



인터폴드(FOLD)

주요내용설명서(국문백서)
Korean White Paper

2026년 8월 28일

Disclaimer

본 번역본은 2026년 8월 28일 기준의 인터폴드(FOLD) 백서 및 공식 Docs 내용 위주로 번역되었습니다.

빗썸은 발행주체 또는 운영주체가 제공하는 가상자산의 총발행량, 유통량 계획, 사업 계획 등이 포함된 정보를 이용자들의 편의를 위해 참고용으로 제공하고 있습니다.

본 번역본은 그 내용이 정확하지 않을 수 있으며 원문의 내용이 일부 누락될 수 있으므로, 정확한 정보 습득을 위해서는 원문을 참고하시거나 원문 작성 측에 문의하시기를 바랍니다. 또한 본 번역본은 오픈 커뮤니티의 검토에 따라 내용이 변경될 수 있습니다.

프로젝트 소개

인터폴드(The Interfold)는 암호화 실행 환경(Encrypted Execution Environment, E3) 형성에 필요한 구성 요소를 갖추고 다양한 행위 주체를 조율하는 오픈 소스 프로토콜입니다. 신개념 실행 환경인 E3는 완전 동형 암호(FHE)¹를 비롯하여 영지식 증명², 분산 임계값 암호화³와 같은 고도화된 암호화 기술을 활용해 안전하게 연산을 실행합니다. 신뢰 가능한 하드웨어를 기반으로 하는 신뢰 실행 환경(TEE)⁴의 경우 부채널 공격⁵에 취약하고 검증의 정확도가 아쉬운 반면, 탈중앙화 아키텍처와 고도화된 암호화 기술, 개인 정보 보호가 가능한 메커니즘 설계가 결합된 인터폴드의 프로토콜은 데이터의 프라이버시 및 무결성과 정확한 연산 실행을 경제적·암호학적 방식으로 강력하게 보장합니다.

그러한 보장은 다양한 사용 사례에 유연하고도 탄력적으로 연산을 지원할 수 있는 인터폴드의 모듈형 아키텍처 덕분에 가능합니다. 인터폴드는 스테이킹⁶ 기반의 노드⁷ 네트워크와 다중 연산 과정을 활용함으로써 스테이킹 메커니즘, 비례 수수료, 페널티가 결합된 정교한 경제 모델을 도입하여 참여자들의 올바른 작업 수행을 유도합니다. 이러한 설계 방식은 신뢰 시스템과 관련된 위험성을 완화해줄 뿐만 아니라 프라이버시 애플리케이션을 다양한 분야에 맞춰 개발하는 데 활용할 수 있는 범용적인 토대를 제공합니다. 인터폴드를 통해 기관은 보안을 유지하고 규제를 준수하면서도 민감한 데이터를 활용할 수 있습니다.

¹ Fully homomorphic encryption

² Zero-knowledge (zk) proof

³ Distributed threshold encryption

⁴ Trusted execution environment

⁵ Side-channel attack

⁶ Staking

⁷ Node

비즈니스 모델

인터폴드 행위 주체

인터폴드는 세 가지 유형의 프로토콜 주체가 협력하여 암호화 데이터를 기반으로 안전한 프라이버시 연산을 실행할 수 있도록 지원합니다. 주체별 역할 및 기여 방식은 아래와 같습니다.

1. 요청자(Requester)

요청자는 보안 연산 과정을 개시하고 연산 관련 매개변수를 설정합니다. 개인 사용자 혹은 단체는 원하는 E3에 대한 스마트 컨트랙트⁸ 진입점을 호출하고 담보를 예치하여(필요한 담보 규모는 노드 수, 임계값 수준, E3 사용 기간에 비례) 인터폴드 네트워크에 E3를 요청할 수 있습니다.

2. 데이터 제공자(Data Provider)

데이터 제공자는 요청된 E3에 입력할 데이터를 공급하는 개인 사용자 혹은 시스템입니다. 데이터 제공자의 평문 데이터는 요청된 E3에 의해 생성 및 온체인에 공개되는 공개 임계값 키⁹를 통해 암호화되기 때문에 연산 과정 중 데이터의 보안과 프라이버시가 유지됩니다.

3. E3

E3는 인터폴드 프로토콜의 작업 조율을 통해 암호화 데이터에 대한 요청된 보안 연산을 실행하는 핵심 단위입니다. E3 내부에서 탈중앙화 노드 네트워크는 요청된 FHE 연산의 출력값에서 검증된 값만을 복호화합니다. 이를 통해 연산을 실행하면서도 데이터의 프라이버시와 보안을 유지할 수 있습니다.

⁸ Smart contract

⁹ Public threshold key

E3 아키텍처

E3는 암호화 데이터에 대한 안전하고 검증 가능한 연산을 가능하게 하는 여러 모듈형 구성 요소로 이루어져 있습니다. E3 구성 요소들은 데이터 프라이버시 및 연산의 무결성을 유지하여 신뢰 솔루션 관련 위험성을 완화합니다. E3의 핵심 구성 요소는 아래와 같습니다.

사이퍼노드 위원회(Ciphernode Committee, CiCo)

선정된 사이퍼노드들의 집합으로서 분산형 키 생성과 연산 제공자(Compute Provider)가 출력 및 공개한 암호문의 복호화를 담당합니다. 위원회에 소속될 노드는 무작위 추천 방식을 통해 선출되기 때문에 신뢰 주체가 분산되어 보안이 강화됩니다. 이러한 탈중앙화 방식은 단일 노드에게 완전한 통제 권한이 주어져 데이터 침해나 위·변조가 발생할 위험을 없앱니다.

E3 프로그램(E3 Program, E3P)

수행될 연산을 정의하는 명령어 집합입니다. E3 프로그램은 온체인에 공개된 암호문을 입력값으로 취해 평문 출력값을 생성하는 방식으로 데이터와 결과값의 기밀성을 보장합니다. 다방면으로 쓰일 수 있게 설계되어 있으므로 보안을 유지하면서 다양한 종류의 연산 작업을 지원하는 것이 가능합니다.

보안 과정(Secure Process, SP)

FHE 연산을 수행하는 E3 프로그램의 구성 요소로서 연산 제공자에 의해 실행됩니다. 인터폴드 프로토콜이나 사이퍼노드, 데이터 제공자가 관리하는 다른 시스템 구성 요소와는 달리, 보안 과정은 연산 제공자의 검증 가능한 구성 요소를 토대로만 실행됩니다. 연산 제공자는 보안 과정이 정확하게 실행되었음을 검증하거나 그에 대한 온체인 증명을 생성하게 됩니다.

연산 제공자(Compute Provider, CP)

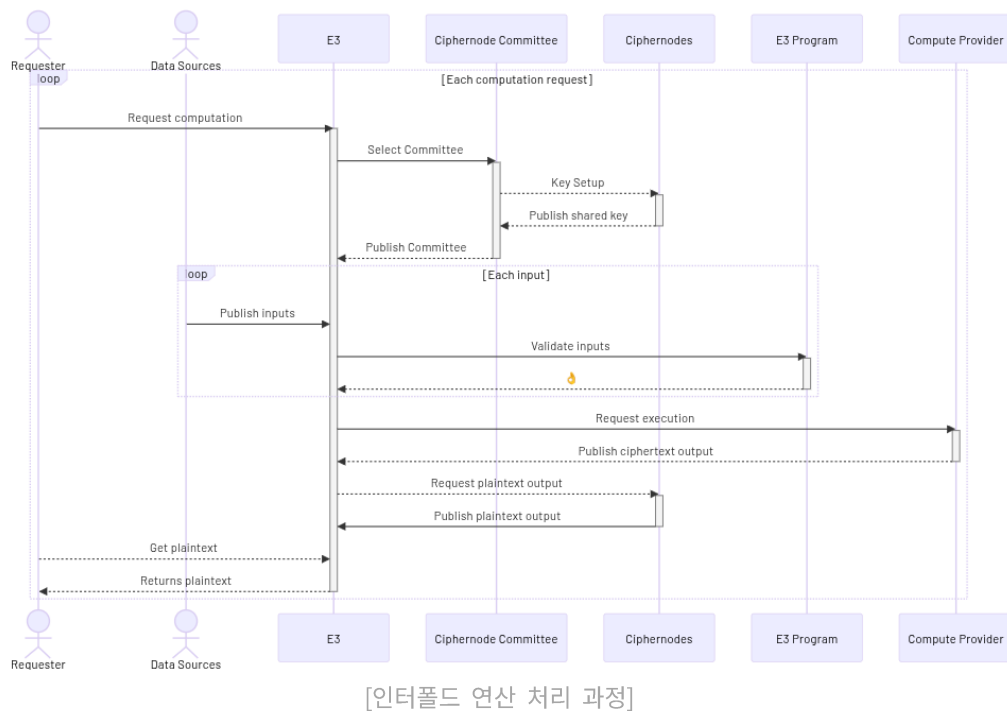
E3 내에서 보안 과정을 실행하는 플랫폼으로, E3는 연산 제공자가 보안 과정을 통해 특정 E3에 대한 공개된 입력값을 연산하여 정확한 암호문을 제공한다는 것을 전제로 작동합니다. 연산 제공자는 증명 기반 시스템과 오라클¹⁰ 기반

¹⁰ Oracle

시스템으로 분류됩니다. 증명 기반 제공자(리스크 제로¹¹, 석싱트의 SP1¹², 졸트¹³, 넥서스)는 실행의 정확성을 암호학적인 방식으로 보장하며, 오라클 기반 제공자(멀티시그¹⁴, 리얼리티닷이드¹⁵, 클레로스 코트¹⁶, 에이피아이쓰리)는 합의 혹은 경제적 메커니즘을 활용해 검증을 수행합니다. 이 같은 모듈성¹⁷을 바탕으로 비용·보안·신뢰 요건을 고려해 E3에서 연산을 실행할 가장 적합한 연산 제공자를 선정할 수 있습니다.

인터폴드 작동 방식

인터폴드는 여러 행위 주체 및 E3 구성 요소가 관여하는 체계적인 다중 절차를 통해 탈중앙화 방식의 안전한 연산 작업을 지원하여 작업 실행의 정확성을 보장하고 프라이버시를 보호합니다. 아래 이미지는 연산 과정에서 발생하는 상호 작용을 시각화한 자료입니다.



¹¹ RISC Zero

¹² Succinct Processor 1

¹³ Jolt

¹⁴ Multisig

¹⁵ Reality.eth

¹⁶ Kleros Court

¹⁷ Modularity

1단계: 요청

누구나 언제든지 인터폴드에 연산을 요청할 수 있습니다. 연산 요청에는 아래와 같은 사항들이 지정되어 있어야 합니다.

- 수행할 FHE 연산
- 연산 제공자 및 관련 매개변수
- 필요한 사이퍼노드 수
- 결과 검증에 필요한 유형별 노드 수
- 데이터 입력 기한 설정을 위한 타임스탬프¹⁸(해당 시점 이후 데이터 추가 입력 불가)
- 노드 활성화 유지 기간

연산 요청을 위해서는 작업을 수행하는 노드에게 최소한의 보상을 보장하기 위한 예치금이 필요합니다. 예치금 규모는 연산 절차의 마지막 단계인 복호화까지 다른 참여자들에 의해 증가할 수 있습니다.

2단계: 노드 선정

연산이 요청되면 추천 방식을 통해 필요한 수(임계값)의 사이퍼노드가 선택되어 사이퍼노드 위원회가 결성됩니다. 선정된 사이퍼노드들은 즉시 공동 공개 키를 생성하여 서로 공유합니다. 이러한 과정을 거쳐 연산을 위한 암호화 프레임워크가 안전하게 형성됩니다.

3단계: 데이터 입력 기한

사이퍼노드 위원회가 공동 공개 키를 공개하면 데이터 입력 기간이 시작됩니다. 입력 기간 동안 데이터 제공자는 연산을 위한 데이터 입력값을 제출할 수 있습니다. 제출된 데이터는 공개 키를 통해 암호화되어 기밀성이 보장됩니다. 모든 데이터 입력값에는 데이터 제공자가 제출한 데이터의 원본 데이터¹⁹를 알고 있으며, 데이터가 올바르게 형성되었고 다른 맥락에는 사용 불가하며 요청된 연산에 필요한 모든 검증 로직을 통과했음을 나타내는 영지식 증명이 필요합니다.

4단계: 실행

데이터 입력 기간이 종료되면 지정된 연산 제공자가 암호화된 입력값을 활용해 사전 설정된 E3 프로그램(FHE 연산 실행을 위한 보안 과정 포함)을 실행합니다. 그런 다음 암호문을 산출한 뒤 공개하여 실행 과정 동안 연산의 무결성이 유지되었음을 입증합니다.

¹⁸ Timestamp

¹⁹ Preimage

5단계: 복호화

연산 제공자가 요청된 연산에 대한 암호문 출력값을 공개했다면, 임계값만큼의 사이퍼노드들이 해당 연산 결과를 공동으로 복호화한 다음 공개해야 합니다. 연산 제공자의 연산 결과를 복호화한 평문을 공개하면 사이퍼노드가 해야 할 일은 끝이 나며, 이후 각 노드는 작업 예치금 중 자신의 몫을 청구할 수 있습니다. 해당 작업을 위해 위원회가 사용한 공개 키는 폐기해야 합니다.

토크노믹스

인터폴드 네트워크 내 인터폴드(FOLD)의 역할

인터폴드는 기밀 방식으로 협업을 진행하는 분산형 네트워크입니다. 애플리케이션은 E3를 요청하고, 사이퍼노드는 협력하여 연산이 안전하게 이루어지도록 합니다. 네이티브 토큰²⁰인 FOLD는 인터폴드 네트워크의 경제적 측면을 지원합니다.

FOLD의 유틸리티

FOLD는 서로 맞물려 있는 세 가지의 주요 유틸리티를 갖고 있습니다.

- **사이퍼노드 담보** – 사이퍼노드 운영자는 네트워크 참여에 대한 담보로 FOLD를 예치해야 합니다. 예치된 FOLD는 운영자가 네트워크에 등록되어 있는 동안 락업²¹되며 프로토콜에서 설정한 출금 대기 기간을 적용받습니다. 또한 운영자가 부적절한 행동을 저지르거나 할당된 작업을 제대로 수행하지 못했다는 점이 입증될 경우 예치된 토큰에 불이익이 가해질 수 있습니다. 이러한 메커니즘을 활용해 노드 운영에 경제적인 방식으로 책임성을 부여합니다.

²⁰ Native token

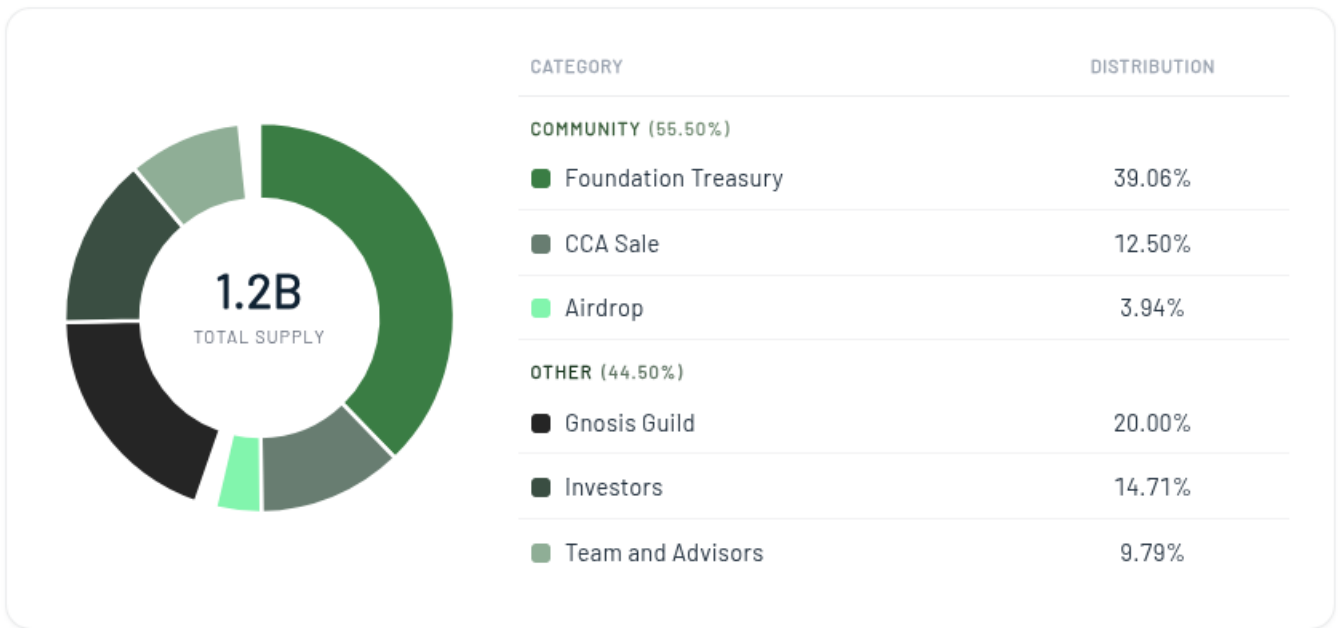
²¹ Lockup

- **프로토콜 인센티브** – 사이퍼노드 운영자는 완료된 E3 작업 수수료 중 일부를 지급받는 것 외에도 E3 위원회 구성원으로서 프로토콜에서 지정한 작업을 성공적으로 완료하는 경우 FOLD 인센티브를 획득할 수 있습니다.
- **거버넌스** – FOLD는 인터폴드 다오²²를 통해 거버넌스 참여를 지원하는 데 활용될 예정입니다. 거버넌스를 통해 네트워크 매개변수, 프로토콜 업그레이드, 트레저리²³ 관리와 관련된 사안들을 결정하게 될 수 있으며, 인터폴드 네트워크에 의해 작동되는 비밀 투표 메커니즘이 거버넌스 과정에 활용될 수 있습니다.

토큰 분배

- 총발행량: 12억 FOLD
- 토큰 생성 이벤트²⁴ 시점 유통량: 27.22%

총발행량 분배 현황은 아래 차트와 같습니다.



[FOLD 토큰 분배]

²² DAO (decentralized autonomous organization)

²³ Treasury

²⁴ Token generation event (TGE)

커뮤니티 할당

- **재단 트레저리**

개방형 환경에서 개발된 인터폴드는 LGPL²⁵ v3 라이선스에 따라 오픈 소스 소프트웨어로서 자유롭게 이용 가능합니다. 총발행량의 일부가 인터폴드 재단에 할당되어 우선 처리가 필요한 작업을 선제적으로 지원하거나 유의미한 기여 활동에 대한 소급 보상을 제공하는 데 활용될 수 있습니다.

- **연속 청산 경매(CCA)²⁶ 세일**

본 할당분은 두 번의 유니스왑 연속 청산 경매를 진행하는 데 할당되었으며, 토큰 전송 활성화 이전 인터폴드 커뮤니티 구성원 및 초기 지지자에게 토큰 세일에 공정하게 참여할 수 있는 기회를 제공하기 위한 목적으로 활용되었습니다.

- **에어드랍²⁷**

총발행량의 3.94%가 웹3.0, 프라이버시, 보안 분야의 전문가 및 단체가 해당 분야에 기여한 공로를 인정하는 차원에서 에어드랍되었습니다. 에어드랍 할당분 전량은 이미 대상자들에게 할당되었으며 24개월에 걸쳐 베스팅²⁸됩니다.

기타 할당

- **노시스 길드²⁹**

본 할당분은 노시스 길드의 초기 기여에 대한 보상을 제공하기 위해 마련되었으며 48개월에 걸쳐 베스팅됩니다.

- **투자자**

인터폴드(이전 명칭 엔클레이브(Enclave))는 아래와 같이 투자 유치 라운드를 진행한 바 있습니다.

- 프리시드: 가치 평가 2,000만 달러
- 시드: 가치 평가 2,580만 달러
- 리전³⁰ 라운드: 가치 평가 2,580만 달러

²⁵ Lesser General Public License

²⁶ Continuous Clearing Auction

²⁷ Airdrop

²⁸ Vesting

²⁹ Gnosis Guild

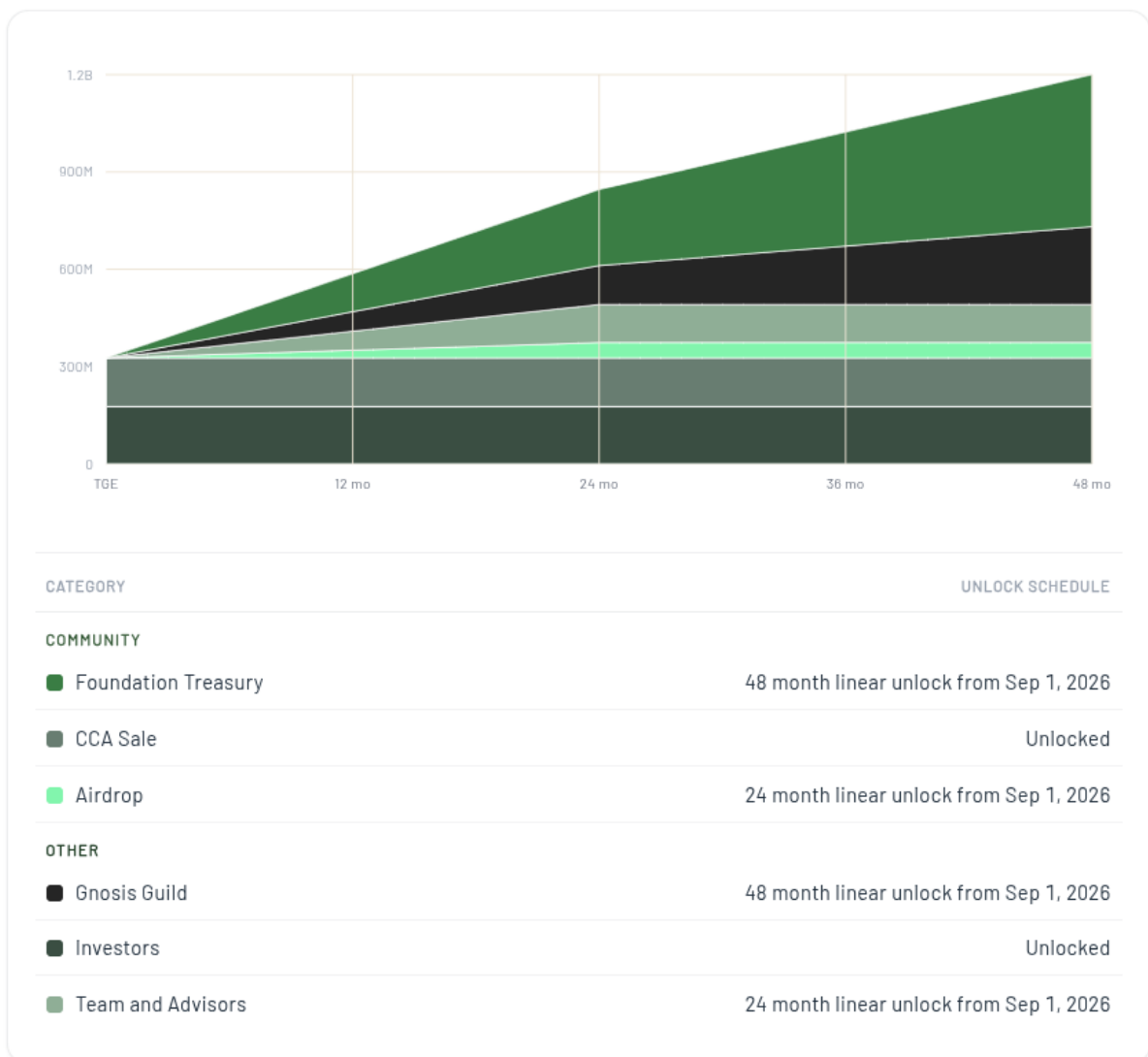
³⁰ Legion

투자자 할당분에는 위의 세 라운드에 할당된 수량이 모두 합산되어 있습니다. 락업이 적용되지 않으며 토큰 생성 이벤트 시점에 전량 전송 가능한 상태가 됩니다. 유니스왑 연속 청산 경매에 대한 할당분은 연속 청산 경매 세일 할당분에 따로 제시되어 있습니다.

- **팀 및 어드바이저**

팀 및 어드바이저 할당분은 핵심 팀과 인터폴드의 초기 개발을 지원해준 어드바이저에게 제공되며 24개월에 걸쳐 베스팅됩니다.

언락³¹ 일정



[FOLD 언락 일정]

³¹ Unlock

로드맵

인터폴드는 별도 로드맵을 공지하고 있지 않으나, 공식 블로그 및 X(구 트위터)를 통해 사업 현황에 대한 공지를 상시로 진행하고 있습니다.

- 블로그 : <https://blog.theinterfold.com/>
- X(구 트위터) : <https://x.com/theInterfold>

*상기 링크는 작성일 기준으로 유효한 링크이며 변경될 가능성이 있습니다.