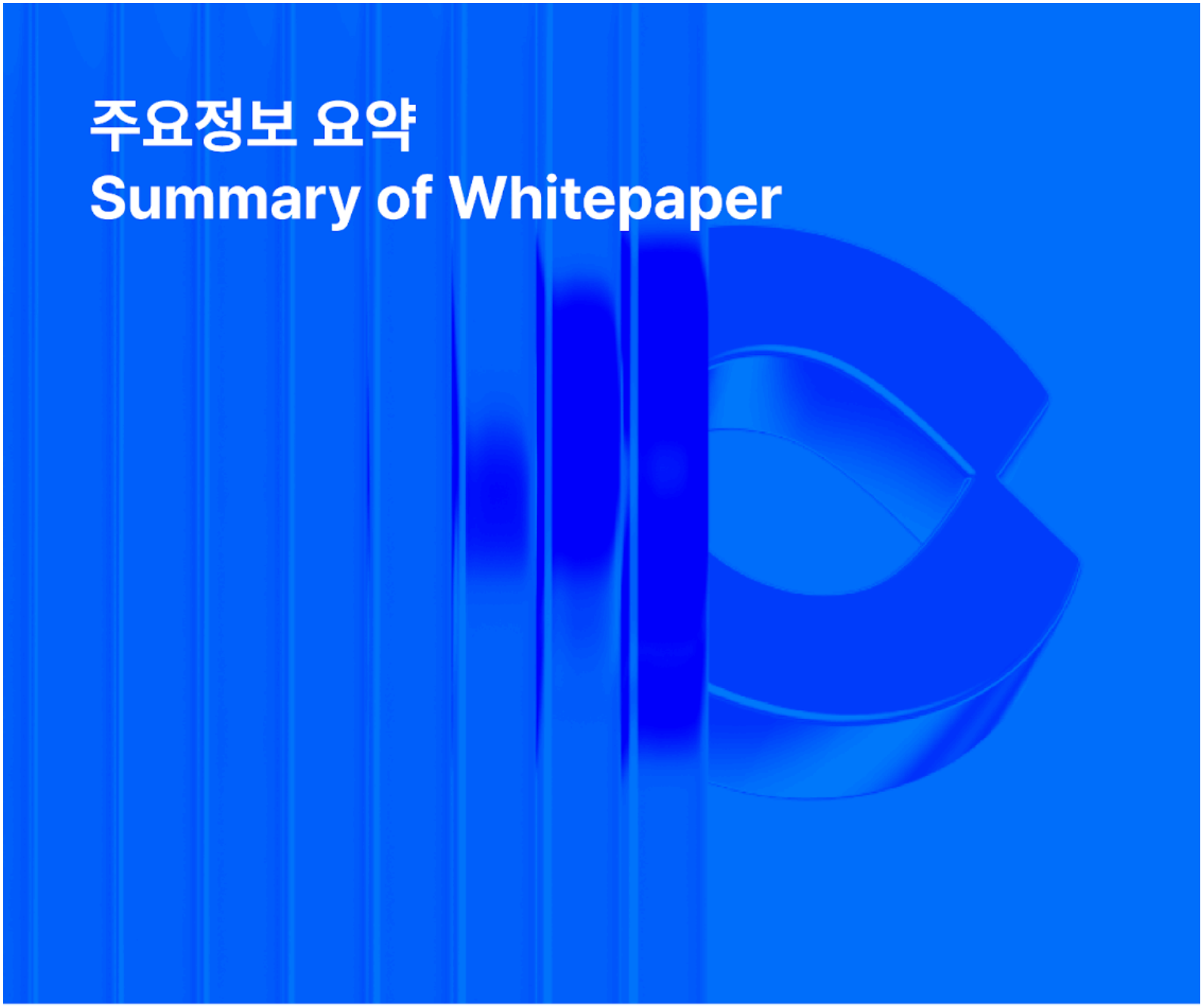
주요정보 요약
Summary of Whitepaper



본 문서는 거래지원 가상자산 백서의 주요 내용을 한글로 설명한 주요정보 요약입니다.
코인원은 거래지원 가상자산의 주요정보 요약을 주기적으로 점검하여 가능한 한 최신 정보를 제공할 예정입니다.

coinone

오비터 파이낸스(OBT)

2025.06.05

기본 정보

가상자산 카테고리	유틸티리
거래지원 네트워크	Arbitrum One
홈페이지	https://www.orbiter.finance/
참고문헌 (백서, Docs 등)	https://docs.orbiter.finance/, https://www.orbiter.finance/ko/blog/sbbmo3egha85quea44cfpirw

1. 프로젝트 정보

개요

크로스롤업 거래의 궁극적인 해답
오비터 파이낸스는 는 이더리움 및 비트코인 네이티브 자산의 크로스롤업 거래를 신뢰 없이, 원활하게 지원합니다.
Ethereum, zkSync Era, zkSync Lite, Linea, Mantle, Base, StarkNet, opBNB, Scroll, Arbitrum, Arbitrum Nova, Loopring, Optimism, Polygon, Polygon zkevm, BNB 체인, Zora, ImmutableX, BOB, BEVM, Bitlayer, BSquared 등 다양한 네트워크를 지원합니다.

주요 기능
오비터 파이낸스는 다음과 같은 다양한 기능을 제공합니다:

- 보안
  롤업의 보안을 활용해 네트워크 간 데이터 동기화에 따른 위험을 최소화합니다. 롤업은 메인넷과 데이터를 동기화하므로 전송 과정의 보안을 보장합니다.

- 호환성
  EVM 롤업뿐 아니라 비EVM L2 및 L3, Validium, DApp 전용 롤업까지 지원합니다. 이러한 다용성으로 다양한 사용 사례에 적합하며, 거래 유연성을 필요로 하는 사용자에게 매력적인 선택지가 됩니다.

- 속도
  오비터 파이낸스는 매우 빠른 처리 속도를 자랑합니다. 두 EOA(외부 소유 계정) 간 거래를 10~20초 이내에 완료합니다.

- 비용 효율성
  오비터 파이낸스는 네트워크 기본 비용 역시 가장 낮게 제공합니다. 출발지와 목적지 네트워크에서 두 EOA 간 거래의 가스비 합계가 비용입니다.

- 개방성
  다양한 ERC20 토큰 유동성의 탈중앙화 추가를 지원합니다. 개발자는 SPV를 배포해 환경을 구축할 수 있고, 크로스롤업 거래 및 메시지 이벤트를 맞춤화할 수 있습니다. 이러한 개방성으로 사용자는 거래에 더 큰 유연성과 제어권을 가집니다.

- 신뢰 불필요
  오비터 파이낸스는 탈중앙화 인센티브 프론트엔드를 개발했습니다. 이를 통해 서드파티 DApp이 크로스롤업 브릿지 프로토콜과 호환되는 프론트엔드 인터페이스를 구축할 수 있습니다.

브릿지 프로토콜

크로스롤업 거래에서의 역할

- **송신자 (Sender)**: 크로스 환경 상호운용 시스템을 통해 거래를 시작하는 사용자입니다.
- **메이커(Maker)**: 서로 다른 네트워크 간의 원활한 연결을 보장하며 크로스롤업 서비스를 제공하는 주체입니다.
- **딜러(Dealer)**: 탈중앙화된 프론트엔드를 제공하고 그에 따른 인센티브를 받는 주체입니다.
- **제출자(Submitter)**: 딜러로부터 생성된 수익 트리의 루트를 제출하는 역할을 담당합니다.

워크플로우

오비터 파이낸스의 주요 목표는 이더리움 생태계 내에서 안전하고 탈중앙화된 크로스롤업 브릿지를 구축하는 것입니다. 메인넷-롤업 간 상호운용성을 개선하기 위해 개발되었습니다.

이 목표를 달성하기 위해 오비터 파이낸스는 원래 크로스롤업 거래를 낙관적 원칙(optimistic principle)에 기반해 설계했습니다. 모든 거래가 유효하다고 가정하며, 사용자가 중재를 신청해 크로스롤업 거래 결과에 이의를 제기할 수 있는 중재 메커니즘을 마련했습니다.

블록 익스플로러를 통해 거래 로그를 확인하면, 오비터 파이낸스의 독특한 특징을 발견할 수 있습니다. 송신자는 컨트랙트 주소가 아닌 메이커의 EOA(외부 소유 계정)로 직접 거래를 시작합니다.

이 특징은 오비터 파이낸스를 다른 브릿지 프로토콜과 차별화합니다. 메이커는 서비스를 자동화하는 클라이언트를 직접 개발·운영하거나, 오비터 파이낸스 팀이 제공하는 오픈소스 클라이언트를 활용할 수 있습니다.

송신자가 출발지 네트워크에서 메이커에게 거래를 시작하면, 메이커는 목적지 네트워크에서 자산을 송신자에게 전송할 책임을 집니다.

메이커는 아래 세 가지 핵심 파라미터를 확인해 거래를 완료합니다.

토큰 표준

메이커가 MDC(메이커 예치 컨트랙트)에 마진을 입금할 때, 보류 수수료(Withholding Fee, 미리 정해진 고정 수수료), 거래 수수료(Trading Fee, 거래 금액의 일정 비율), 인정된 토큰(Endorsed Token)을 지정해야 합니다.

이 파라미터는 EBC(이벤트 바인딩 컨트랙트)에 저장되며, 메이커 클라이언트와 지속적으로 동기화됩니다.

(참고: 가스비가 변동하는 특성을 고려해 오비터 파이낸스는 목적지 네트워크의 Gwei 비율에 따라 주기적으로 수수료를 조정합니다. 이로써 오비터 파이낸스의 수수료가 시장 평균보다 낮은 수준을 유지합니다. 수수료 조정은 자주 발생하지 않습니다. 송신자는

Orbiter 웹사이트에서 현재 수수료를 확인할 수 있습니다.)

계산 예시:

메인넷에서 zkSync로 1ETH를 전송할 때, 거래 수수료는 전송 금액의 0.03%, 보류 수수료는 0.0014ETH입니다.

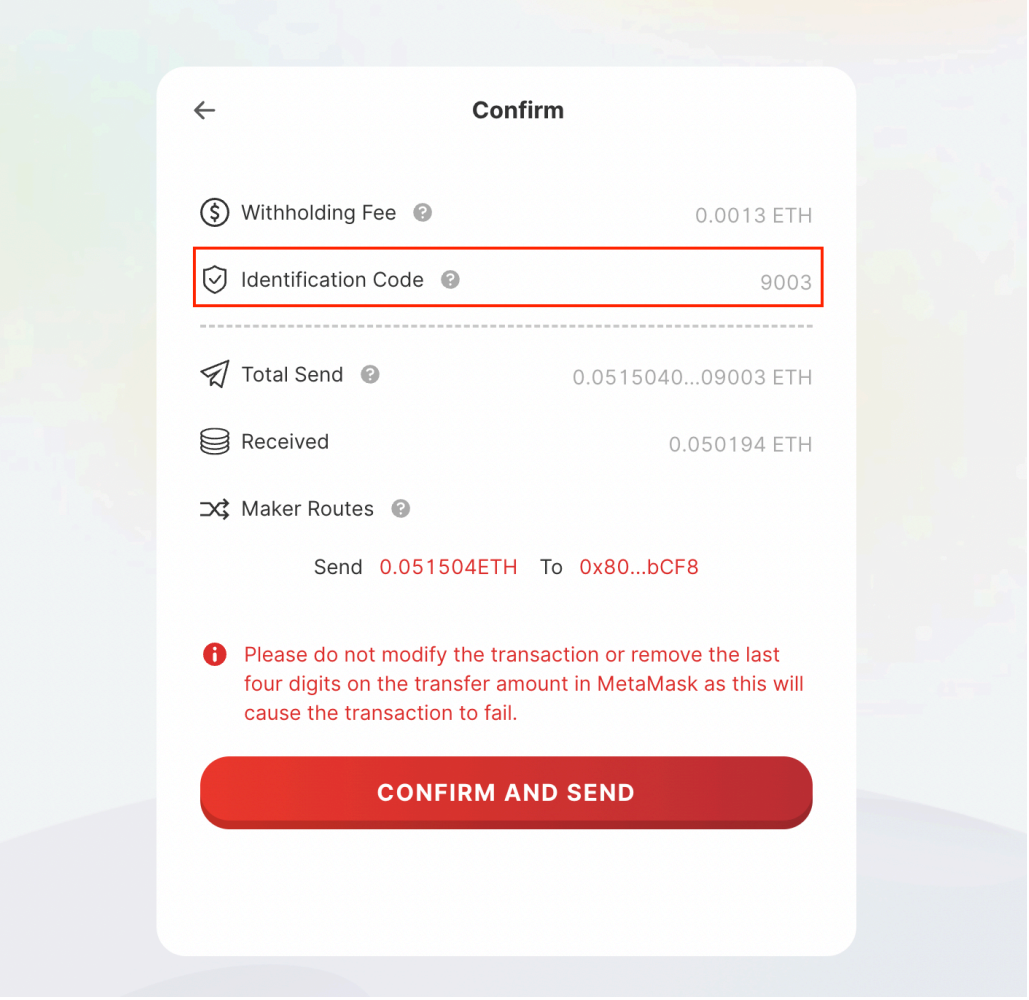
전송 비용은 0.03%(1-0.00014)ETH + 0.0014ETH = 0.0017ETH입니다.

100 USDC를 메인넷에서 zkSync로 전송할 때, 거래 수수료는 전송 금액의 0.3%, 보류 수수료는 1.5USDC입니다.

전송 비용은 0.3%(100-1.5)USDC + 1.5USDC = 1.8USDC입니다.

송신자가 받는 금액

메이커는 송신자가 받아야 할 토큰 종류를 확인한 후, EBC에 정의된 공식에 따라 정확한 금액을 계산합니다.



보안 보증 방식

크로스롤업 보안 모델

이 프로토콜의 목적은 크로스체인 거래가 아닌, 크로스롤업 시나리오 내의 과제를 해결하는 데 있습니다. 크로스체인 프로젝트는 서로 다른 체인 간 거래의 안전성 확보와 51% 공격 방지에 주력합니다. 반면, 크로스롤업 프로젝트는 각 롤업이 이더리움 데이터 레이어를 공유함으로써 51% 공격 위험을 본질적으로 줄입니다.

이 전제에 기반해, 오비터 파이낸스가 설계한 크로스롤업 메커니즘은 이더리움 레이어2의 보안 특성을 그대로 계승합니다.

거래 내 보안 메커니즘: 중재(Arbitration)

송신자(Sender) 또는 메이커(Maker)가 프로토콜을 위반하거나 악의적 행위를 할 경우, 해당 행위를 유발한 당사자는 도전자(Challenger)가 되고, 상대방은 도전받은 자(Challenged)가 됩니다. 양측 모두 제로지식 증명(ZKP)과 시스템 내 배포된 스마트 컨트랙트를 활용해, 비용 효율적으로 거래의 유효성을 입증할 권리가 있습니다.

이런 악의적 행위를 방지하기 위해, 오비터 파이낸스는 중재(Arbitration) 메커니즘을 도입합니다.이는 송신자가 합리적 시간 내에 자산을 받지 못할 경우, 거래 이슈를 추적하고 해결할 수 있도록 지원하는 혁신적 시스템입니다.

송신자는 목적지 네트워크에서 자산을 일정 시간 내에 받지 못할 경우 중재 절차를 시작할 수 있습니다. 이때, 송신자는 거래의 유효성을 증명할 거래 증명을 제출해야 합니다. 메이커는 자산 전송이 진행 중이거나 완료되었음을 입증하는 증거를 제출할 수 있습니다. 메이커가 필요한 거래 증거를 송신자에게 제출하면, 메이커는 손실을 입지 않습니다. 증거를 제출하지 못할 경우, 송신자는 해당 거래와 관련된 메이커의 초과 마진 일부를 포함해 전액 환불을 받습니다.

중재 절차 내 세 가지 컨트랙트

중재 과정에서 거래를 검증하기 위해 세 가지 컨트랙트가 네트워크에 배포됩니다.

- MDC 컨트랙트(Maker Deposit Contract):

  메이커가 예치한 초과 마진을 보관하며, 송신자에게 보상을 처리합니다.

- EBC 컨트랙트(Event Binding Contract):

  출발지와 목적지 거래 간의 대응 관계를 검증합니다.

- ZK-SPV(Zero-Knowledge Simple Payment Verification):

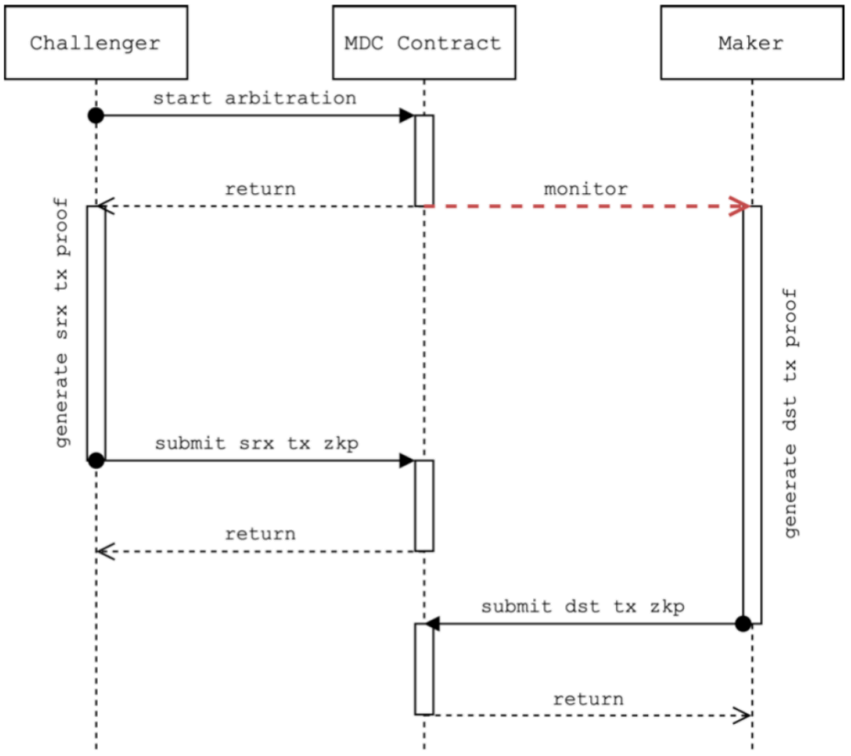
  제로지식 증명 기술을 활용해 크로스롤업 거래의 존재와 유효성을 입증합니다.

  존재(Existence) : 출발지와 목적지 거래가 각각 레이어1에서 검증 가능하며, 실제로 각 레이어2에서 발생했음을 확인합니다.

  유효성(Validity) : 송신자의 출발지 거래 의도를 확인하고, 메이커의 목적지 거래 결과가 사전 정의된 규정을 따르는지 검증합니다.

MDC, EBC, ZK-SPV는 이더리움 생태계 내 스마트 컨트랙트가 지원되는 도메인에 구현됩니다.

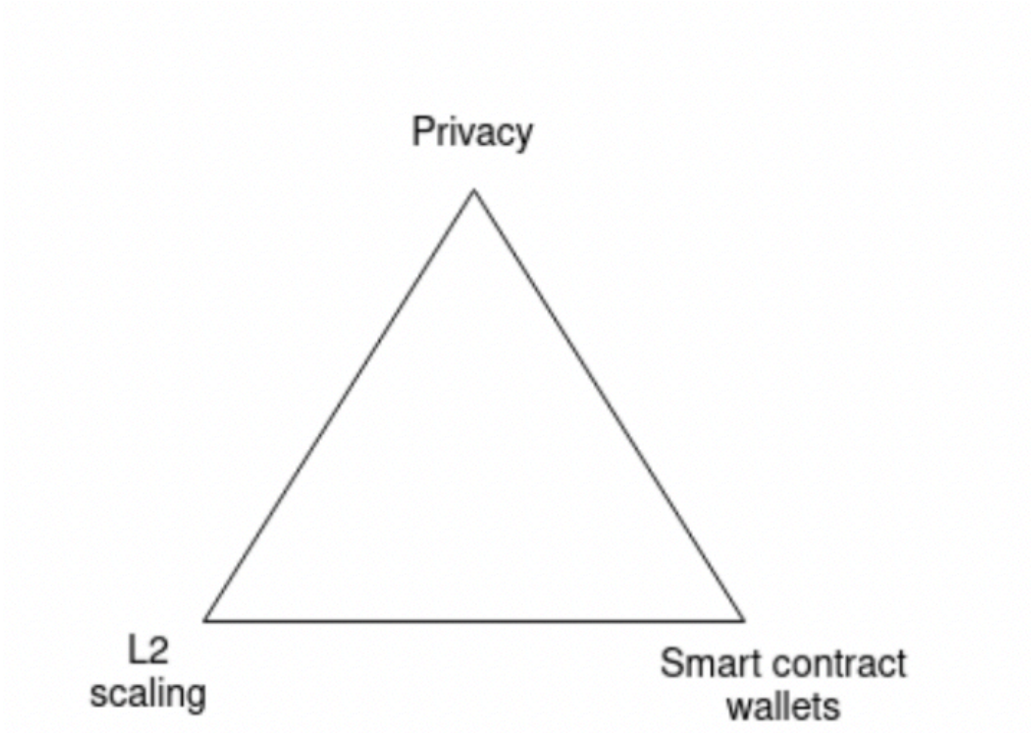
아래 차트는 이 세 가지 스마트 컨트랙트가 중재 절차에서 어떻게 작동하는지 보여줍니다.



인사이트와 인프라 진화 방향

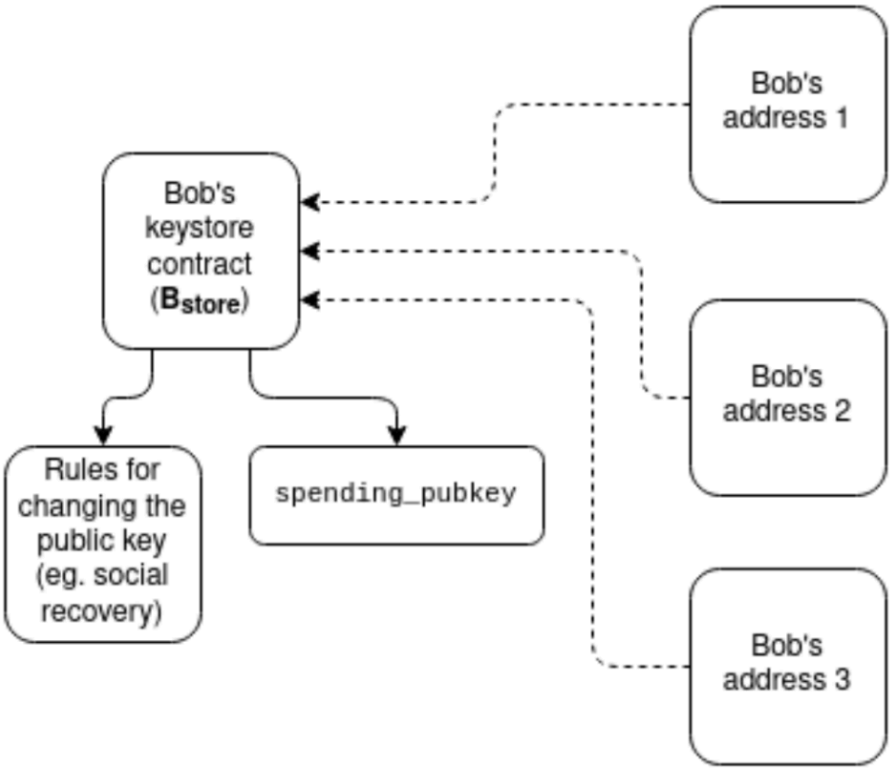
오비터 파이낸스의 진화적 여정

오비터 파이낸스의 진화는 이더리움의 발전 경로와 밀접하게 연결되어 있습니다. 이더리움의 성장은 크게 세 가지 핵심 기술, 즉 프라이버시 강화, 레이어2 확장성 솔루션, 그리고 스마트 컨트랙트 지갑의 발전에 의해 이뤄졌습니다. 이 세 가지 변화는 이더리움이 실험적 단계를 넘어 성숙한 기술 생태계로 자리매김하는 데 결정적 역할을 했으며, 사용자에게 열린 글로벌 무허가형 경험을 제공합니다. 비탈릭이 'The Three Transitions'에서 언급했듯, 이 세 요소는 동시에 필수적이며, 이더리움 생태계 내 상호작용의 기본 요소로 자리 잡고 있습니다.



확장성은 이더리움 생태계의 생명줄입니다. 레이어2 확장성 솔루션은 이더리움의 확장성 한계를 극복하는 데 핵심적 역할을 하며, 더 빠르고 저렴한 거래를 가능하게 하면서도 메인넷의 보안을 유지합니다. 레이어2 확장성의 등장은 DApp의 글로벌 접근성을 높이고 새로운 기회를 창출합니다. 오비터 파이낸스는 레이어2 생태계에 진입하면서, 레이어2 도입이 확대될수록 사용자가 다양한 레이어2 네트워크에 자산을 보유하게 됨을 인식합니다. 대부분의 레이어2 사용자는 EOA(외부 소유 계정)에 의존하며, EOA 주소는 공개키 해시로 구성되어 레이어1과 레이어2에서 일관된 사용자 경험을 제공합니다. 그러나 스마트 컨트랙트 지갑을 사용할 경우, 단일 불변의 주소 유지가 복잡해지고, 다양한 계정에 접근하는 데 필요한 키가 시간이 지나면서 변경될 수 있습니다. 이 문제를 해결하기 위해 다양한 네트워크에서 키를 효율적으로 관리할 수 있는 솔루션이 필요합니다.

비탈릭은 '자산/키스토어 분리 아키텍처'를 제안해 이 문제를 해결하고자 했습니다. 이 아키텍처에서 각 사용자는 메인넷 또는 특정 레이어2 네트워크에 위치한 키스토어 컨트랙트를 보유하며, 다양한 레이어2 네트워크에 주소를 두고 각 주소의 검증 로직이 키스토어 컨트랙트를 가리키도록 합니다. 자산을 사용하려면 현재 또는 최근 사용된 지출 공개키임을 증명하는 증거를 키스토어 컨트랙트에 제출해야 합니다. 오비터 파이낸스는 이 패러다임을 시스템 복잡성 최소화와 키스토어 업데이트 절약에 맞춰 접근합니다. 각 거래마다 크로스체인 증명을 제출해 키스토어 키의 현재 상태를 명확히 해야 하며, 이 방식은 장점이 있지만 크로스체인 증명을 경제적으로 만들기 위한 엔지니어링 노력이 필요합니다. 또한 거래당 비용이 높고, 현재 ERC-4337 표준과는 호환성이 떨어집니다.



오비터 파이낸스의 기술 전문가들은 이 증명을 ZK-SNARK로 구현할 수 있음을 확인했습니다. 전체 브랜치 대신 Merkle 브랜치의 ZK-SNARK를 사용해 데이터 비용을 줄일 수 있으며, 오프체인 집계 기술(예: EIP-4337 기반)을 활용해 한 블록 내 모든 크로스체인 상태 증명을 단일 ZK-SNARK로 검증할 수 있습니다. 이 집계란 각 블록 내 사용자가 제출한 모든 증명을 하나의 메타 증명으로 결합하는 것을 의미하며, 사용자 기반이 충분히 커졌을 때 실현 가능합니다. 오비터 파이낸스는 ZK-SNARK를 도입함으로써 사용자의 AA 거래를 집계해 가스를 절약할 수 있음을 깨달았으며, ERC-20 거래 가스 소모를 최대 20~30%까지 줄일 수 있습니다. 이는 전체 인프라의 핵심 요소입니다.

비탈릭은 레이어2가 레이어1의 확장성 솔루션이라면, 레이어2 위에 또 다른 레이어가 존재해 확장성과 TPS를 더욱 높일 수 있다고 언급했습니다. 오비터 파이낸스는 레이어2 솔루션 영역에서 이더리움 전체 성능을 더욱 높일 수 있는 또 다른 확장성 솔루션이 존재하는지 탐구합니다. 현재 롤업과 같은 확장성 솔루션은 계산과 데이터라는 병목 현상을 완화하기 위해 다양한 접근법이 결합된 결과물입니다. 데이터의 특성상 반복 압축에는 한계가 있으며, 각 롤업 구현체마다 고유한 특성과 보안·속도·비용 간 트레이드오프가 존재합니다. 따라서 또 다른 레이어를 쌓는 것은 항상 실현 가능하거나 쌓을 수 있는 것은 아니며, 모든 레이어2 솔루션을 아우르는 인프라 구축이 과연 현명한지도 의문이 듭니다. 롤업 위에 롤업을 쌓거나 레이어3를 도입하면 초기 가정보다 더 복잡해질 수 있기 때문입니다.

오비터 파이낸스는 이더리움 롤업 간 상호운용성을 높이는 데 꾸준히 집중해 왔으며, 롤업 간 원활한 소통을 위해 견고한 인프라가 필요함을 인식합니다. 이더리움 확장성에서 가장 큰 과제 중 하나는 원활한 상호운용성 달성입니다. 현재 오비터 파이낸스는 AA와 유사한 '슈퍼 DApp' 개념을 탐구하고 있습니다. 이 슈퍼 DApp은 다양한 롤업의 고유 특성을 활용해 특정 사용 사례를 해결할 수 있으며, 최종 거래를 완료하려면 수많은 이전 롤업의 거래에 의존해야 합니다. 하지만 현재 롤업 아키텍처에서 이를 구현하면 가스비가

높아지고 지연이 발생해 모든 롤업에 적용하기 어렵습니다. 롤업은 1,000만 가스 이상의 L2 거래 배치가 쌓일 때까지 기다릴 수 있지만, 이 경우 검증 시간이 길어집니다.

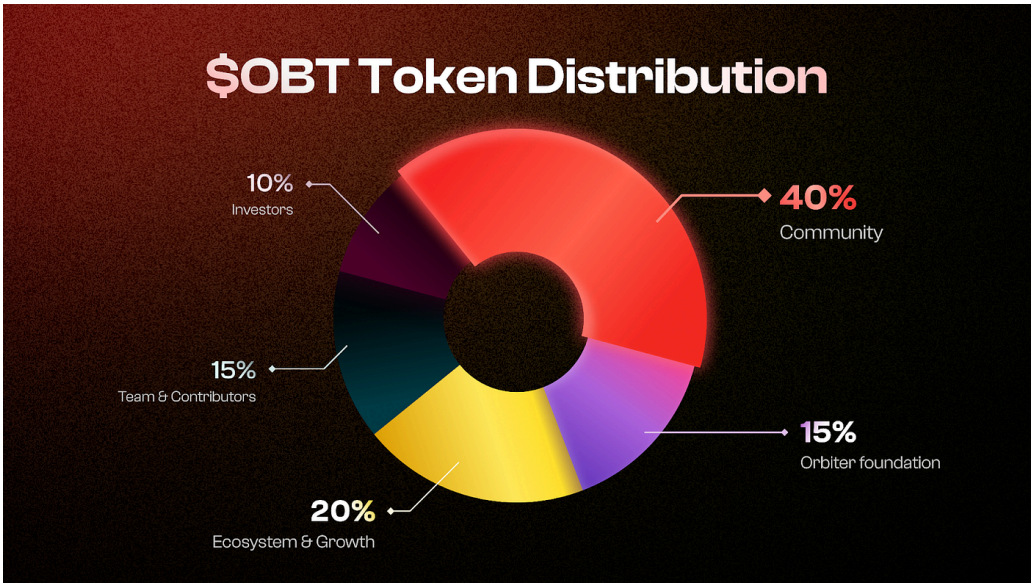
제안하는 방식은 ZK 롤업이 배치 검증자 컨트랙트로부터 메시지를 받아 여러 개의 유사한 패턴의 명제를 한 번에 검증받는 것입니다. 이 배치 증명은 재귀적 SNARK 방식으로 구성할 수 있습니다. 오비터 파이낸스는 모든 ZK 롤업이 참여할 수 있는 오픈 프로토콜인 Aggregated zkProver를 개발했습니다. 이 프로토콜은 호환 가능한 모든 ZK 롤업의 증명을 집계하며, 각 롤업은 거래 수수료에서 발생하는 수익을 받을 수 있습니다. 배치 핸들러 컨트랙트는 증명을 한 번 검증한 뒤, 각 롤업에 해당 롤업의 요구사항에 맞는 트리플(세 가지 정보)을 담은 메시지를 보냅니다. 이 트리플이 배치 핸들러 컨트랙트에서 왔다는 사실이 전환의 유효성을 입증하는 증거가 됩니다. 이 방식은 각 롤업에 상당한 비용 절감 효과를 제공하며, 모든 ZK 롤업 간 트레이드오프를 균형 있게 조정하는 인프라 역할을 합니다. 비탈릭도 '레이어3'에 관한 글에서 Aggregated zkProver와 유사한 개념을 언급하며, 단순화되고 고도로 특화된 중간 레이어가 추가적인 토큰 없이도 구축 가능하고, 빈번한 거버넌스 변경에 강하며, 보안성이 높을 수 있음을 강조합니다.

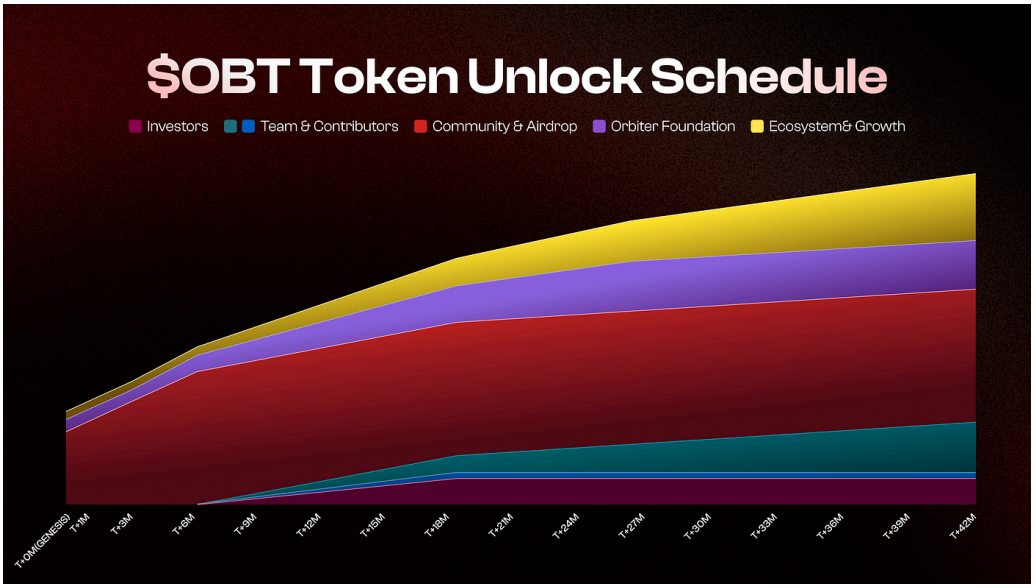
2. 토큰 이코노미

가상자산 소개

오비터 파이낸스는 탈중앙화를 위한 첫 단계로, 자체 토큰인 OBT를 도입했습니다. OBT는 이더리움 기반의 ERC-20 토큰으로, 거버넌스, 스테이킹, 생태계 참여 보상 등 다양한 기능을 수행하며, 2025년 2월부터 온체인 거버넌스 기능이 활성화될 예정입니다. 토큰의 전체 공급량 중 약 28%가 토큰 생성 이벤트(TGE) 시점에 유통되며, 커뮤니티를 중심으로 강한 참여 기반을 구축하고자 설계되었습니다.

발행량 및 유통량계획





- **40% 커뮤니티**
  커뮤니티 인센티브 및 에어드랍을 통해 사용자에게 분배되며, 사용자 성장, 프로젝트 홍보, 생태계 활성화를 도모합니다.
    - **초기 에어드랍**: 전체 공급량 중 22%를 기존 Orbiter 사용자에게 분배합니다.
    - 이후 **6개월 동안 매월 3%**씩 자격 보유자에게 에어드랍됩니다.
- **20% 생태계 및 성장**
  생태계 구축과 시장 확장을 위한 토큰으로, 파트너십 육성과 지속 가능한 사업 개발을 목표로 합니다.
    - **2.5%는 TGE(토큰 생성 이벤트)** 시점에 언락됩니다.
- **15% Orbiter 재단**
  Orbiter 재단은 “All Chains One Hub” 비전을 실현하기 위해 $OBT를 사용합니다.
    - **3.5%는 TGE 시 언락되며**, 나머지는 23개월에 걸쳐 매월 분할되어 배분됩니다.
- **15% 팀 및 기여자**
  프로젝트에 장기적으로 기여한 팀 및 핵심 기여자에게 할당되며, 기술적 혁신과 지속적 발전을 위한 동기를 제공합니다.
- **10% 투자자**
  시드 및 시리즈 A 투자자에게 할당됩니다.

에어드랍 자격 조건은 2021년 12월 이후 최소 2개월 이상 Orbiter 프로토콜(브릿지/생태계)을 사용하고, 최소 40 OPoints를 보유해야 합니다. OPoints는 주로 크로스체인 거래를 기준으로 산정되며, 최대 5,000점까지 인정됩니다. 추가로 Discord 모더레이터, Ace NFT 및 Expert NFT 보유자, Orbiter가 주최한 특정

오프라인 이벤트 참가자도 에어드랍 대상에 포함됩니다. 봇 방지를 위해 여러 안티 시빌 규칙이 적용되며, Arbitrum 등 다른 프로젝트의 시빌 라이브러리 및 관련 지갑 주소는 차단됩니다.

에어드랍 청구 일정은 다음과 같습니다. 1단계(2025년 1월 20일 06:00 UTC)에는 첫 번째 스냅샷 기준 최대 5,600 OBT를 청구할 수 있으며, Ace NFT 보유자는 NFT당 17,000 OBT를 청구할 수 있습니다. 2단계(2025년 1월 23일 06:00 UTC)에는 Expert NFT 보유자가 NFT당 2,300 OBT를 청구할 수 있습니다. 3단계(2025년 1월 25일 06:00 UTC)에는 모든 사용자가 나머지 OBT를 청구할 수 있습니다.

OBT는 단순한 유틸리티 토큰을 넘어, 커뮤니티가 직접 운영과 의사결정에 참여할 수 있는 수단으로 기능하며, Orbiter 생태계 내 실질적인 영향력을 행사하는 핵심 자산으로 자리매김할 예정입니다.

위험고지 안내
Disclaimer

본 문서에 기재된 정보는 당사(코인원)가 본 가상자산 심사 시점에 접근 가능한 정보 채널을 통하여 확인한 것으로, 정확하지 않거나 투자시점에는 변경 또는 유효하지 않을 수 있습니다.

가상자산 발행자가 공시한 내용 및 백서를 통해 정확한 정보를 확인하신 후 투자하시기 바랍니다.

가상자산은 법정화폐가 아니므로 특정 주체가 가치를 보장하지 않습니다.

coinone