쓰레스홀드(T)

주요내용설명서(국문백서)

Korean White Paper

2026년 6월 4일

Disclaimer

본 번역본은 2026년 6월 4일 기준의 쓰레스홀드(Threshold) Docs 페이지 내 관련 내용 위주로 번역됐습니다.

빗썸은 발행주체 또는 운영주체가 제공하는 가상자산의 총 발행량, 유통량 계획, 사업계획 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.

빗썸

프로젝트 소개

탈중앙화 앱이 디지털 표준이 되면서, 웹3 플랫폼은 퍼블릭 블록체인에서 상호작용할 때 사용자의 개인정보와 주권을 보장해야 하는 과제에 점점 더 직면하게 될 것입니다.

쓰레스홀드 네트워크는 완전한 탈중앙화 임계값 암호화 서비스를 제공함으로써 이러한 문제를 해결합니다. 임계값 암호화는 데이터를 보호하기 위해 독립적인 노드 네트워크에 작업을 분산시키는 방식입니다. 이 간단한 아이디어는 보안과 가용성을 높이고, 신뢰할 수 있는 당사자에 대한 의존도를 낮춥니다.

쓰레스홀드와 T를 통해 토큰 보유자는 탈중앙화된 노드를 스테이킹하고 운영함으로써 임계값 암호화 서비스를 위한 원스톱 플랫폼을 구축할 수 있습니다. 노드 운영자는 중앙 권한 없이도 이러한 서비스를 제공할 수 있도록 암호경제적 인센티브를 받습니다.

쓰레스홀드 네트워크의 핵심 서비스에는 비트코인 자산 브리지인 tBTC와 접근 제어 플러그인인 TACo가 있습니다. 전통적으로 서명, 무작위성 생성, 접근 제어와 같은 중요한 작업에는 단일 기관에 대한 신뢰를 요구합니다.

하지만 쓰레스홀드 네트워크에서는 이러한 기능이 탈중앙화되고 신뢰가 최소화되어 강력한 보안과 무결성을 보장합니다. 블록체인 혁명이 계속됨에 따라, 커뮤니티가 주도하는 쓰레스홀드 네트워크는 프라이버시 중심의 자기 주권적인 탈중앙화된 미래를 위한 다양한 암호화 도구를 제공할 것입니다.

쓰레스홀드 네트워크와 함께 탈중앙화된 보안의 미래가 다가오고 있습니다.

비즈니스 모델

tBTC 비트코인 브릿지

기존의 비트코인(BTC)을 이더리움(ETH)으로 브릿지하는 솔루션은 사용자가 비트코인을 중개자에게 전송하고, 그 대가로 원래 자산을 대표하는 ERC-20 토큰을 받는 방식입니다. 이러한 중앙 집중식 모델은 제3자에 대한 신뢰를 요구하며 검열에 취약해, 비트코인이 가진 주권적이고 안전하며 허가가 필요 없는 디지털 자산이라는 전제를 위협합니다.
2세대 tBTC는 비트코인과 이더리움 사이의 진정한 탈중앙화(그리고 확장 가능한) 브릿지 역할을 합니다. 이는 비트코인 보유자에게 더 광범위한 디파이 생태계에 대한 안전하고 개방적인 접근을 제공합니다. tBTC v2를 통해 비트코인의 가치를 활용해 대출과 대여, 스테이블코인 발행, 유동성 공급 등 다양한 활동을 할 수 있습니다.

중앙화된 중개자 대신, tBTC는 쓰레스홀드 네트워크에서 노드를 운영하는 무작위로 선택된 운영자 그룹을 사용하여 임계값 암호화를 통해 예치된 비트코인을 보호합니다. 즉, tBTC는 운영자가 비트코인으로 어떤 작업을 수행하기 전에 임계값 과반수 동의가 필요합니다. 매주 운영자를 교체함으로써 tBTC는 개인 또는 운영자 그룹이 기본 예치금을 사기적으로 압류하기 위해 공모하는 것을 방지합니다. 정직한 다수 가정에 의존하여, 정직하지 않은 운영자들의 정족수로 지갑이 있을 가능성을 계산할 수 있습니다.

시중의 다른 솔루션과 달리, tBTC 사용자는 하드웨어나 사람이 아닌 수학을 신뢰합니다.

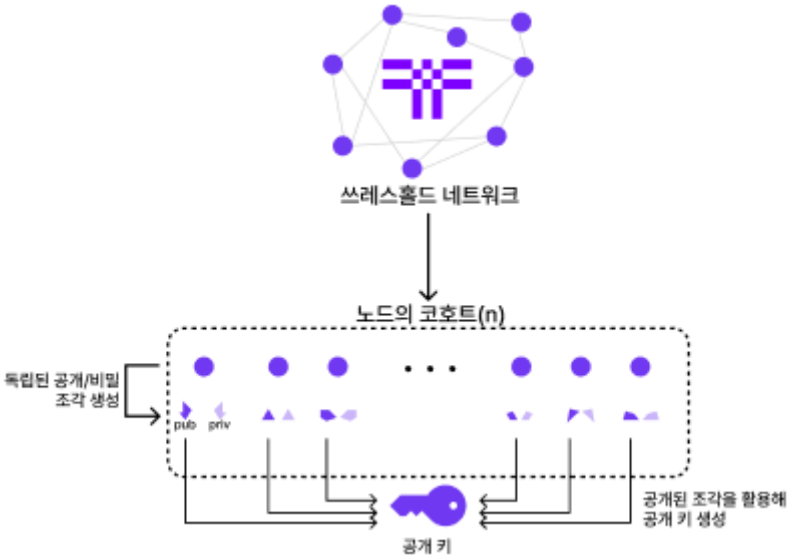
TACo - 쓰레스홀드 접근 제어

TACo(쓰레스홀드 접근 제어)는 엔드투엔드 암호화된 데이터 공유 및 통신을 가능하게 합니다. 중앙 집중식 권한이나 기관에 대한 신뢰가 필요 없으며, 이들이 일방적으로 서비스를 거부하거나 심지어 (은밀하게) 개인 사용자 데이터를 암호 해독할 위험이 없습니다.

현재 TACo는 웹3 개발자들이 사용할 수 있는 유일한 접근 제어 레이어로, 개발 단계부터 탈중앙화되어 있으며, 잘 담보되고 실전에서 테스트를 거친 쓰레스홀드 네트워크를 통해 제공됩니다. 즉, TACo 메인넷 DKG 공개 키를 사용해 암호화된 모든 데이터에 대한 접근은 첫번째 바이트부터 분산된 시스템에서 관리된다는 것을 의미합니다.

임계값 복호화

TACo는 내부적으로 공동 비밀(복호화 키)을 여러 개의 조각으로 분할하고 이를 승인된 담보 노드 운영자(쓰레스홀드 네트워크의 스테이커)에게 분배하는 과정을 포함합니다. 키 조각을 보유한 운영자 중 최소한의 수, 즉 임계값이 온라인 상태여야 하며 부분 복호화에 적극적으로 참여해야 합니다. 이후 요청자의 클라이언트에서 이를 결합하여 원본 평문 데이터를 재구성합니다.



[임계값 복호화 과정]

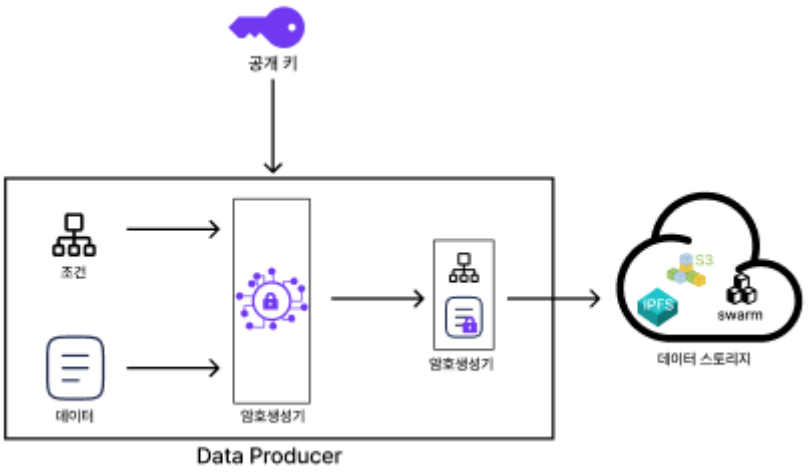
조건 제한

조건은 암호 텍스트 단위로 '첨부'됩니다. 즉, 모든 페이로드, 메시지 또는 비트는 지정된 고유 조건 세트에 의해 접근이 제한될 수 있습니다. 대부분의 경우, 조건 세트는 최종 사용자가 적극적으로 구성할 때까지 자동으로 재사용됩니다. 예를 들어, 그룹 채팅에서 메시지에 계속 접근하지 못하도록 주소를 제거하려는 경우가 이에 해당합니다.

데이터 소유자는 다양한 접근 조건 유형을 정의할 수 있습니다. 예를 들면 다음과 같습니다:

- EVM 기반
    - 예: 요청자가 특정 NFT를 소유하고 있나요?
- RPC 기반
    - 예: 요청자가 지갑에 지정된 토큰을 최소 X개 이상 보유하고 있는가?
- 시간 기반
    - 예: 미리 정의된 기간이 경과했는가, 그 이후에는 요청이 무시되는가?

이러한 조건들은 또한 조합 가능하며, 어떤 논리적 순서나 의사 결정 트리로도 결합할 수 있습니다.



[조건 제한 과정]

조건 충족 검증

대부분의 사용 사례에서, 요청자는 특정 조건 충족에 대한 자신과의 연관성 - 즉, 일정 수의 복호화 조각을 받을 권리 - 을 증명하기 위해 거래에 서명하여 이더리움 지갑 소유권을 확인합니다. 이 지갑은 특정 조건의 충족 여부 - 예를 들어, DAO의 지식 기반에 접근하기 위해 NFT를 소유하고 있는지 - 를 확인합니다.

이 서명은 사용자가 나중에 접근을 위해 반복적으로 다시 서명할 필요가 없도록, 애플리케이션에 의해 적절한 기간 동안 캐시될 수 있습니다. 그러나 검증은 여전히 백그라운드에서 이루어지며, 예를 들어 NFT를 통해 접근이 허용된 그룹 채팅에서 지갑 주소가 제거되면, 해당 사용자는 새로운 메시지를 즉시 볼 수 없게 됩니다. 캐시된 서명은 데이터 소유자/암호화기가 지정한 것보다 더 길게 접근 권한을 부여하지 않습니다.

네트워크 매개변수화

향후 버전에서는 개발자가 특정 네트워크 수준 매개변수를 조정할 수 있는 옵션이 제공되며, 이는 TACo의 공모 저항, 중복성, 지연 시간 및 사용 비용에 영향을 미칩니다. 이러한 매개변수는 주로 주요 자료 관리 및 조건 검증을 담당하는 각 노드 집단과 관련이 있습니다:

- 복호화 조각의 수 n, 즉, 집단의 크기
- 집단 구성원 교체 빈도 및/또는 비즈니스 로직
- 항상 집단에 포함될 '직접 선택된' 노드 주소
- 집단 구성원을 선택하기 위한 샘플링 메커니즘

이 선택권은 최종 사용자에게도 제공될 수 있습니다. 예를 들어, 네트워크 수준에서 매개변수를 결합한 '패키지' 형태로 제공될 수 있습니다. 최종 사용자는 신뢰, 위험 및 비용 선호에 따라 몇 가지 구체적인 옵션 중에서 선택할 수 있습니다.

Threshold USD

쓰레스홀드 USD(thUSD)는 USD에 소프트 페깅된 스테이블코인으로, 최소 담보 비율은 110%이며 ETH와 tBTC를 담보로 합니다.

BTC 또는 ETH를 담보로 사용할 경우, 매우 낮은 비용으로 thUSD를 대출할 수 있습니다.

쓰레스홀드 USD는 리퀴티 프로토콜의 수정된 포크로, PCV("프로토콜 통제 가치")를 통해 자립적으로 운영되도록 설계되었습니다. 쓰레스홀드 USD에는 LQTY 토큰에 상응하는 토큰이 없습니다. 대신 모든 수익은 PCV에 축적됩니다. 토큰이 없기 때문에 부트스트래핑은 초기 프로토콜 대출을 통해 완료됩니다.

프로토콜이 자체 유동성("PCV")을 소유한 결과, 더 예측 가능한 경로와 장기적인 지속 가능성을 확보할 수 있습니다. 안정성 풀은 사용자 예치금이 아닌 PCV에 의해 자금이 조달됩니다. 덕분에 수동적인 LQTY 스테이커(유동성 임대)에 대한 보상으로 자금이 낭비되지 않으며, 대신 해당 자금을 안정성 풀에 재투입할 수 있습니다. 프로토콜이 성장하고 수수료가 발생함에 따라 안정성 풀은 지속적으로 충전될 것입니다.

다중 담보

리퀴티는 이더리움만을 담보로 사용할 수 있습니다. 쓰레스홀드 USD는 탈중앙화된 BTC 래퍼 tBTC를 통해 BTC를 담보로 지원하여 대출할 수 있도록 확장되었습니다. 향후에는 충분히 탈중앙화되어 있다면 다른 유형의 담보가 고려될 수 있습니다.

각 담보물은 자체 컨트랙트와 함께 배포되며, 새로운 담보는 배포되기 전에 긴 시간 지연을 두고 DAO 투표가 필요합니다. 각 담보를 자체 컨트랙트로 만들면, 특정 컨트랙트에 대한 발행을 허용하지 않음으로써 담보를 쉽게 폐기할 수 있습니다.

토크노믹스

T는 쓰레스홀드 네트워크를 위한 ERC-20 작업 토큰으로, 여러 가지 기능을 수행합니다. 이는 네트워크의 지분 증명 토큰으로, 쓰레스홀드 네트워크를 보호하는 데 도움이 되며, 커뮤니티가 네트워크에 대한 집단적 결정을 내릴 수 있도록 하는 쓰레스홀드 DAO의 거버넌스 토큰이기도 합니다.

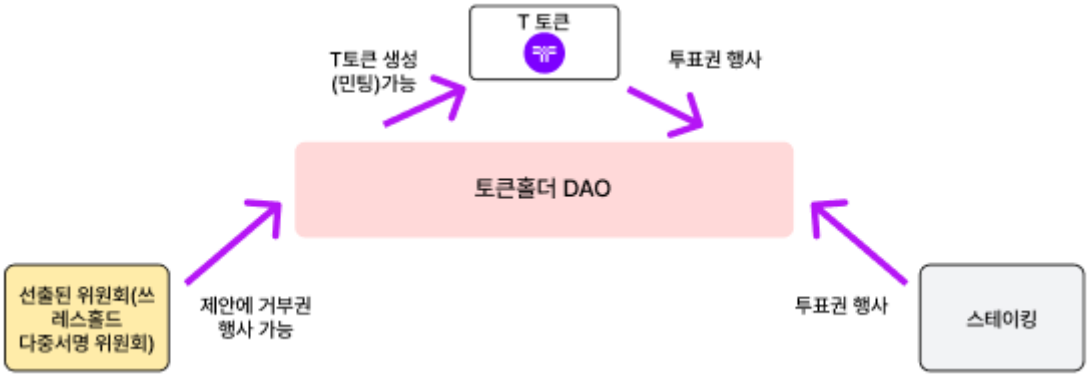
T의 초기 공급량은 DAO에 의해 런칭 시 100억 T로 설정되었으며, 다음과 같은 분배가 이루어졌습니다:

- 45억 T는 NU 토큰 보유자에게 분배
- 45억 T는 KEEP 토큰 보유자에게 분배
- 10억 T는 쓰레스홀드 DAO 트레저리에 분배

추가로 네트워크의 인플레이션 기반 부트스트래핑 단계에서 스테이커와 노드 운영자에 대한 인센티브로 11억 5,500만 개의 토큰이 발행되었으며, 그 결과 최종 총 공급량은 111억 5,500만 개의 T 토큰이 되었습니다.

쓰레스홀드 DAO

쓰레스홀드는 커뮤니티가 주도하며, 누사이퍼(NuCypher)와 킵 네트워크(Keep Network)의 구성원을 모두 포함하는 동명의 DAO에 의해 운영됩니다. 쓰레스홀드 DAO에는 토큰홀더 DAO와 선출된 위원회라는 두 개의 주요 기관이 있습니다. 이 이중 구조의 목표는 대표성을 강화하면서도 책임성을 보장하는 것입니다. 이들 각각의 거버넌스 기관은 서로를 책임지며, 이는 대부분의 헌법 정부에서 볼 수 있는 견제와 균형 시스템과 유사합니다. 또한, 이들은 거버넌스 구조에 내재된 별도의 책임을 지고 있습니다.



[쓰레스홀드 DAO 구조]

구현 관점에서 토큰홀더 DAO는 거버너 브라보(Governor Bravo) 거버넌스 모델(특히 오픈제플린 거버넌스 사용)을 기반으로 합니다. 토큰홀더 DAO는 이더리움 메인넷의 0xd101f2B25bCBF992BdF55dB67c104FE7646F5447에 있습니다. 선출된 위원회는 노시스 세이프 컨트랙트로 구현되며, 6-of-9 구성으로 이더리움 메인넷의 0x9F6e831c8F8939DC0C830C6e492e7cEf4f9C2F5f에 배포되어 있습니다.

로드맵

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

- 홈페이지 https://threshold.network/
- 블로그 https://www.threshold.network/blog
- X(구 트위터) https://x.com/thetnetwork

*상기 링크는 작성일 기준으로 유효한 링크이며 변경될 가능성이 있습니다.