시설 위치에 소유 및 저장하는 서버와 제3차 데이터센터에서 빌린 서버를 통해 구축됩니다. 토큰발행인 및/또는 프로젝트 회사가 상업적으로 합리적인 조건으로 데이터시설 임대를 갱신할 수 없다면, 토큰발행인 및/또는 프로젝트 회사는 각자 서버를 새로운 데이터센터 시설로 옮겨야 될 수 있고, 이러한 이전과 관련하여 상당한 비용이 발생하거나 서비스 중단 현상이 있을 수 있습니다. 또한 이런 시설들은 다른 무엇보다도 자연재해, 방화, 테러공격, 정전 및 통신장애 등으로 인한 피해 또는 중단에 취약합니다. 추가적으로, 그러한 시설들의 제3자 공급자는 제3자 행위, 직원 실수, 불법행위 등의 결과로 보안침해를 입을 수 있고 제3자는 그러한 서버에 있는 데이터에 무단 접근을 할 수 있습니다. 시스템에 무단으로 접근하거나 시스템을 파괴하기 위해 사용되는 기술은 자주 바뀌고 타겟을 대상으로 개시되기 전까지 발견되지 않기 때문에, 토큰발행인, 프로젝트 회사 및 그러한 시설 공급자는 이러한 기술을 예상하거나 적절한 예방 조치를 실행하지 못할 수 있습니다. 토큰발행인 및/또는 프로젝트 회사의 인프라 네트워크 및/또는 Origo 플랫폼에 영향을 주는 모든 보안상 침해 또는 손실의 발생은 Origo 토큰의 거래가격에 악영향을 줄 수 있습니다.

전반적 글로벌 시장 및 경기는 토큰발행인 및/또는 프로젝트 회사의

경영성적, 운용성과 및 현금유동성에 부정적 영향을 줄 수 있습니다.

토큰발행인 및/또는 프로젝트 회사는 전반적인 글로벌 경제 및 시장상황에 의해 영향을 받을 수 있습니다. 세계적으로 경기 상황이 좋지 않을 때 대체적으로 정보기술 산업의 둔화되어왔고 장래에도 그럴 수 있습니다. 경제 약화는 수익감소 및 경영상 현금유동성의 감소 등 토큰발행인 및/또는 프로젝트 회사의 각 사업운영 및 재무 상태에 악영향을 줄 수 있습니다. 또한, 토큰발행인 및/또는 프로젝트 회사는 경기 하락세에 가격 압박의 상승과 Origo 플랫폼의 개시 및 사용 침체라는 부정적 영향을 받을 수 있습니다. 토큰발행인 및/또는 프로젝트 회사가 의탁하는 서버 공급자, 대역폭, 위치 및 기타 서비스 역시 경제 상황에 부정적인 영향을 받을 수 있고, 결과적으로 이는 토큰발행인 및/또는 프로젝트 회사 각각의 운영 또는 부대비용에 부정적인 영향을 줄 수 있습니다. 그러므로, 현재 경제상황이나 경기악화, 또는 장기불황, 불황재발이 토큰발행인 및/또는 프로젝트 회사 각각의 사업, 재정상태 및 운영성과에 지대한 악영향을 미쳐 결과적으로 Origo 토큰의 거래가격에 타격을 주지 않을 것이라는 보장을 할 수 없습니다.

토큰발행인, 프로젝트 회사 및/또는 Origo 토큰은 새로운 규제 실행으로 인한 영향을 받을 수 있습니다.

전세계적으로 암호화폐 거래는 보통 규제를 받지 않으나 여러 관할권에서 수많은 규제당국들이 암호화폐 또는 암호화폐 시장을 통제하는 규제제도를 시행하자는 목소리를 높여왔습니다. 토큰발행인, 프로젝트 회사 및/또는 Origo 토큰은 암호화폐 또는 암호화폐 시장과 관련한 신규 규정에 의해 영향을 받을 수 있고, 여기에는 그러한 규정을 준수하기 위한 행동을 하거나 규제당국의 질의, 통지, 요청 또는 시행조치 등을 처리하는 일들이 포함되며 이는 상당한 비용을

유발할 수 있고, 또한 Origo 토큰 및/또는 Origo 플랫폼의 상당한 변경을 요할 수도 있습니다. 플랫폼이 사용자 대상으로 가지는 장점이 타격을 입을 수 있고 그 사용자 수가 감소할 수 있습니다. 더욱이, 신규로 실행되는 해당 규제 준수를 위한 비용 (금전상 또는 기타)이 특정 기준치를 초과하게 되면, Origo 토큰 및/또는 Origo 플랫폼을 유지하는 것이 상업적으로 불가해질 수 있고, 토큰발행인 및/또는 프로젝트 회사는 Origo 토큰 및/또는 Origo 플랫폼 운용을 중단할 수도 있습니다.

또한, 정부 또는 규제당국이 Origo 토큰 및 플랫폼을 포함하여 분산원장기술 및 어플리케이션에 영향을 주는 법규를 변경할 것인지, 어느 방법으로 변경할 것인지 등을 예측하기가 어렵습니다. 토큰발행인 및/또는 프로젝트 회사는 관할권 내에서 운영이 불법화되거나 관할권 내에서 운영에 대한 규제 승인 취득이 불가하거나 바람직하지 않게 되는 사업을 중단해야 할 수도 있습니다. 이러한 상황에서 Origo 토큰 거래가가 악영향을 받게 되거나 Origo 토큰 거래가 중단될 수 있습니다.

블록체인 기술, 암호화폐, 토큰 및 토큰판매 등의 토큰공개, Origo 플랫폼 및 Origo 토큰에 대한 규제제도는 불확실하고 규정이나 정책은 Origo 플랫폼 개발과 Origo 토큰의 효용성에 중대한 역효과를 줄 수 있습니다.

토큰 (Origo 토큰 등)과 토큰판매와 같은 토큰공개, 암호화폐, 블록체인 기술 및 암호화폐 거래소에 대한 규제는 현재 개발 중에 있고 국제, 연방, 주 관할 차원에서 급속도로 변동할 가능성이 있으며 매우 불확실합니다. 싱가포르 및 타 국가의 여러 입법/행정기관에서는 추후 Origo 플랫폼의 개발 및 성장과 Origo 토큰의 채택 및 효용에 극심하게 영향을 미칠 수 있는 법률, 규정, 지침 및 기타 조치를 채택할 수 있습니다. 토큰발행인, 프로젝트 회사 또는 Origo 플랫폼

사용자가 아직 존재하지 않거나, 해석이 달라지거나 변경 가능성이 있는 법률, 규칙 및 규정을 준수하지 않는 경우, 민사 벌과금을 포함해 여러 불리한 결과를 얻게 될 수 있습니다. 블록체인 네트워크는 또한 유럽연합, 중국, 한국 및 러시아와 같은 여러 외국 사법권에서 불확실한 규제 상황에 직면할 수 있습니다. 여러 외국 사법권은 가까운 장래에 Origo 플랫폼에 영향을 주는 법률, 규정 또는 법령을 채택할 수 있습니다. 그러한 법률, 규정 또는 법령은 토큰발행인 및/또는 프로젝트 회사의 각 사업에 직접적으로 부정적인 영향을 미칠 수 있습니다. 장래 규제의 변경에 따른 영향은 예측이 불가능하지만, 그러한 변경은 Origo 플랫폼의 개발 및 성장과 토큰의 채택 및 효용성에 상당부분 매우 불리하게 작용할 수 있습니다.

신규 또는 개정 법규나 기존 법규의 해석방법이 Origo 토큰 매매 시 통화 가치, 토큰발행인 및/또는 프로젝트 회사에 의한 할당액, Origo 토큰 자금유동성, Origo 토큰이 거래되는 시장 또는 거래소에의 접근성, Origo 토큰의 구조, 권리 및 양도성 등에 중대하고 부정적인 영향을 줄 수 있습니다.

Origo 토큰 소지자는 토큰발행인 또는 프로젝트 회사에 대한 통제권이 없습니다.

Origo 토큰 소지자는 투표권이나 배당권이 없고 어떤 이유로든 토큰발행인 또는 프로젝트 회사 주식자본의 주주로 간주되지 않습니다. 또한 어떠한 것도 구매자에게 토큰발행인 또는 프로젝트 회사의 주주권 또는 이사회 선임 및 주주회의 회부사안에 관해 투표할 권리, 법인행위에 대한 동의를 승낙 또는 보류할 권리 또는 회의통지를 수령할 권리, 신주인수권 또는 기타를 수령할 권리를 양도하는 것으로 해석되지 않습니다. 구매자는 투자에 관한 모니터링을 하는 데 있어 정보가 부족할 수 있고, Origo 토큰 구매자들은 토큰발행인,

프로젝트 회사, Origo 토큰 또는 Origo 플랫폼에 관하여 원하는 수준의 모든 정보를 적시에 얻지 못하거나 아예 얻지 못할 수도 있습니다. 불리한 주요 변화가 있었음을 구매자가 적시에 알지 못할 가능성이 있습니다. 토큰발행인이 Origo 토큰용 오픈소스 개발에 많은 노력을 기울인 한편 해당 정보는 그 특성상 매우 전문적일 수 있습니다. 이러한 어려움과 기타 불확실성에 따른 결과로 구매자는 Origo 플랫폼에 관한 정확하고 명확한 정보를 얻지 못할 수 있습니다.

Origo 토큰으로 인해 발생하는 예기치 못한 위험이 있을 수 있습니다.

Origo 토큰과 같은 암호토큰은 상대적으로 새롭고 역동적인 기술입니다. 본 섹션에 명시된 위험요소 외에도, 토큰발행인 및 프로젝트 회사가 예측할 수 없는 것들을 포함하여 Origo 토큰 구매, 소지 및 사용과 관련한 다른 위험성들이 있습니다. 그러한 위험은 추후에 예상치 못한 변동이나 본 문서에서 논의된 위험요소들이 결합된 양상으로 실현될 수 있습니다.