

쓰레스홀드(Threshold)

해당 번역본은 이용자가 디지털자산 관련 정보를 편리하게 확인할 수 있도록 단순 참고용으로 번역된 것이며, 투자 권유를 목적으로 하지 않습니다.
그 내용이 정확하지 않을 수 있으므로 정확한 정보 습득을 위해서는 원문을 참고하시거나 원문 작성 주체 측에 문의하시기 바랍니다.
두나무는 해당 번역본 내용의 진실성 및 정확성을 보장하지 않고, 제공된 정보에 의한 투자 결과에 대하여 어떠한 책임도 지지 않으며, 투자 손실은 투자자에게 귀속됩니다.

Threshold Network란 무엇인가?

Threshold Network는 DeFi를 위한 비트코인 표준인 tBTC를 구동한다. 이는 신뢰를 최소화한 방식으로 비트코인 유동성을 크립토 생태계로 가져오면서, 언제나 원본 비트코인으로 직접 결제(settlement)할 수 있는 경로를 유지한다.

다른 비트코인 파생상품이나 래핑된 토큰과 달리, tBTC는 비트코인에 최대한 가깝게 설계되었으며 DeFi에 원활히 참여할 수 있도록 한다. 복잡한 스테이킹 메커니즘도 없고, 단일 주체에 대한 의존도 없다 — 언제나 비트코인으로 결제되는 순수한 BTC 유동성만 존재한다.

Threshold Network의 T 토큰은 tBTC를 구동하며, 브리지 수수료를 통한 토큰 바이백(token buyback)을 통해 발생한 수익을 분배하는 가치 축적 자산이다.

기본 원리: 더 깊이 알아보기

Threshold Network의 기본 개념을 이해하면 주요 기능을 더 깊이 있게 파악할 수 있다.

tBTC 발행(Minting) 안내

이 가이드를 따라 비트코인을 활용하여 tBTC를 발행해보자.

시작하기 전에

tBTC 발행 프로세스를 시작하기 전 필요한 것들은 다음과 같다:

- ✓ 비트코인 (BTC)
- ✓ 이더리움 (ETH) — 이더리움 트랜잭션 가스비용용
- ✓ 비트코인 호환 지갑
- ✓ 이더리움 호환 지갑

비트코인 지갑이 아직 없다면, 새로 설정해야 한다. 추천할 만한 지갑으로는 Green Wallet이 있다. 다운로드를 아래 링크에서 가능하다:

- Apple Store 다운로드
- Google Store 다운로드

지갑을 생성한 후, 네트워크로 비트코인을 선택하라.

tBTC 발행 시작하기

 준비 완료! 이제 다음 링크에서 tBTC dApp으로 이동하라: <https://dashboard.threshold.network/tBTC/mint>

용어가 생소하다면, dApp 내 **How it Works** 페이지로 이동하여 더 알아볼 수 있다. 또한 문서에서 지갑 생성 및 브리지 퍼미션 리스 관련 문서도 참고할 수 있다.

STEP 1: 예치 주소 생성

1. 선호하는 이더리움 지갑을 tBTC dApp에 연결한다. **Connect Wallet**을 클릭한다.
2. 왼쪽 탐색창에서 tBTC 아이콘으로 표시된 **tBTC Bridge** 페이지로 이동한다.
3. 비트코인 지갑 주소를 **BTC 복구 주소(BTC Recovery Address)**로 입력하고 **Generate Deposit Address**를 클릭하여 고유한 예치 주소를 생성한다.
4. **Download**를 클릭하여 JSON 파일을 반드시 다운로드하라. JSON 파일에는 지갑 공개키, 환불 공개키, 환불 잠금 시간이 포함되어 있다. tBTC 토큰을 받을 때까지 이 파일을 안전하게 보관해야 한다.

STEP 2: BTC 예치

1. 비트코인 지갑에서 tBTC dApp에 표시된 예치 주소의 QR코드를 스캔한다. 예시는 다음과 같다:
2. 비트코인 지갑에서 해당 예치 주소로 BTC를 송금한다. 최소 예치 금액은 0.01 BTC이다.
3. tBTC dApp으로 돌아가면, 송금이 완료된 후 자동으로 Step 3으로 진행된다.

STEP 3: 발행 시작

1. **Confirm deposit & mint**를 클릭하여 발행 절차를 시작한다.
2. 이더리움 지갑에서 트랜잭션에 서명한다.

STEP 4: tBTC 발행

1. 이제 발행이 진행 중이다! tBTC가 발행될 때까지 dApp에 머물 필요는 없다. dApp에서 발행 진행 상태를 확인할 수 있다. 첫 단계는 비트코인 네트워크에서 1건의 컨펌이 발생한 후 다음 단계로 넘어간다.
2. 민팅 초기화를 평가하는 민터(Minter)를 기다리는 동안 다음 화면이 표시된다.

3. 이후, 가디언(Guardian)이 발행 요청을 검증하는 동안 다음 화면이 표시된다.
4. 성공! 이 화면에서 모든 트랜잭션 링크를 확인할 수 있다.
5. **token address**를 클릭하여 tBTC 토큰 주소를 이더리움 지갑에 추가하라.

축하합니다 — 발행 완료!

🎉 성공적으로 tBTC를 발행했습니다! 🎉

tBTC 비트코인 브리지

DeFi를 향한 탈중앙화-퍼미션리스 비트코인 브리지

비트코인을 이더리움으로 브리지하는 기존 솔루션들은 사용자가 원자산을 대표하는 ERC-20 토큰과 교환하는 대가로 비트코인을 중개자에게 보내도록 요구한다. 이 중앙화된 모델은 제3자를 신뢰해야 하며 검열에 취약하므로, 비트코인을 주권적이고 안전하며 퍼미션리스한 디지털 자산으로 보는 전제를 위협한다.

tBTC의 두 번째 세대는 비트코인과 이더리움 사이의 진정한 탈중앙화(그리고 확장 가능한) 브리지다. 이는 비트코인 보유자에게 더 넓은 DeFi 생태계로의 안전하고 개방된 접근을 제공한다. tBTC v2를 사용하면 대출-차입, 스테이블코인 발행, 유동성 공급 등 다양한 방식으로 비트코인의 가치를 잠금 해제할 수 있다.

정직한 다수 가정(Honest Majority Assumption)

중앙화된 중개자 대신, tBTC는 Threshold Network에서 노드를 구동하는 무작위 선정된 오퍼레이터 그룹을 사용하여 임계값 암호(Threshold cryptography)를 통해 예치된 비트코인을 보호한다. 이는 오퍼레이터가 사용자의 비트코인으로 어떠한 행동을 수행하기 전에 임계 다수 합의를 요구함을 의미한다. 오퍼레이터 선정을 주간으로 로테이션함으로써, tBTC는 특정 개인이나 오퍼레이터 집단이 결탁하여 기초 예치를 부정하게 탈취하는 것을 방지한다. 정직한 다수 가정에 의존함으로써, 우리는 부정직한 오퍼레이터 정족수(quorum)로 구성된 지갑의 발생 가능성을 계산할 수 있다(확률 계산에 대한 보다 심층적인 논의는 여기 참조).

시중의 다른 솔루션들과 달리, tBTC 사용자는 하드웨어나 사람을 신뢰하지 않고 수학을 신뢰한다.

수수료

tBTC 수수료는 행위 기반이다(즉, 브리지를 사용할 때 민팅 및 상환 수수료가 발생한다). 현재 민팅 수수료는 0%이며 상환 수수료는 0.2%다. 브리지 수수료는 거버넌스를 통해 변경될 수 있다.

지갑 생성

지갑은 거버넌스에 따라 주기적으로 생성된다. `updateWalletParameters`는 지갑 간 시간 간격을 변경하며, `walletParameters`는 이를 읽는다. 새 지갑 사이의 시간은 초 단위의 `walletCreationPeriod`에 저장되며, 현재 값인 1209600은 14일을 의미한다.

지갑이 자금을 이동하려면, 임계 타원곡선 디지털 서명 알고리즘(Threshold Elliptic Curve Digital Signature Algorithm)을 사용하여 서명을 생성해야 하며, 100명 서명자 중 51명의 협력이 필요하다.

각 지갑의 100명 서명자는 Sortition Pool을 통해 선택되며, 무작위성은 Random Beacon이 제공한다.

스테이커가 서명자로 선택될 확률은 전체 TBTC 스테이크에서 자신의 비중과 같다. 각 서명자는 독립적으로 선택된다. 동일한 스테이커가 같은 지갑에서 여러 번 서명자가 될 수 있다. 동일한 스테이커가 여러 지갑에서 동시에 서명자가 될 수 있다.

예시

단순화를 위해 스테이커가 앨리스, 밥, 캐럴 세 명뿐이라고 가정하자. 앨리스는 2.5억 T, 밥은 4억 T, 캐럴은 3.5억 T를 스테이킹 했으므로, 각자의 지분은 각각 25%, 40%, 35%다. 이는 앨리스가 서명자가 될 확률이 25%, 밥은 40%, 캐럴은 35%임을 의미한다. 각 서명자는 독립적으로 선택된다.

Sortition Pool은(강력한 가스 최적화 때문에) 더 복잡하지만, 이를 이해하는 방식은 다음과 같을 수 있다:

각 서명자에 대해 1부터 100까지의 무작위 수를 생성한다. 수가 [1, 25]에 속하면 앨리스가 서명자다. 수가 [26, 65]에 속하면 밥이 서명자다. 수가 [66, 100]에 속하면 캐럴이 서명자다. 예를 들어, 첫 번째 무작위 수가 33이라면 첫 번째 서명자는 밥이 된다. 100개의 무작위 수 (75, 51, 13, 48, 36, 62, 46, 65, 97, 67...)를 생성하고, 이를 사용해 서명자를 결정할 수 있다: (캐럴, 밥, 앨리스, 밥, 밥, 밥, 밥, 캐럴, 캐럴...).

이 예시는 앞서 언급한 몇 가지 성질을 보여준다:

- 각 서명자는 독립적으로 선택된다. 캐럴이 첫 번째 서명자인지 여부는 캐럴이 두 번째 서명자가 되는지에 아무런 영향을 주지 않는다.
- 특정 서명자가 될 확률은 자신의 스테이크 점유율과 같다.

통계

캐럴이 특정 서명자가 될 확률이 35%라면, 캐럴이 100석 중 최소 51석을 차지하여(혼자서 지갑을 통제할 수 있게 될) 확률은 어느 정도인가?

캐럴이 한 지갑에서 통제하는 서명자 수는 이항 분포로 모델링된다. 위키피디아에 따르면:

매개변수 n 과 p 를 가진 이항 분포는 n 번의 독립 실험에서 성공 횟수에 대한 이산 확률분포이며, 각 실험은 예/아니오 질문을 던지고 불리언 값의 결과를 갖는다. 성공(확률 p) 또는 실패(확률 $1-p$).

이는 정확히 우리의 상황이다! 캐럴의 관점에서 보면, $n=100$ 번의 독립 실험이 있으며, 각 실험은 예/아니오 질문(이 서명자가 캐럴에 속하는가)을 던지고, 각 실험의 성공 확률은 35%다.

따라서 우리는 이항 확률 계산기를 사용하여 질문에 답할 수 있다:

관련 있는 값은 마지막 항목인 “Cumulative probability: $P(X>51)$ ”이다. 이는 캐럴이 특정 지갑에서 지배적 지분을 가질 확률이 약 0.074%임을 의미한다.

다음으로 중요한 질문은 “캐럴이 한 지갑을 통제할 확률은 낮지만, 한 번만 발생해도 문제가 된다. 앞으로 2년 동안 캐럴이 어느 지갑이든 통제할 확률은 얼마인가?”이다.

지갑은 14일마다 하나씩 생성되므로, 향후 2년 동안 시스템은 약 52개의 지갑을 생성한다. 각 지갑이 캐럴에게 통제되지 않을 확률은 $1 - 0.00074 = .99926$, 즉 99.926%다. 따라서 제곱 반복을 적용할 수 있다:

$$0.99926^{52} = 0.9622$$

캐럴이 2년 내에 어느 한 지갑을 통제할 확률은 약 3.8%다. 이는 캐럴이 전체 스테이크의 35%를 보유하는 상황에서의 결과다! 앨리스의 경우 확률은 훨씬 낮다. 그녀가 한 지갑을 통제할 확률은 0.0002131%이며, 52개의 지갑을 기준으로 2년 동안 어느 지갑이든 통제할 확률은 0.02131%다.

작성 시점 기준, 가장 큰 스테이커는 전체 스테이크의 약 8.83%를 보유한다.

시빌 저항(Sybil Resistance)

스테이커가 자신의 스테이크를 여러 정체성으로 분할함으로써 달성하는 유일한 일은 시스템이 더 다양해 보이게 만든다는 점뿐이다.

예를 들어, 앨리스가 자신의 스테이크를 동일하게 5개의 계정으로 나눴다고 하자: Alice1, Alice2, Alice3, Alice4, Alice5. 이제 앨리스가 서명자가 될 확률이 25%인 대신, 각 계정은 5%의 확률을 가지며, 합산하면 25%가 된다.

앞선 예시를 사용하면, 앨리스는 2.5억 T, 밥은 4억 T, 캐럴은 3.5억 T를 스테이킹했다. 앨리스는 각 정체성에 5천만 T씩 나눴다. Alice1은 $50M/1000M = 5\%$ 를 보유한다.

정체성에 1부터 100까지의 숫자를 할당하는 단순화를 유지하면, Alice1은 [1, 5], Alice2는 [6, 10], Alice3는 [11, 15], Alice4는 [16, 20], Alice5는 [21, 25], 밥은 [26, 65], 캐럴은 [66, 100]을 갖는다. 이전과 동일한 무작위 수 (75, 51, 13, 48, 36, 62, 46, 65, 97, 67...)를 사용하면, 할당은 (캐럴, 밥, Alice3, 밥, 밥, 밥, 밥, 캐럴, 캐럴...)이 된다. 실질적으로 달라진 것은 없다!

지갑 서명

지갑의 주요 책임은 tBTC 사용자가 예치한 비트코인을 관리하는 것이다. 프로토콜 동작(예: 예치 스왑 또는 상환)으로 인해 지갑이 일부 비트코인을 이동해야 할 때마다, 적절한 비트코인 트랜잭션을 구성하고 tECDSA 서명 알고리즘을 사용하여 각 트랜잭션 입력에 서명해야 한다. tECDSA 서명 동안, 무작위로 선택된 100명 중 51명의 지갑 서명자가 협력하여 올바른 서명을 생성해야 한다.

서명 시도의 구조

단일 tECDSA 서명 시도는 여러 단계로 구성된다. 각 단계는 호스트 체인(예: 이더리움) 블록 수로 표현되는 최대 지속 시간을 갖는다:

1. 서명자 준비 상태 알림 단계로, 정확히 6블록이 소요된다
2. 서명 생성 및 광고 단계로, 최대 30블록이 소요된다
3. 쿨다운 기간으로, 정확히 5블록이 소요된다

즉, 단일 서명 시도는 최대 41블록이 소요될 수 있다(이더리움의 평균 블록 시간을 12초로 가정하면 약 8분). 해당 시간 내에 서명이 생성되지 않으면, 지갑 서명자들은 해당 시도를 포기하고 재시도한다.

서명 재시도

주어진 메시지(예: 비트코인 트랜잭션 입력)에 대한 서명을 요청받은 지갑은 단일 tECDSA 서명 시도에만 국한되지 않는다. 서명 알고리즘의 분산 특성 때문에, 단일 서명 시도는 서명자 간 통신에 영향을 미치는 예기치 않은 네트워크 문제 등으로 실패할 수 있다. 첫 시도가 실패하면, 무작위로 새로 선택된 51명의 지갑 서명자 집합이 다음 시도에서 서명을 재시도한다. 이후 서명 시도는 첫 시도가 시작된 블록과 단일 시도의 알려진 최대 지속 시간(41블록)을 기준으로 고정 간격으로 예약된다. 예를 들어, 첫 시도가 블록 B에서 시작되었다면, 이후 시도는 다음과 같이 예약된다:

- 시도 2 -> B + 41
- 시도 3 -> B + 82
- 시도 N -> B + (N-1) * 41

지갑은 항상 최대 5번의 서명 시도를 수행한다. 이러한 최대 시도 횟수는 합리적인 서명 타임아웃과 오작동하는 지갑 서명자에 대한 충분한 내성을 균형 있게 달성하기 위한 수용 가능한 트레이드오프다. 5번의 서명 시도를 수행하면 서로 다른 51명 서명자 부분집합을 5번 시도할 수 있다. 이는 가능성은 낮지만 2명의 서명자가 오작동하는 경우에도 서명을 생성하기에 충분하다. 이 경우, 98명의 정직한 서명자 중에서 51명을 선택해야 한다. 이는 성공적인 부분집합을 선택할 확률이 다음과 같음을 의미한다:

$$P = (98\text{choose}51)/(100\text{choose}51) = 0.24$$

이는 최악의 경우 5회의 선택이 필요함을 의미한다.

단일 시도당 최대 41블록과 최대 5회의 서명 시도를 결합하면, 지갑은 주어진 메시지에 대해 $5 * 41 = 205$ 블록 동안 서명을 시도하게 된다(이더리움의 평균 블록 시간을 12초로 가정하면 약 40분). 그 시간 동안 서명이 생성되지 않으면, 지갑 서명자들은 최종적으로 포기한다.

직렬 서명(Serial signing)

지갑은 여러 메시지(예: 단일 비트코인 트랜잭션의 여러 입력)를 직렬 방식으로, 즉 한 메시지씩 순차적으로 서명할 수 있다. 이러한 경우, 배치에 포함된 모든 메시지가 서명을 획득해야만 전체 서명 프로세스가 성공한 것으로 간주된다.

앞 절에서 언급했듯이, 단일 메시지에 대한 서명의 최대 허용 시간은 205블록(이더리움 기준 약 40분)이다. 이는 N개의 메시지 배치를 서명하는 데 필요한 최대 시간이 $N * 205$ 블록임을 의미한다. 그동안 서명은 계산적으로 무거우므로 지갑은 다른 작업을 수행할 수 없다. 이 요소는 서명을 활용하는 지갑 액션을 설계할 때 반드시 고려해야 한다.

지갑 액션의 기반으로서의 서명

tBTC 프로토콜은 유한한 집합의 지갑 액션을 정의한다:

- Heartbeat
- Deposit sweep
- Redemption
- Moving funds
- Moved funds sweep

각 액션은 내부적으로 지갑 서명을 수반한다. 특정 액션을 완료하는 데 필요한 시간은 실행 중에 생성해야 하는 서명 수에 따라 달라진다. 단일 서명을 생성하는 데 필요한 최악의 시간(205블록)과 주어진 액션이 요구할 수 있는 서명 수를 알고 있으면, 특정 액션에 적절한 시간 경계를 설정할 수 있다. 이 정보는 적절한 지갑 조정을 위해 매우 중요하다.

예시: Deposit sweep

서명이 지갑 액션에 어떤 영향을 미치는지 보여주기 위해 Deposit sweep 액션을 사용하자. 이 액션은 WalletCoordinator 체인 컨트랙트를 통해 deposit sweep 제안을 제출하는 코디네이터에 의해 시작된다. 이 액션의 기대 결과는 여러 입력(스왑된 예치금)과 하나의 출력으로 구성된 비트코인 트랜잭션이며, 비트코인 체인에 제출된다. 이는 해당 액션의 실행 시간이 주어진 스왑 제안에 포함된 예치금 수에 강하게 좌우됨을 의미한다. WalletCoordinator 컨트랙트에는 Deposit sweep 액션에 영향을 미치는 일부 거버넌스 가능한 파라미터가 있다:

- 단일 스왑 제안에 포함될 수 있는 최대 예치금 수를 설정하는 depositSweepMaxSize
- 제안의 유효 시간을 결정하는 depositSweepProposalValidity. 이는 지갑이 해당 스왑을 실행하기 위해 확보하는 배타적 시간이며, 그동안 다른 액션은 수행될 수 없다

다시 말해, 지갑은 최대 depositSweepMaxSize 개의 예치금을 스왑할 수 있으며 이를 수행할 시간으로 depositSweepProposalValidity를 갖는다.

서명은 Deposit sweep 액션에서 가장 중요하고 복잡한 단계이며, 레퍼런스 클라이언트 구현은 스윙 트랜잭션의 모든 입력에 대해 서명 타임아웃을 depositSweepProposalValidity - 1 hour로 설정한다. 단일 예치 입력에 대한 서명을 생성하는 데는 최대 205블록(내부적으로 5회의 시도)이 소요될 수 있다. 이는 이더리움의 평균 블록 시간을 12초로 가정할 때 약 40분이다. 이를 염두에 두면, 앞서 언급한 WalletCoordinator의 거버넌스 가능한 파라미터는 서명 실행에 큰 영향을 미치므로 신중하게 선택해야 한다:

- depositSweepMaxSize = 5 그리고 depositSweepProposalValidity = 4 hours인 경우, 지갑은 3 시간 동안 5개의 입력에 서명을 시도하게 되며, 입력당 약 36분이 주어진다. 5회의 서명 시도에는 약 40분이 필요하므로, 이 구성에서는 입력당 4회의 시도가 가능하다
- depositSweepMaxSize = 10 그리고 depositSweepProposalValidity = 4 hours인 경우, 지갑은 3 시간 동안 10개의 입력에 서명을 시도하게 되며, 입력당 약 18분이 주어진다. 5회의 서명 시도에는 약 40분이 필요하므로, 이 구성에서는 입력당 2회의 시도가 가능하다
- depositSweepMaxSize = 20 그리고 depositSweepProposalValidity = 4 hours인 경우, 지갑은 3 시간 동안 20개의 입력에 서명을 시도하게 되며, 입력당 약 9분이 주어진다. 5회의 서명 시도에는 약 40분이 필요하므로, 이 구성에서는 입력당 1회의 시도가 가능하다

퍼미션리스로 가는 길(The Path to Permissionlessness)

이 시스템은 처음부터 완전히 퍼미션리스가 되도록 설계되었으며 — 최소한의 T 스테이크를 보유한 누구나 노드를 운영하고 커스터디언이 될 비례적 기회를 가질 수 있도록 했다.

제품을 효과적으로 출시하기 위해, 우리는 퍼미션드된 서명자 집합과 더불어 퍼미션드된 가디언 및 민터 집합과 함께 런칭했다. 이 문서는 이러한 변경의 배경 아이디어와 향후 우리가 취하고 있는 조치에 대해 설명한다.

TL;DR

- tBTC는 현재 정직한 다수 가정하에서 운영되는 퍼미션드 서명자 집합(일명 Beta Stakers)을 사용한다.
- 퍼미션드 정직한 다수 서명자 집합은 BitVM2(또는 동등한 설계)를 사용하여 커스터디가 1-of-N 신뢰 가정으로 업그레이드될 때까지 유지될 것이다.

퍼미션리스 커스터디(Permissionless Custodianship)

지갑의 100명 서명자를 선택하기 위해, tBTC는 퍼미션드 목록에 있는 Beta Stakers 중에서 선택한다. 이러한 결정은 여러 이유에 기반한다:

1. 시스템의 초기 단계인 테스트넷 및 카오스넷 단계에서는 서명자가 변경 사항 테스트를 돕고 치명적 버그에 신속히 대응할 수 있도록 보장하는 것이 중요하다. 개발 팀이 알고 있는 개인들에게 직접 접근할 수 있는 것은 이 맥락에서 결정적이다.
2. 기반 서명 알고리즘인 GG18은 오작동 서명자를 식별할 수 없다.

GG18에 관한 이 지점은 매우 중요하다. 오작동 서명자를 식별할 수 없다면, 소수이지만 정교하고 악의적인 집단이 비트코인 트랜잭션에 적시에 서명하는 것을 어렵게 만들 수 있다. 만약 오작동 서명자를 식별할 수 있다면, 우리는 그들을 서명 프로세스에서 직접 제외할 수 있을 것이다.

오작동 서명자를 식별하기 위한 대체 알고리즘들이 존재하지만, 다음 중 하나 이상의 이유로 아직 프로덕션 사용에 적합하지 않다:

- 아직 프로덕션 준비가 된 코드베이스가 아니다.
- 오픈소스가 아니다.
- 백서 형태로만 존재한다.

이 문제를 해결하기 위해, 우리는 CGGMP에 대한 개념증명(proof-of-concept)을 개발하고 있으며 FROST를 탐색하고 있다.

비트코인 브리지 설계의 최근 발전, 특히 BitVM2는 커스터디를 정직한 다수 가정에서 1-of-N 신뢰 가정으로 개선할 가능성을 시사한다. Threshold Network는 이 설계와 다양한 구현의 발전을 면밀히 모니터링하고 있으며, 기술이 충분히 성숙해지는 중기 시점에 tBTC의 기본 커스터디 메커니즘을 업그레이드할 의도를 가지고 있다.

가디언과 민터(Guardians and Minters)

가디언과 민터는 높은 신뢰를 받는 퍼블릭 오퍼레이터의 퍼미션드 집합이며, 그들의 평판이 걸려 있다.

가디언은 민팅 및 상환 요청을 검증하며, 악의적이거나 사기성 요청을 거부(veto)할 수 있다. 이 목록을 퍼미션리스로 만들 경우, 악의적인 민터가 가짜 민팅 요청으로 시스템을 도배하여 가디언에게 부담을 줄 수 있고, 악의적인 가디언이 모든 제안된 민팅을 거부하여 성장을 중단시킬 수도 있다.

가디언이나 민터가 오작동할 경우, Threshold DAO는 그들을 제거하기 위해 투표할 수 있다.

민터는 “빠른 민팅(fast minting)”을 가능하게 하는 편의 기능을 제공한다. 중요한 점은, 그들이 민팅 요청을 게이트키핑할 권한을 갖고 있지 않다는 것이다. 모든 민터가 승인을 거부하거나 가디언이 수락을 거부한 예치라 하더라도, 서명자들에 의해 여덟 시간마다 여전히 민팅될 수 있다. 이는 악의적 행위자가 민팅 프로세스를 교란하려는 상황에서도 시스템이 탄력성을 유지하고 이를 처리할 수 있게 보장한다.

스위핑(Sweeping)

스위핑이란 무엇인가?

스위핑은 tBTC 컨트랙트에서 비트코인 예치를 추적하기 위한 회계 최적화다. 이는 최근의 비트코인 예치들을 주기적으로 하나의 미사용 트랜잭션 출력(UTXO)으로 통합하여, 이더리움에 대한 보다 최적의 커밋 주기를 달성하는 것을 포함한다. 이 과정은 관련 공개키와 환불 타임락 추적을 단순화하고, 동시에 공급 페그 붕괴를 방지하는 데 도움을 준다. 일반적으로 스위핑은 예치의 규모와 빈도에 따라 8시간마다 수행된다.

작동 방식(How it works)

사용자가 예치를 수행하면, 우리 고유의 잠금 스크립트를 사용하여 자금을 잠근다. 이는 미사용 트랜잭션 출력(UTXO)을 생성한다.

일반적으로 비트코인 “지갑”(지갑은 이더리움에서와 동일한 방식으로 존재하지 않는다)의 역할은, 자신이 잠금을 해제할 수 있다고 판단하는 특정 잠금 스크립트 패턴(예: 사용자의 공개키에 연관된 P2PKH 스크립트)을 찾기 위해 블록체인을 스캔하고 관련 자금을 합산하는 것이다. 다른 사람에게 비트코인을 보내고자 할 때, 지갑 소프트웨어가 어떤 UTXO를 해제하여 송금할지 계산해 주므로 사용자는 이를 직접 할 필요가 없다.

우리가 비트코인 예치를 상환(redeem)할 수 있기를 원한다면, 지갑 소프트웨어가 하는 것과 동일한 방식으로 어떤 예치가 어떤 공개키와 연관되어 있는지 추적해야 할 것이다. 이는 특히 비트코인 채굴 수수료 관점에서 골치거리다.

더 나아가, 우리의 잠금 스크립트는 시간 잠금 환불(time-locked refund)의 개념을 포함한다. 특정 시간(작성 시점 기준 9개월; 스크립트의) 동안 자금이 건드려지지 않으면, 우리는 예치자가 자신의 예치를 회수할 수 있도록 허용한다. 이는 프로토콜이나 예치에 문제가 발생했을 때 효과적인 탈출구 역할을 하도록 설계되었다.

이로 인해, 우리는 예치를 수집하는 데 동일한 시간 제한을 갖게 된다. 만약 그 시간까지 자금을 이동하지 않으면, 사용자가 5 BTC를 예치하고 5 tBTC를 받은 다음, 9개월 후 상환 없이 원래의 5 BTC를 다시 회수할 수 있게 된다. 이는 tBTC의 공급 페그를 붕괴시킬 것이다.

스위핑(sweeping)은 이러한 두 가지 문제를 동시에 해결하는 것을 목표로 하며 성능 최적화 역할도 수행한다. 매 8시간마다 최근 예치들을 모두 모아 잠금을 해제하고, 일반적인 P2PKH 스크립트를 사용해 자금을 다시 지갑 자체로 송금하여 UTXO들을 하나의 UTXO로 통합한다.

그 결과, 여기저기 흩어진 예치들이 하나의 UTXO로 표현되는 단일 “더미(pile)”로 “스위프”되며, 우리는 이를 이더리움에 커밋할 수 있다.

예시(Example)

다음은 10.3 BTC의 예치다. 해당 예치는 트랜잭션 `odb1929c2fa41649264b95b9162bc7a12f43cb455a91bae7177667a53290d7e8`에서(다른 많은 예치들과 함께) 스위프되었다. 이는 해당 지갑이 수행한 세 번의 스위프 중 하나였다(작성 시점 기준).

그 트랜잭션은 1.51614471 BTC 상당의 UTXO를 생성했다. 다음 트랜잭션은

이전 UTXO(첫 번째 입력)와 모든 최근 예치를 사용하여 15.42475511 BTC 상당의 새로운 UTXO(오른쪽 출력)를 생성했다. 마지막 트랜잭션은

동일한 패턴을 따른다. 이전 UTXO(첫 번째 입력)와 최근 예치를 사용하여 59.52818486 BTC 상당의 새로운 UTXO를 생성한다.

커버리지 풀(Coverage Pool)

tBTC 프로토콜로 보호되는 자산을 위한 백스톱

요약(Summary)

Threshold Coverage Pool은 DAO가 비준한 “Sunsetting tBTC coverage pools” 제안에 따라 종료되었다.

Threshold Coverage Pool은 tBTC 프로토콜로 보호되는 자산의 백스톱 역할을 수행했다. 프로토콜에서 보호되던 비트코인이 손실되는 경우, 커버리지 풀의 리스크 매니저가 자산을 인출하여 BTC로 전환하고, 공급 페그를 가능한 한 가깝게 달성하기 위해 이를 다시 프로토콜로 투입하도록 되어 있었다. 커버리지 풀의 리스크 매니저는 Threshold Treasury Guild 멀티시그였다.

시간이 지나면서, tBTC와 T 간의 관계를 감안할 때 이 백스톱 모델이 최적이지 아니라는 점이 분명해졌다. BTC 담보 손실 사태 발생 시 T의 가치도 하락하여, 보험 백스톱으로서의 효율성이 크게 저하되기 때문이다. 결과적으로, TIP-064 승인과 함께 명시적 Threshold Coverage Pool은 종료되었다.

새롭게 구현된 “암묵적 커버리지 풀(implicit coverage pool)” 모델 하에서, tBTC는 Threshold DAO의 전적인 신용과 지급 능력 — 현재 T, ETH, wBTC, tBTC, 스테이블코인, CVX, veCRV, 관련 LP 토큰 등 — 으로 뒷받침된다.

Threshold USD

비트코인 담보 스테이블코인

Threshold USD(thUSD)는 USD에 소프트 페그되어 있으며 ETH와 tBTC를 담보로 하는 스테이블코인으로, 최소 담보 비율은 110%다.

담보로 BTC 또는 ETH를 사용하면 매우 낮은 비용으로 thUSD를 대출받을 수 있다.

Threshold USD는 PCV(“Protocol Controlled Value”)를 통해 자립하도록 구축된 Liquity 프로토콜의 수정 포크다. Threshold USD에는 LQTY 토큰에 해당하는 것이 없다. 대신 모든 수익은 PCV에 축적된다. 토큰이 없으므로, 부트스트래핑은 초기 프로토콜 대출(Initial Protocol Loan)을 통해 완료된다.

프로토콜이 자체 유동성(“PCV”)을 보유하는 결과는 장기적으로 더 예측 가능한 궤적과 지속 가능성이다. 스테빌리티 풀은 사용자 예치금 대신 PCV로 자금이 조달된다. 덕분에, 수동적 LQTY 스테이커(임차 유동성)에 대한 보상으로 자금이 낭비되지 않으며, 해당 자금은 대신 스테빌리티 풀에 재주입될 수 있다. 프로토콜이 성장하고 수수료가 축적됨에 따라, 스테빌리티 풀은 지속적으로 보강될 것이다.

멀티 담보(Multi-collateral)

Liquity는 담보 유형으로 ETH만을 허용한다. Threshold USD는 탈중앙화된 BTC 래퍼 tBTC를 통해 대출 담보로 BTC를 지원하도록 확장한다. 향후 충분히 탈중앙화된 경우 다른 유형의 담보도 온보딩 대상으로 고려될 수 있다.

각 담보는 자체 컨트랙트로 배포되며, 새로운 담보 추가는 배포 전 충분한 시간 지연을 수반하는 DAO 투표가 필요하다. 각 담보를 별도의 컨트랙트로 분리함으로써, 특정 컨트랙트에서 민팅을 불허하는 것만으로 해당 담보를 쉽게 폐기(deprecate)할 수 있다.

thUSD 개요

Threshold USD의 배경, 주요 파라미터 및 핵심 특성

소개(Introduction)

Threshold 프로토콜은 2023년에 비트코인과 이더리움 사이의 탈중앙화되고 확장 가능한 브리지인 tBTC 2세대를 출시했다. 이는 비트코인 보유자에게 더 넓은 DeFi 생태계로의 안전하고 개방된 접근을 제공한다.

즉각적으로 제기되는 질문은 DeFi 애플리케이션을 위해 브리지된 tBTC에 효용을 제공하는 것이다. Threshold USD는 thUSD를 민팅할 수 있게 함으로써 tBTC에 대체적 효용을 제공하며, 그 후 thUSD는 더 넓은 생태계에서 다양한 목적에 사용할 수 있다.

Threshold USD란 무엇인가?

Threshold USD는 tBTC와 ETH를 담보로 대출을 실행할 수 있게 하는 탈중앙화 대출 프로토콜이다. 대출은 thUSD(USD 페그 스테이블코인)로 지급되며, 최소 담보 비율 110%를 유지해야 한다.

담보 외에도, 대출은 thUSD를 보유한 스테빌리티 풀과 최후의 보증인 역할을 집합적으로 수행하는 동료 차입자들에 의해 보호된다. 이러한 메커니즘에 대해서는 Liquidation 항목에서 더 알아볼 수 있다.

Threshold USD 프로토콜은 Liquity(<https://www.liquity.org/>)의 포크를 기반으로 하며, Liquity는 2021년 5월 출시 이후 여러 차례의 중대한 스트레스 테스트를 성공적으로 통과하며 성공적인 프로토콜로 자리 잡았다.

Liquity는 완전히 거버넌스 프리이며 불변이다. 이는 프로토콜을 완전한 검열 저항적으로 만든다는 점에서 DeFi 프로토콜에 막대한 강점이지만, 동시에 프로토콜을 본질적인 오라클 리스크에 노출시키고 시장 역학에 맞춰 확장하고 대응할 수 있는 능력을 제한한다.

이를 염두에 두고, Threshold USD에는 일부 유연성이 내장되어 있다. 거버넌스를 통해 변경할 수 있는 몇 가지 파라미터가 존재한다:

- 담보 유형(Collateral Type): tBTC 외에도 다른 담보 유형이 추가될 수 있으며(ETH는 이더리움에서 가장 탈중앙화되고 풍부한 자산이므로 tBTC에 추가 담보가 된다), 민팅 및 소각 권한을 취소함으로써 제거될 수도 있다.
- 가격 피드 컨트랙트(Price Feed Contract): 오라클은 프로토콜의 건전성(청산 정의)에 핵심적이며, 기존 오라클의 성능

저하로 인해 업데이트가 필요할 수 있다.

- PCV 컨트랙트(PCV Contract): BAMM에서 PCV로 인출, 부채 상환, 모든 부채 상환 후 PCV에서 자금 인출.
- BAMM 컨트랙트(BAMM Contract): Dao는 “A” 파라미터 및 B.Protocol 수수료 변경 제출에 대해 거부권을 가진다.

이 문서는 Threshold USD와 관련된 적절한 변경 사항을 반영하여 Liquity 문서(<https://docs.liquity.org/>)를 기반으로 작성되었다.

Threshold USD의 동기는 무엇인가?

안정적 가치 자산은 이더리움 애플리케이션의 필수 빌딩 블록이며, 그 가치는 수십억 달러 규모로 성장해 왔다.

그러나 이 가치의 절대다수는 USDT와 USDC 같은 법정화폐 담보 스테이블코인 형태로 존재한다. DAI와 sUSD 같은 탈중앙화 스테이블코인은 전체 스테이블코인 공급에서 극히 일부분을 차지하며, 이는 대다수 스테이블코인이 중앙화되어 있음을 의미한다.

Threshold USD는 더 높은 자본 효율성과 사용자 친화성을 갖춘 스테이블코인 대출 방식을 제시함으로써 이러한 문제를 해결한다.

Threshold USD의 핵심 이점은 무엇인가?

Threshold USD의 핵심 이점은 다음과 같다:

- tBTC 대출에 대한 낮은 비용(발행 수수료 0.5%, 출시 시점 기준 이자율 없음).
- 최소 담보 비율 110% — 예치된 tBTC의 보다 효율적인 활용.
- 거버넌스 최소화 — 대부분의 운영은 알고리즘적이고 완전 자동화되어 있으며, 대부분의 프로토콜 파라미터는 컨트랙트 배포 시점에 설정된다.
 - 참고: 거버넌스를 통해 변경 가능한 파라미터는 위 섹션을 참조하라
- 직접 상환 가능 — thUSD는 언제든지 액면가로 기초 담보와 교환하여 상환할 수 있다.

Threshold USD는 업그레이드되거나 변경될 수 있는가?

그렇다. Threshold USD 토큰 컨트랙트의 민트 함수는 추가 컨트랙트를 추가할 수 있게 될 것이다. 이는 모든 컨트랙트를(가격 피드 컨트랙트를 예외로 하고) 불변으로 유지하면서도 업그레이드 옵션을 보유하는 방식이다.

Threshold USD는 어떻게 사용할 수 있는가?

웹 인터페이스(일명 프론트엔드)를 통해 또는 스마트 컨트랙트를 직접 호출하여 thUSD를 사용할 수 있다.

Threshold USD의 주요 사용 사례는 무엇인가?

- 볼트를 열어 tBTC를 담보로 thUSD를 대출받고, 이를 직접 DeFi 애플리케이션에서 사용하거나 다른 코인으로 교환한다
- 청산 보상을 대가로 스테빌리티 풀에 thUSD를 제공하여 Threshold USD를 보호한다
- Curve(<https://curve.fi/>)의 thUSD 풀에 유동성을 제공하여 스왑 수수료 및 경우에 따라 인센티브 수수료를 획득한다(이는 시간 의존적일 수 있으며 온/오프로 전환될 수 있다)
- thUSD 페그가 1 아래로 하락할 때 *thUSD*를 상당의 tBTC로 상환한다(즉, 시스템에 대한 차익거래)

thUSD란 무엇인가?

thUSD는 Threshold USD 프로토콜에서 대출금을 지급하는 데 사용되는 USD 페그 스테이블코인이다. 언제든지 액면가로 기초 담보에 대해 상환될 수 있다.

Threshold USD를 사용하기 위해 무엇이 필요한가?

thUSD를 대출받으려면, 지갑(예: MetaMask 또는 TaHo)과 볼트를 열고 가스 비용을 지불할 수 있을 만큼의 충분한 tBTC 또는 ETH만 있으면 된다.

스테빌리티 풀 예치자가 되려면 thUSD가 필요하며, 이는 볼트를 열어 대출받을 수 있다. 또한 Curve 또는 기타 (탈중앙화된) 거래소를 사용하여 공개 시장에서 토큰을 구매할 수도 있다.

Threshold USD는 수수료를 부과하는가?

다음은 Threshold USD 프로토콜 사용 시 부과되는 수수료다:

- thUSD를 차입할 때마다, 인출 금액(thUSD 기준)의 퍼센티지로 일회성 수수료가 부과된다
- thUSD를 상환할 때 부과되는 수수료(상환 메커니즘에 대한 자세한 내용은 “Redemptions and thUSD Price Stability” 섹션 참조)
 - 상환자 입장에서는, thUSD를 tBTC로 교환할 때 시스템이 사용자에게 지급하는 금액(tBTC 기준)에 상환 수수료가 부과된다. 상환은 차입자로서의 대출 상환(수수료 없음)과는 별개임에 유의하라
- 두 수수료는 상환 규모에 의존한다. 즉, 상환 금액에 함수적으로 따라 각 상환 시 증가하며, 상환이 발생하지 않는 동안에는 시간이 지남에 따라 감소한다. 의도는 높은 수수료로 대규모 상환을 억제하고, 대규모 상환 직후의 차입을 억제하는 데 있다. 시간 경과에 따른 수수료 감소는 상환 규모가 낮을 때 차입자와 상환자 모두의 수수료가 “냉각”되도록 보장한다.
- 수수료는 0.5%보다 작아질 수 없다(리커버리 모드 제외). 이는 가격 피드를 프런트런닝하는 차익거래자에 의해 상환 기능이 오용되는 것을 방지한다. 차입 수수료는 5%로 상환이 설정되어 있어, 상환으로 인해 통화량이 축소되는 국면에서도 시스템이(어느 정도) 차입자에게 매력적일도록 유지한다. 그 외에는 두 수수료는 동일하다.
- 이자율: 출시 시점에서는 ETH와 tBTC를 담보로 사용할 때 진행성 이자율은 부과되지 않으며, 초기 차입 수수료만 존재한다.

대출 원금(thUSD)에 대해 경과 시간과 사전에 정해진 이자율을 기반으로 계산되는 진행성 이자율을 도입할지 여부에 대한 결정은, 가까운 미래에 DAO가 해당 담보들과 향후 추가될 수 있는 다른 담보들에 대해 내릴 것이다.

Threshold USD로 어떻게 수익을 낼 수 있는가?

Threshold USD를 사용하여 수익을 창출하는 주요 방법은 두 가지다:

- Curve(<https://curve.fi/>)의 thUSD 풀에 유동성을 제공하여 스왑 수수료와 경우에 따라 인센티브 수수료를 획득한다 (이는 시간 의존적일 수 있으며 온/오프로 전환될 수 있다)
- thUSD를 스테빌리티 풀에 예치하고 청산 이익(tBTC)을 획득한다.

시간이 지나면서 DeFi 생태계에서 thUSD를 사용하여 보상이나 수익을 얻을 수 있는 다른 기회가 생길 수 있다.

자금을 잃을 수도 있는가?

비수탁형 시스템으로서, 프로토콜로 전송된 모든 토큰은 어떤 개인이나 법인의 개입 없이 알고리즘에 의해 보관·관리된다. 이는 사용자의 자금이 스마트 컨트랙트 코드에 규정된 규칙에만 종속됨을 의미한다.

다음과 같은 청산 시나리오에서는 자금의 전부 또는 일부를 잃을 수 있다:

- 당신이 차입자(볼트 소유자)이고, 당신의 tBTC 담보가 청산된다. 당신은 차입한 thUSD는 유지하지만, 볼트는 닫히며 담보는 스테빌리티 풀 예치자들에게 보상하는 데 사용된다.
 - 청산이 노멀 모드(Normal Mode)에서 발생하는 경우(즉, 당신의 볼트가 담보 비율 110%인 경우), 모든 담보가 청산 및 수수료에 사용된다
 - 청산이 리커버리 모드(Recovery Mode)에서 발생하는 경우(즉, 프로토콜 총 담보 비율이 150% 미만인 경우), 당신의 볼트가 담보 비율 110%와 150% 사이에 있다면 담보의 일부를 회수할 수 있다

추가로, 다음과 같은 시나리오가 발생하여 자금 손실로 이어질 수 있다:

- 버그/해킹: 시스템이 면밀히 감사를 받았더라도, 사용자에게 손실을 초래하는 해킹이나 버그 가능성을 완전히 배제할 수는 없다. 여기에는 thUSD의 담보인 tBTC에서의 잠재적 버그/해킹도 포함된다.
- 가격 오라클 리스크: 청산은 담보 비율에 의해 촉발되며, 이는 담보 가격의 함수다. 가격 피드의 오작동 또는 조작 위험이 존재한다. 우리는 이러한 리스크에 대한 노출을 최소화하고 있지만, 완전히 배제할 수는 없다
- Threshold USD가 받아들여지지 않아 모든 사용자가 이탈하려는 경우, 마지막 일부 담보는 회수할 수 없다. 이는(대출 수수료 누적으로 인해) 충분한 thUSD가 존재하지 않기 때문이다. 이는 극히 일부의 자본에만 영향을 미칠 것이다
- 상환의 경우, 상환이 급격히 증가하면 상환 수수료가 상승하여 손실로 이어질 수 있다. 프로토콜 총 담보 비율이 110% 미만이면 상환은 차단된다

차입(Borrowing)

thUSD 차입의 핵심 측면과 파라미터

왜 Threshold USD로 차입해야 하는가?

Threshold USD 프로토콜은 낮은 이자율의 대출을 제공하며, 다른 차입 시스템보다 자본 효율적이다(즉, 동일한 대출에 필요한 담보가 더 적다). 유동 자금을 확보하기 위해 tBTC를 판매하는 대신, 프로토콜을 사용하여 tBTC를 잠그고, 담보를 기반으로 thUSD를 인출한 뒤, 향후 시점에 대출을 상환할 수 있다.

예를 들어: 향후 tBTC 가격 상승을 예상하는 차입자는 프로토콜을 사용하여 자신의 tBTC 포지션을 최대 11배까지 레버리지할 수 있으며, 가격 변동에 대한 익스포저를 증가시킬 수 있다. 이는 tBTC를 담보로 thUSD를 차입한 다음, 공개 시장에서 이를 판매하여 더 많은 tBTC를 구매하고 — 이를 반복할 수 있기 때문에 가능하다.*

*참고: 이는 Threshold USD 사용 방법에 대한 권고가 아니다. 레버리지는 매우 위험할 수 있으며, 모든 자금을 잃을 수 있으므로 경험이 있는 사용자이거나 투기적 소액에 대해서만 사용해야 한다.

담보란 무엇을 의미하는가?

담보는 차입자가 대출을 받기 위해 제공해야 하는 자산으로, 부채에 대한 담보 역할을 한다.

tBTC만이 Threshold USD에서 허용되는 담보인가?

현재 Threshold USD는 담보로 tBTC와 ETH를 지원하지만, 코드가 이를 허용하므로 거버넌스 투표에 따라 추가 담보가 도입될 수 있다. 이 두 담보를 채택한 이유는 이들이 이더리움 생태계에서 가장 탈중앙화된 두 자산을 대표하기 때문이다.

Threshold USD로 어떻게 차입할 수 있는가?

차입하려면 볼트를 열고 일정량의 담보(tBTC)를 예치해야 한다. 그런 다음 담보 비율 110%까지 thUSD를 인출할 수 있다. 최소 부채는 2,000 thUSD가 요구된다. 이 최소 부채 임계값은 공격자가 대규모의 볼트를 생성한 뒤 청산이 비경제적으로 되도록 만드는 것을 방지한다.

볼트(Vault)란 무엇인가?

볼트는 대출을 실행하고 유지하는 곳이다. 각 볼트는 하나의 이더리움 주소에 연결되며, 각 주소는 오직 하나의 볼트만 가질 수 있다. 다른 플랫폼의 Trove나 CDP에 익숙하다면, 볼트는 개념적으로 유사하다.

볼트는 두 가지 잔액을 유지한다. 하나는 담보 역할을 하는 자산(tBTC)이고, 다른 하나는 thUSD로 표시된 부채다. 담보를 추가하거나 부채를 상환함으로써 각 잔액을 변경할 수 있다. 이러한 잔액 변동에 따라 볼트의 담보 비율도 그에 맞게 변한다.

언제든지 부채를 전액 상환하여 볼트를 닫을 수 있다.

차입자인 나는 수수료를 지불해야 하는가?

기본 상황에 대해서는 “Threshold USD는 수수료를 부과하는가?” 섹션을 참조하라.

볼트에서 thUSD를 인출할 때마다, 인출 금액에 대해 일회성 차입 수수료가 부과되어 부채에 추가된다. 차입 수수료는 가변적이며 (알고리즘적으로 결정됨) 정상 운영 하에서 최소값은 0.5%임에 유의하라. 리커버리 모드에서는 수수료가 0%다.

또한 200 thUSD의 청산 준비금(Liquidation Reserve) 수수료가 적용되나, 부채 상환 시 반환된다.

차입 수수료는 어떻게 계산되는가?

대출이 개시되면, 차입 수수료는 볼트의 부채에 추가되며 baseRate에 의해 결정된다. 수수료율은 0.5%에서 5% 사이의 범위로 제한되며, 차입자가 인출한 유동성 금액에 곱해진다.

예시: 차입 수수료가 0.5%이고 차입자가 자신의 지갑으로 4,000 thUSD를 받고자 한다. 20.00 thUSD의 차입 수수료가 부과되며, 청산 준비금과 발행 수수료가 추가된 후 차입자의 부채는 4,220 thUSD가 된다.

대출은 언제 상환해야 하는가?

프로토콜이 발행한 대출에는 상환 일정이 없다. 담보 비율을 최소 110% 이상으로 유지하는 한, 볼트를 열린 상태로 두고 언제든지 부채를 상환할 수 있다.

담보 비율이란 무엇인가?

이는 볼트에 있는 담보의 달러 가치와 그 부채(thUSD) 간의 비율이다. 볼트의 담보 비율은 tBTC 가격이 변함에 따라 시간에 따라 변동한다. 볼트의 담보 및/또는 부채를 조정하여 — 즉, 더 많은 tBTC 담보를 추가하거나 부채의 일부를 상환하여 — 이 비율에 영향을 줄 수 있다.

예시: 현재 tBTC 가격이 \$30,000이고 1 tBTC를 예치한다고 하자. 10,000 thUSD를 차입하면, 볼트의 담보 비율은 200%가 된다.

$$(1\text{tBTC} * \$30,000 / 10,000 \text{ thUSD}) * 100 = 300\%$$

대신 15,000 thUSD를 차입한다면 비율은 200%가 된다.

최소 담보 비율(MCR)과 “권장” 담보 비율은 무엇인가?

최소 담보 비율(MCR)은 정상 운영(일명 Normal Mode) 하에서 청산을 촉발하지 않는 최소 부채 대 담보 비율이다. 이는 프로토콜 파라미터로 110%로 설정되어 있다. 따라서 볼트의 부채가 10,000 thUSD라면, 청산을 피하려면 최소 \$11,000 상당의 tBTC를 담보로 예치해야 한다.

리커버리 모드 동안 청산을 피하려면, 비율을 150%를 충분히 상회하도록 유지하는 것이 권장된다(예: 200% 또는 가능하면 250%).

내 볼트가 청산되면 어떻게 되는가?

청산을 통해 부채가 상환되므로 담보를 잃게 된다. 즉, 부채를 상환하여 담보를 되찾을 수 없게 된다. 따라서 청산은 담보의 달러 가치에서 순손실 9.09%(= 100% * 10 / 110)를 초래한다.

청산 준비금(Liquidation Reserve)이란 무엇인가?

볼트를 열고 대출을 실행할 때, 200 thUSD가 따로 적립되어, 볼트가 청산되는 경우 트랜잭션 송신자의 가스비를 보전하는 데 사용된다. 볼트가 청산되지 않으면 청산 준비금은 전액 환불되며, 부채를 상환하고 볼트를 닫을 때 사용자에게 반환된다. 청산 준비금은 부채로 계산되어 볼트의 담보 비율 계산에 포함되므로, 실제 담보 요건을 약간 증가시킨다.

내 볼트가 상환 대상이 되면 어떻게 되는가?

thUSD가 상환될 때, 상환자에게 제공되는 tBTC는 담보 비율이 가장 낮은 볼트(110% 이상이라도)에서 할당된다. 상환 시점에 당신의 볼트가 가장 낮은 비율을 가진 경우, 일부 담보를 포기하게 되지만, 그에 상응하여 부채가 감소한다.

tBTC 담보가 줄어드는 USD 가치는 볼트의 부채가 감소하는 명목상의 thUSD 금액에 해당한다. 상환은 다른 누군가가 당신의 부채를 상환하고 그에 상응하는 담보를 회수하는 것으로 생각할 수 있다. 긍정적인 부수 효과로, 상환은 해당 볼트들의 담보 비율을 개선하여, 그 볼트들을 덜 위험하게 만든다.

부채를 0으로 만들지 않는 상환은 부분 상환이라 하고, 볼트의 부채를 전액 상환하는 상환은 전액 상환이라 한다. 이 경우, 볼트는 닫히며, 언제든지 담보 초과분과 청산 준비금을 청구할 수 있다.

당신이 2 tBTC를 담보로 예치하고 32,000 thUSD의 부채를 가진 볼트를 보유하고 있다고 하자. 현재 tBTC 가격이 \$20,000 이라면, 담보 비율(CR)은 $125\% (= 100\% * (2 * 20,000) / 32,000)$ 가 된다. 이것이 Threshold USD 시스템에서 가장 낮은 CR이라고 가정하고, 부분 상환과 전액 상환의 두 가지 예를 살펴보자:

부분 상환의 예

어떤 사용자가 12,000 thUSD를 상환하여 0.6 tBTC를 받고, 이로써 당신의 부채 12,000 thUSD가 상환되어 32,000 thUSD에서 20,000 thUSD로 줄어든다. 그 대가로, \$12,000에 해당하는 0.6 tBTC가 당신의 볼트에서 상환자에게 이전된다. 담보는 2 tBTC에서 1.4 tBTC로 감소하는 반면, 담보 비율은 125%에서 $140\% (= 100\% * (1.4 * 20,000) / 20,000)$ 로 상승한다.

전액 상환의 예

어떤 사용자가 60,000 thUSD를 상환하여 3 tBTC를 받는다. 상환액이 당신의 부채에서 200 thUSD(청산 준비금으로 적립)만큼을 뺀 값보다 크므로, 당신의 32,000 thUSD 부채는 전액 상환되고, 담보는 \$30,000 상당의 tBTC만큼 줄어들어 0.5 tBTC가 남는다($= 2 - 30,000 / 20,000$).

어떻게 110%처럼 낮은 담보 비율을 제공할 수 있는가?

Threshold USD는 청산을 즉각적이고 더 효율적으로 만들어, 청산 시 담보를 매각하기 위해 장기간의 경매 메커니즘에 의존하는 유사 프로토콜과 동일한 보안 수준을 제공하는 데 필요한 담보를 적게 한다.

레버리지는 어떻게 활용할 수 있는가?

차입한 thUSD를 시장에서 tBTC로 판매하고, 이를 사용해 볼트의 담보를 보강할 수 있다. 그러면 더 많은 thUSD를 인출하여 판매할 수 있으며, 이 과정을 반복함으로써 원하는 레버리지 비율에 도달할 수 있다.

참고: 이는 Threshold USD 사용 방법에 대한 권고가 아니다. 레버리지는 매우 위험하며, 경험이 있는 사용자만 사용해야 하고, 대부분의 경우 결국 청산으로 이어질 수 있으므로 피해야 한다.

내 개입 없이 볼트의 담보와 부채가 증가한 이유는 무엇인가?

볼트들이 청산되었고 스테빌리티 풀이 비어 있거나(청산으로 인해 비워진 경우), 재분배 과정의 일부로서 모든 차입자는 청산된 담보와 부채의 일부를 배분받게 된다.

스테빌리티 풀과 청산(Stability Pool and Liquidations)

담보 가격 변동 하에서 thUSD의 지급 능력을 유지하기 위한 메커니즘

스테빌리티 풀은 무엇인가?

스테빌리티 풀은 시스템 지급 능력을 유지하기 위한 1차 방어선이다. 이는 청산된 볼트의 부채를 상환하기 위한 유동성 공급원으로 작동함으로써 — 총 thUSD 공급이 항상 담보로 뒷받침되도록 보장함으로써 — 이를 달성한다.

어떤 볼트가 청산되면, 해당 볼트의 잔여 부채에 해당하는 thUSD가 스테빌리티 풀의 잔액에서 소각되어 부채를 상환한다. 그 대가로, 볼트의 전체 담보가 스테빌리티 풀로 이전된다.

스테빌리티 풀은 사용자가 thUSD를 이전하여(스테빌리티 프로바이더라 부름) 자금을 공급한다. 시간이 지남에 따라 스테빌리티 프로바이더는 thUSD 예치금의 지분 비율만큼을 상실하는 반면, 청산된 담보의 지분 비율만큼을 획득한다. 그러나 볼트는 담보 비율이 110%를 약간 하회하는 지점에서 청산될 가능성이 높으므로, 스테빌리티 프로바이더는 자신이 상환한 부채에 비해 더 큰 달러 가치를 가진 담보를 받게 될 것으로 예상된다.

왜 스테빌리티 풀에 thUSD를 예치해야 하는가?

스테빌리티 풀 프로바이더는 청산 이익을 얻게 된다.

청산이란 무엇인가?

스테이블코인 공급 전량이 담보로 완전히 뒷받침되도록 보장하기 위해, 담보 비율이 110% 미만으로 떨어진 볼트는 닫히며(청산된다).

볼트의 부채는 취소되어 스테빌리티 풀에 흡수되고, 담보는 스테빌리티 프로바이더들 사이에 분배된다.

볼트 소유자는 차입한 thUSD 전액을 계속 보유하지만, 총 가치의 약 10%를 상실하므로, 담보 비율을 항상 110% 이상, 이상적으로는 150% 이상으로 유지하는 것이 매우 중요하다.

누가 볼트를 청산할 수 있는가?

볼트가 최소 담보 비율 110% 아래로 떨어지는 즉시 누구나 청산을 실행할 수 있다. 개시자는 이 서비스에 대한 보상으로 가스 보상(200 thUSD + 볼트 담보의 0.5%)을 받는다.

볼트를 청산했을 때 나는 어떻게 보상받는가?

볼트 청산에는 개시자가 부담해야 하는 특정 가스 비용이 수반된다. 볼트당 비용은 최대 160–185개의 볼트를 일괄 청산(batch liquidation)함으로써 감소시켰지만, 가스비 급등 시에도 청산이 수익성을 유지하도록 하기 위해 프로토콜은 다음 수식을 통해 가스 보상을 제공한다:

$$\text{gas compensation} = 200 \text{ thUSD} + 0.5\% \text{ of Vault's collateral (ETH)}$$

200 thUSD는 청산 준비금에서 충당되며, 가변적인 0.5%(tBTC 기준) 부분은 청산된 담보에서 나오므로, 스테빌리티 프로바이더의 청산 이익을 약간 줄인다.

스테빌리티 프로바이더로서 청산에서 나는 어떤 이익을 얻는가?

청산은 담보 비율 110% 바로 아래에서 발생하므로, 볼트가 청산될 때마다 순이익을 얻을 가능성이 높다.

예를 들어, 스테빌리티 풀에 총 1,000,000 thUSD가 있고, 당신의 예치금이 100,000 thUSD라고 하자.

이제 부채가 200,000 thUSD이고 담보가 10.9 tBTC인 볼트가 tBTC 가격 20,000에서 청산되어, 담보비율 109.21,800에 해당한다. 청산에서의 순이익은 \$1,800다.

예치자는 상환 예외(다음 섹션 참조)를 제외하고, tBTC의 USD 가치가 하락할 것으로 예상되는 경우, 청산으로 받은 담보를 즉시 인출하여 매도함으로써 tBTC에 대한 익스포저를 줄일 수 있음을 유의하라.

언제든지 예치금을 인출할 수 있는가?

일반 원칙으로, 스테빌리티 풀에 한 예치금은 언제든지 인출할 수 있다. 최소 락업 기간은 없다. 다만, 담보 비율이 110% 미만임에도 아직 청산되지 않은 볼트가 존재하는 경우에는 인출이 일시적으로 중단된다.

tBTC의 가격을 결정하기 위해 어떤 오라클을 사용하는가?

프로토콜은 Chainlink의 tBTC:USD 가격 피드를 사용하며, 다음과 같은(극단적인) 조건 하에서는 Tellor tBTC:USD 오라클로 폴백한다:

- Chainlink 가격이 4시간 이상 업데이트되지 않은 경우
- Chainlink 응답 호출이 리버트되거나, 유효하지 않은 가격 또는 유효하지 않은 타임스탬프를 반환하는 경우
- 연속된 두 번의 Chainlink 가격 업데이트 사이의 가격 변화가 50%를 초과하는 경우

스테빌리티 풀에 자금을 예치하면 손실을 볼 수 있는가?

대부분의 경우 청산은 100%를 훨씬 상회하는 담보 비율에서 발생하지만, 플래시 크래시 또는 오라클 오류로 인해 100% 미만에서 볼트가 청산될 가능성이 이론적으로 존재한다. 이러한 경우, 담보 수취액이 예치금 감소분보다 작아 손실이 발생할 수 있다.

thUSD가 1초과가격에 거래될 때는, 담보비율이 100% 초과 가격으로 thUSD를 매도한 경우에만 “손실”이 실현된다.

시스템이 면밀히 감사를 받았더라도, 사용자에게 손실을 초래할 수 있는 해킹이나 버그 가능성을 완전히 배제할 수 없음을 유의하라.

청산이 발생할 때 스테빌리티 풀이 비어 있으면 어떻게 되는가?

스테빌리티 풀이 비어 있는 경우, 시스템은 재분배(redistribution)라 불리는 이차 청산 메커니즘을 사용한다. 이 경우, 시스템은 청산된 볼트의 부채와 담보를 다른 모든 기존 볼트로 재분배한다. 부채와 담보의 재분배는 수취 볼트의 담보 규모에 비례하여 이루어진다.

상환과 thUSD 가격 안정성

상환은 thUSD가 \$1 아래로 떨어질 경우 그 가치를 1USD로 복귀시키기 위한 메커니즘이다

thUSD는 USD 가격을 어떻게 밀접하게 추종하는가?

액면가(즉, 1 thUSD를 \$1 상당의 tBTC와 교환)로 thUSD를 tBTC로 상환할 수 있는 능력과 최소 담보 비율 110%는 각각 차익거래 기회를 통해 가격 하한과 가격 상한을 만든다. 우리는 이를 직접 프로세스에 기반하므로 “하드 페그 메커니즘”이라 부른다.

thUSD는 USD 패리티를 위한 덜 직접적인 메커니즘(“소프트 페그 메커니즘”)의 이점도 누린다. 이러한 메커니즘 중 하나는 쉘링 포인트로서의 패리티다. Threshold USD는 thUSD를 USD와 동등하게 취급하므로, 양자 간 패리티는 프로토콜의 합의된 균형 상태다. 또 다른 메커니즘은 신규 부채에 대한 차입 수수료다. 상환이 증가(즉 thUSD가 1 이하임을 시사)하면 baseRate도 증가하여 차입을 덜 매력적으로 만들어 새로운 thUSD가 시장에 유입되어 가격을 1 이하로 밀어내는 것을 억제한다.

(thUSD 프로토콜이 기반한) Liquity는 LUSD의 가격 안정성에 대해 여기서 철저한 분석을 수행했다(<https://www.liquity.org/blog/on-price-stability-of-liquity>). 이 분석은 thUSD에도 동일하게 관련된다.

상환(Redemptions)이란 무엇인가?

상환은 thUSD를 액면가로 tBTC와 교환하는 과정으로, 1 thUSD가 정확히 1의 가치가 있는 것처럼 취급한다. 즉, x thUSD에 대해 x 상당의 tBTC를 돌려받는다.

사용자는 언제든지 제한 없이 thUSD를 tBTC로 상환할 수 있다. 다만, 상환 금액에는 상환 수수료가 부과될 수 있다.

예를 들어, 현재 상환 수수료가 1%이고 tBTC 가격이 \$50,000이며 10,000 thUSD를 상환한다면, 0.198 tBTC(0.2 tBTC에서 0.002 tBTC의 상환 수수료 차감)를 받게 된다.

상환된 금액은 baseRate 계산에 반영되며, 특히 규모가 큰 경우 상환 수수료에 영향을 미칠 수 있음을 유의하라.

상환 메커니즘이 어떻게 작동하는지 보여주기 위해, 아래에는 LUSD의 가치가 1 USD 아래로 하락했을 때의 작동 모습을 제시한다. 차입률(빨간선)은 즉시 0.5%에서 약 1.8%로 급등했고, 상환(파란 막대)이 발생하기 시작했다. 즉, 사용자가 1 USD 미만 가격에 LUSD를 매수한 뒤, 볼트에서 1 USD로 평가된 ETH와 상환하여 차익거래를 수행하고, LUSD 공급을 줄이며 가격을 끌어 올렸다.

상환은 내 부채를 상환(갚는)하는 것과 동일한가?

아니다. 상환은 완전히 별개의 메커니즘이다. 자신의 부채를 갚으려면, 볼트의 부채와 담보를 조정하기만 하면 된다.

상환 수수료는 어떻게 계산되는가?

정상 운영 하에서, 상환 수수료는 $(baseRate + 0.5\%) * tBTCdrawn$ 공식에 의해 결정된다.

baseRate는 어떻게 계산되는가?

상환 수수료는 Threshold USD의 상태 변수인 baseRate에 기반하며, 이는 동적으로 업데이트된다. baseRate는 각 상환과 함께 증가하며, 마지막 수수료 이벤트(즉, 마지막 상환 또는 thUSD 발행) 이후 경과 시간에 따라 감소한다.

각 상환 시:

- baseRate는 마지막 수수료 이벤트 이후 경과 시간에 따라 감소된다
- baseRate는 상환된 총 thUSD 공급의 비율에 비례하는 양만큼 증가한다
- 상환 수수료는 $(baseRate + 0.5\%) * tBTCdrawn$ 으로 주어진다

차입자인 내가 상환 대상이 되면 손실을 보는가?

당신의 볼트가 상환 대상이 되더라도 순손실은 발생하지 않는다. 다만, tBTC 익스포저의 일부를 잃게 된다. 상환 이후 당신의 볼트 담보 비율은 개선된다.

상환 대상이 되는 것을 어떻게 피할 수 있는가?

가장 좋은 방법은 시스템 내 다른 볼트 대비 높은 담보 비율을 유지하는 것이다. 기억하라: 상환이 발생할 때 가장 위험한 볼트(즉, 담보 비율이 가장 낮은 볼트)가 우선 순위가 된다.

리커버리 모드(Recovery Mode)

모든 볼트를 통틀어 총 담보 비율이 150%를 상회하도록 보장함으로써 thUSD의 시스템적 리스크를 낮추는 메커니즘

리커버리 모드란 무엇인가?

시스템의 총 담보 비율(TCR)이 150% 미만으로 떨어지면 리커버리 모드가 발동한다.

리커버리 모드 동안에는 담보 비율이 150% 미만인 볼트가 청산될 수 있다.

더욱이, 시스템은 TCR을 추가로 낮출 차입자 트랜잭션을 차단한다. 새로운 thUSD는 기존 볼트의 담보 비율을 개선하는 방식으로 조정하거나, 담보 비율이 150% 이상인 새로운 볼트를 개설하는 경우에만 발행될 수 있다. 일반적으로, 기존 볼트의 조정이 담보 비율을 낮춘다면, 그 트랜잭션은 결과적인 TCR이 150%를 상회하는 경우에만 실행된다.

총 담보 비율(TCR)이란 무엇인가?

총 담보 비율 또는 TCR은 현재 ETH:USD 가격에서 시스템 전체 담보의 달러 가치를 시스템 전체 부채로 나눈 비율이다. 다시 말해, 모든 볼트의 담보를 USD로 표현한 값을 합산한 뒤, 모든 볼트의 부채(thUSD로 표현)를 합산한 값으로 나눈 것이다.

리커버리 모드의 목적은 무엇인가?

리커버리 모드의 목표는 차입자가 TCR을 신속히 150% 이상으로 끌어올리도록 동기를 부여하고, thUSD 보유자가 스테빌리티 풀을 보충하도록 유인하는 것이다.

경제적으로, 리커버리 모드는 담보 추가와 부채 상환을 장려하도록 설계되어 있으며, 동시에 자기 상쇄적 억지(deterrent)로 작동한다: 리커버리 모드가 발생할 가능성 자체가 시스템이 그 상태에 도달하지 않도록 유도한다. 리커버리 모드는 시스템에 바람직한 상태가 아니다.

리커버리 모드에서의 수수료는 무엇인가

리커버리 모드는 상환 수수료에는 영향을 주지 않으며, 차입 수수료는 0%로 설정되어(위에서 설명한 한계 내에서) 차입을 최대한 장려한다.

리커버리 모드에서 내 볼트를 안전하게 유지하려면?

담보 비율을 150% 이상으로 높이면, 볼트는 청산으로부터 보호된다. 이는 담보를 추가하거나, 부채를 상환하거나, 또는 둘 다 수행함으로써 가능하다.

리커버리 모드에서 내 담보 비율이 150% 미만이면 청산될 수 있는가?

그렇다. 볼트의 담보 비율이 150% 미만이라면 150% 아래에서 청산될 수 있다. 노멀 모드와 리커버리 모드 모두에서 청산을 피하려면, 사용자는 담보 비율을 150% 이상으로 유지해야 한다.

리커버리 모드에서 볼트 담보의 어느 정도가 청산될 수 있는가?

리커버리 모드에서는, 청산 손실이 볼트 담보의 110%로 상한(cap)된다. 나머지, 즉 110%를 초과하는(그리고 TCR 아래의) 담보는 표준 웹 인터페이스를 사용하여 청산된 차입자가 회수할 수 있다.

이는 볼트가 청산되는 경우 차입자가 리커버리 모드에서나 노멀 모드에서나 동일한 청산 “패널티”(10%)에 직면한다는 것을 의미한다.

부트스트래핑(Bootstrapping)

비트코인 담보 스테이블코인

스테이블코인이 제대로 작동하기 위해서는 일정한 네트워크 효과가 필요하다. 부트스트래핑은 프로토콜이 자급자족할 만큼 충분한 견인력을 확보했음을 보장하는 과정이다.

과거에는 이를 대개 코인의 초기 채택자가 됨으로써 달성했다. 예를 들어 비트코인을 일찍 매수하고 더 낮은 가격의 혜택을 누리는 방식이다. DeFi는 수익 파밍(일명 임차 유동성)을 통해 자본의 부트스트래핑을 가능하게 함으로써 부트스트래핑 개념을 혁신했다.

Liquity 프로토콜(LUSD 스테이블코인의 창시자)은 스테빌리티 풀 예치자에게 LQTY 토큰을 발행함으로써 부트스트래핑했다. 이는 사람들이 대출을 받고 스테빌리티 풀에 예치하도록 유인했다.

프로토콜이 정상적이고 건강하게 운영되려면, 모든 청산을 커버할 만큼 스테빌리티 풀에 충분한 자금이 존재하는 것이 매우 중요하다. 그러나 LQTY 인센티브는 필요 이상으로 많은 예치를 초래하여, 사실상 자본 낭비를 만들었다. 더욱이 초기 1억 LQTY가 발행된 이후에도, 풀(스테빌리티 풀)이 오직 청산 보상만으로 유지되는 상황에서 Liquity가 얼마나 지속 가능할지에 대한 우려가 있다.

Threshold USD는 이를 어떻게 접근하는가?

Threshold USD에서는 다른 접근법을 취한다. DeFi의 비교적 새로운 개념인 프로토콜 통제 가치(PCV, Protocol Controlled Value)는 프로토콜 자체가 유동성을 소유하고 이를 프로토콜 개선에 사용하는 아이디어다. 이는 다른 곳에서 유동성을 임차(일명 수익 파밍)하는 것에 대한 새로운 대안이며, 장기적 지속 가능성이라는 이점을 갖는다.

그러나 PCV는 어딘가에서 와야 한다. thUSD에서는 PCV에 초기 프로토콜 대출(Initial Protocol Loan)을 발행하고, 그 자금을 스테빌리티 풀에 직접 예치함으로써 이를 해결한다. 자세한 내용은 여기에서 확인하라:

Initial Protocol Loan

이는 프로토콜에 비용을 들이지 않고 스테빌리티 풀을 부트스트랩할 수 있게 해준다.

그뿐만 아니라, LQTY 토큰을 제거함으로써 모든 수익(이자, 상환 수수료 등)이 직접 PCV로 유입된다. 수익이 LQTY 보유자에게 분배되는 Liquity와 비교하면, 우리는 비용 없이 시스템에 대한 막대한 유출을 제거했다.

스테빌리티 풀이 자체적으로 자금을 갖추는 것만으로도 프로토콜은 기능할 수 있으며, 자신의 tBTC를 담보로 대출받고자 하는 일부 사용자가 참여할 것으로 예상된다. 그러나 이것만으로 대규모 채택이 일어나지는 않을 것이며, thUSD가 제대로 기능하려면 약 \$1에서 안정적이어야 하고, 이를 위해서는 탈중앙화 거래소에 유동성이 공급되어야 한다.

더 많은 사용자를 유치하고 thUSD의 유동성을 창출하기 위해, 우리는 다른 플랫폼(예: Curve의 thUSD 스테이블코인 풀)에 보상을 지급할 것이다. 이는 사용자가 부채를 발행하고 Curve에 예치하도록 유인하며, 유동성과 탄력성 개선이라는 부가적인 이점을 제공한다.

우리가 얼마나 빠르게 성장하길 원하는지는 풀에 보내는 보상 규모를 통해 거의 전적으로 조정할 수 있다.

이 부분은 실제로 단점이 있는 임차 유동성이 맞지만, Threshold USD의 수익이 LQTY 보유자가 아닌 PCV로 귀속된다는 점을 기억하라. 프로토콜의 인기가 높아짐에 따라, 프로토콜 자체의 수익을 이 보상을 자금 조달하는 데 사용할 수 있어, 자가 지속적 피드백 루프를 만든다.

더불어, Threshold DAO는 일부 준비금을 스테이블코인으로 보관할 것이므로, Threshold DAO는 Curve에 예치함으로써 PCV를 개시할 수 있다. 이는 thUSD의 안정성을 더욱 높여 채택에 중요하다.

초기 프로토콜 대출(Initial Protocol Loan)

초기 프로토콜 대출(IPL)은 스테빌리티 풀에 자금을 공급하기 위해 프로토콜 자체를 담보로 발행하는 부채다. 기술적으로는 부채이지만, 모든 자금이 계정 처리되므로 프로토콜 자체를 부분 준비금(fractional reserve)으로 만들지는 않는다.

작동 방식(How it works)

thUSD는 PCV에 의해 민팅되어 스테빌리티 풀에 예치된다. 부채가 완전히 상환될 때까지 인출 동결이 시작된다. 언제든지 Threshold DAO는 인출을 개시할 수 있으며, 이때 부채를 소각(destroy)하고 초과분을 인출한다. PCV가 어떤 이유로 부채보다 적은 자금만 보유한 경우, 인출은 거부된다.

프로토콜 사용(대출 이자, 상환 수수료 등)으로부터의 수익은 PCV로 축적되므로, 가용 자금이 부채보다 적은 경우에는 먼저 프로토콜이 부족분을 벌어들여야 한다.

하이브리드 PCV + IPL 모델의 이점:

- 스테빌리티 풀을 무상으로 부트스트랩
- 프로토콜 토큰 불필요 = 모든 수익이 직접 PCV로 축적
- 첫 대출 실행/청산 시점부터 즉각적인 잉여
- 예측 가능성과(부채 상환 이후) 블랙스완에 대한 높은 회복력
- 유틸 자본 없음(“실제로” 존재하지 않음)

단점

- 초기 단계에서 더 높은 부족 담보(언더콜래터럴라이제이션) 리스크
- PCV를 부실하게 관리할 경우 스테빌리티 풀 자금 부족 발생 가능

리스크에 대하여>About the risk)

각 청산은 스테빌리티 풀에서 인출을 유발하며, 스테빌리티 풀에 약 10%의 이익을 남긴다. 이는 또한, 청산 이후 가격이 최대 10%까지 하락하더라도 스테빌리티 풀이 청산에서 손실을 보지 않을 수 있음을 의미한다. 우리 B.Protocol 연동은 청산된 tBTC가 자동으로 thUSD로 전환되어 스테빌리티 풀에 재예치되도록 보장한다. 정상적인 상황이며 다른 요인이 없다면, 풀에 있는 thUSD 잔액은 시간이 지남에 따라 증가할 것으로 예상된다.

그러나 블랙스완 이벤트 — 짧은 시간에 BTC 가격이 크게 하락하거나 유동성 문제가 발생하는 경우 —에서는, 약 10%의 이익에도 불구하고 손실이 발생할 수 있다. 이는 프로토콜이 언더콜래터럴라이즈드가 될 리스크이지만, 부채가 없더라도(스테빌리티 풀이 수익성이 없을 때) 동일한 문제가 적용된다. 프로토콜은 지속 가능하도록 설계되었으므로, 이러한 종류의 희귀 이벤트는 장기적으로 평균화될 것이다. 또한 Threshold USD의 모든 수익 흐름은 PCV로 귀속되어 언더콜래터럴라이제이션 리스크를 더욱 줄인다.

언더콜래터럴라이제이션은 주로 초기 부트스트래핑 단계에서 우려되는 사안이다. 이자가 누적되어 초기 부채를 상환함에 따라, 스테빌리티 풀의 자금은 완전히 소유된 PCV로 대체되어, 이 단점은 제거된다.

B. 프로토콜(B. Protocol)

B. Protocol은 대출 플랫폼을 보다 안정적으로 만들기 위한 서드파티 탈중앙화 백스톱 유동성 프로토콜이다.

문제(The problem)

Liquity 프로토콜에는 “스테빌리티 풀”이라는 개념이 있다. 스테빌리티 풀의 목적은 Threshold USD(thUSD)를 결제 수단으로 사용하여 청산된 담보(tBTC)를 할인된 가격으로 매수하는 것이다.

사용자들은 thUSD를 스테빌리티 풀에 예치하며, 그들의 자금은 다른 예치자의 자금과 함께 풀링된다. 예를 들어 풀이 900,000 thUSD로 구성되어 있고 한 사용자가 100,000 thUSD를 예치했다면, 해당 사용자는 압류된 담보의 10%에 대한 권리를 갖는다.

스테빌리티 풀의 문제는 청산이 발생할수록 thUSD가 tBTC로 교환되지만, 다시 thUSD로 돌아오지 않는다는 점이다. 그대로 방치하면 풀은 결국 tBTC만으로 구성되어, 더 이상의 청산을 풀에 대해 실행할 수 없게 된다. 더욱이 tBTC 담보를 취득함으로써, 풀 내 예치자의 가치가 BTC 가격에 노출된다.

따라서 사용자는 가격 리스크를 피하기 위해 tBTC를 신속히 thUSD로 매도하도록 유인되지만, Liquity에서는 이 과정이 수동적이다. 사용자는 UI를 직접 열어 tBTC를 인출하고, 이를 thUSD로 매도한 다음, thUSD를 재예치해야 한다. 이는 시간과 가스가 많이 드는 작업으로, 대형 보유자(고래)나 자체 봇을 가진 사용자에게 적합하다.

더 나쁜 점은, 현재의 스테빌리티 풀 모델에서는 DAO가 현실적으로 운영되기 어렵다는 것이다. 자금을 이동·매도하기 위한 투표는 비실용적이고, 비용이 많이 들며, 느리다.

비인간적·알고리즘적·완전 자동화된 방식으로 수익을 복리화(compound)하기 위해 우리는 B.Protocol을 주목한다.

B.Protocol의 구원(B.Protocol to the rescue)

스테빌리티 풀에 직접 예치하는 대신, 우리는 B.Protocol의 래핑 스마트 컨트랙트 인터페이스를 사용할 수 있으며, 이는 모든 사용자(그리고 PCV)를 대신하여 thUSD를 스테빌리티 풀에 예치한다.

청산이 발생하면, 할인된 tBTC는 B.Protocol의 백스톱 AMM(B.AMM)에 의해 자동으로 매도에 부쳐진다. 이는 현재 tBTC 및 thUSD 재고, 그리고 현재 BTC-USD 시장 가격(Chainlink에서 가져옴)을 고려하는 결정적(deterministic) 공식에 따라 수행된다. 매도가 이루어질 때마다, 스마트 컨트랙트는 회수된 thUSD를 스테빌리티 풀에 다시 예치한다.

B.AMM에서 오퍼에 응하는 참가자가 없을 경우, Gelato Keepers가 대중적인 DEX 페어를 통해 차익거래하여 주문을 이행한다.

이 방식으로 PCV는 자금자족이 가능해지고 외부 개입 없이 무기한 운영될 수 있다.

통합 세부 정보(Integration details)

B.Protocol 팀은 Threshold USD와 호환되는 업그레이드 불가능한(non-upgradeable) 풀을 배포할 예정이다.

이 풀은 Chainlink의 BTC/USD 오라클(Threshold USD와 동일)을 사용한다.

풀은 어떠한 이자 농사(yield farming) 애플리케이션에도 유휴 자금을 배치하지 않는다.

Threshold USD의 PCV는 B.Protocol 풀에 대한 스마트 컨트랙트를 화이트리스트에 등록하며, Threshold Network DAO(T DAO)는 투표를 통해 thUSD를 B.Protocol 풀에 예치하는 절차를 개시한다. 예치금은 PCV 스마트 컨트랙트에서 B.Protocol로 이동하며, T DAO가 투표로 승인하는 한, 언제든지 제한 없이 다시 PCV로 이동할 수 있다. 인출 시점에 풀에 tBTC가 존재하는 경우, 해당 tBTC도 PCV로 이전될 수 있다.

B.AMM 컨트랙트의 "A" 파라미터("A"는 증폭 계수로, 값이 높을수록 슬리피지가 작음)는 T DAO와 B.Protocol 간의 공동 소유(co-ownership)를 통해 운영된다. B.Protocol이 "A" 값을 제안하면, T DAO가 이를 승인하거나 거부할 수 있다.

배포 시 디스카운트율은 4%로 설정되며, T DAO와 B.Protocol 간의 공동 거버넌스 메커니즘을 통해 최대 10%까지 조정할 수 있다.

모든 청산 수익은 B.Protocol 풀 내에서 자동 복리화(auto-compound)된다.

키퍼(Keeper)

백업 메커니즘으로서, B.Protocol은 경로를 라우팅할 수 있는 Gelato 키퍼를 배포한다.

예시:

tBTC -> WBTC -> USDC -> thUSD

이 예시에서 자금은 Curve Finance의 풀(스테이블코인 및 래핑된 비트코인 풀 모두)을 통해 라우팅될 수 있다.

또한 자금은 Uniswap(v2 또는 v3)의 WBTC 또는 USDC 페어드 풀을 통해 라우팅될 수도 있다.

기타 가능한 경로는 다음과 같다:

tBTC -> WBTC -> DAI -> thUSD

tBTC -> WBTC -> USDT -> thUSD

키퍼는 DAO의 자금으로 운영되며, 키퍼가 발생시키는 모든 이익은 PCV로 다시 분배된다.

BOB 네트워크에서의 thUSD (thUSD on Build on Bitcoin, BOB)

Threshold USD(thUSD)는 ETH와 tBTC를 담보로 하여 USD에 소프트 페그된 스테이블코인이다. 자세한 내용은 THUSD 개요를 참조하라.

thUSD를 통해 이제 다음이 가능하다:

- 브리징된 tBTC 또는 ETH를 사용하여 BOB 네트워크에서 손쉽게 담보 볼트를 개설
- thUSD를 민팅하고 BOB 네트워크 생태계 전반에서 활용

먼저 선호하는 지갑(예: MetaMask)을 app.gobob.xyz/wallet에서 연결하고, app.gobob.xyz/bridge에서 tBTC를 브리징하라.

BOB 네트워크 연결(Connecting to BOB Network)

1. 지갑 설정 접근

- app.gobob.xyz/wallet로 이동한다.

2. 지갑 연결

- 선호하는 지갑(예: MetaMask)을 선택하고, BOB 네트워크에 연결하기 위한 안내를 따른다.

3. BOB 네트워크로 전환

- “Switch to BOB” 옵션을 클릭한다. 이 작업은 BOB 네트워크를 지갑에 자동으로 추가하고, 지갑을 BOB 네트워크에 연결한다.

4. 수동 설정

- 또는 다음 설정을 사용하여 지갑을 수동으로 구성할 수 있다:
 - Chain ID: 60808
 - Gas Token: ETH
 - RPC URL: <https://rpc.gobob.xyz/>
 - WS URL: <wss://rpc.gobob.xyz>
 - Explorer: <https://explorer.gobob.xyz/>

담보를 BOB 네트워크로 브리징(Bridging Collateral to BOB Network)

지갑에 트랜잭션 수수료를 위한 충분한 ETH가 있는지 확인하라.

Ethereum 메인넷에서 tBTC 또는 ETH를 전송하여 BOB 지갑에 자금을 충전할 수 있다.

참고: BOB에서 thUSD를 민팅하기 위한 최소 금액은 2,000(=1,800 최소 부채 + \$200 청산 준비금) 상당의 tBTC 또는 ETH + 트랜잭션 수수료다.

준비(Preparation)

1. 지갑 설정:

Ethereum 메인넷에 연결된 지갑을 설정하고, 브리징에 사용할 충분한 tBTC 또는 ETH를 보유해야 한다.

브리징 프로세스(Bridging Process)

1. 브리지 인터페이스 접근:

- app.gobob.xyz/bridge에서 BOB 브리지 인터페이스로 이동한다.

2. 지갑 연결:

- Ethereum 메인넷 네트워크에서 지갑을 브리지 인터페이스에 연결한다.

3. tBTC 또는 ETH 선택:

- 브리징할 자산으로 tBTC 또는 ETH를 선택한다.

4. 금액 입력:

- 브리징할 tBTC 또는 ETH의 양을 지정한다.

5. 트랜잭션 확인:

- 수수료를 포함한 트랜잭션 세부 정보를 검토하고 트랜잭션을 확인한다.

6. 트랜잭션 승인:

- 지갑에서 트랜잭션을 승인한다.

7. 확인 대기:

- 트랜잭션이 이더리움 블록체인에서 확정될 때까지 기다린다.

8. 수령 확인:

- 트랜잭션이 확인되면, BOB 네트워크 지갑에서 브리징된 tBTC 또는 ETH의 수령을 확인한다.

참고: 자산을 BOB 네트워크에서 다시 브리징할 때는, 프로세스에 최대 7일이 걸릴 수 있다.

담보 볼트 개설 및 thUSD 민팅

담보 볼트를 개설하고 thUSD를 민팅하는 단계

1. thUSD 앱 인터페이스 접근:
 - app.thresholdusd.org로 이동하여 BOB 네트워크에서 선호하는 지갑을 연결한다.
2. 새로운 볼트 열기:
 - “Borrow(차입)” 메뉴로 이동하여 담보로 사용할 자산(tBTC 또는 ETH)을 선택하고 “Open a Vault(볼트 열기)”를 클릭한다.
3. tBTC 또는 ETH 예치:
 - 담보로 예치할 tBTC 또는 ETH의 양을 지정한다. 예치 금액이 최소 담보 요건인 2,000(=1,800 최소 부채 + \$200 청산 준비금) + 트랜잭션 수수료를 충족해야 한다.
4. 담보 금액 설정:
 - 원하는 담보 금액을 설정한다. 부채의 최소 110%에 해당하는 담보 비율을 충족해야 한다.
5. thUSD 민팅:
 - 담보 및 담보 비율을 기준으로 민팅할 thUSD 양을 입력한다.
 - 담보 금액, 담보 비율, 민팅된 thUSD 등 볼트 세부 정보를 검토한다.
 - 담보로 tBTC를 사용하는 경우, tBTC 사용 권한을 승인한다.
 - 확인 후 트랜잭션을 승인하여 thUSD를 민팅한다.
6. 볼트 관리:
 - app.thresholdusd.org에서 볼트를 모니터링하여 충분히 담보화되어 있는지 확인한다. 담보 및 부채 포지션을 조정하여 담보 비율을 변경하거나 필요 시 thUSD를 상환할 수 있다.

거버넌스(Governance)

Threshold DAO

Threshold는 커뮤니티 중심으로 운영되며, NuCypher와 Keep 네트워크의 참여자들을 포함하는 동명의 DAO에 의해 관리된다. Threshold DAO는 두 개의 주요 기관으로 구성된다: **토큰 보유자 DAO(Tokenholder DAO)**와 **선출 위원회(Elected Council)**.

이 이중 구조의 목표는 대표성을 강화하는 동시에 책임성을 보장하는 것이다. 각 거버넌스 기관은 서로를 견제하며, 행정 정부의 견제와 균형 시스템과 유사한 구조를 갖는다. 또한 각각 고유한 역할과 책임이 거버넌스 구조에 내재되어 있다.

기술적 관점에서 보면, **토큰 보유자 DAO**는 Governor Bravo 거버넌스 모델(특히 OpenZeppelin Governance 기반)을 따른다.

토큰 보유자 DAO는 이더리움 메인넷 주소 0xd101f2B25bCBF992BdF55dB67c104FE7646F5447에 배포되어 있다.

선출 위원회(Elected Council)는 Gnosis Safe 컨트랙트로 구현되어 있으며, 6-of-9 구성으로 이더리움 메인넷 주소 0x9F6e831c8F8939DC0C830C6e492e7cEf4f9C2F5f에 배포되어 있다.

아래는 기술적 아키텍처 다이어그램이다.

거버넌스 프로세스(Governance Process)

성공적인 제안의 라이프사이클

1. 포럼 토론:

Threshold 커뮤니티 구성원이 거버넌스 포럼에 잠재적인 제안을 게시한다. 제안을 게시한 구성원은 포럼 및 Discord의 Meta Governance 토론에 적극 참여하여 제안에 대한 지지를 얻는 것이 권장된다. 포럼에 새 제안을 생성하기 위해 필요한 최소 토큰 보유량은 없다. 커뮤니티 모더레이터는 스팸성 제안을 삭제할 권리를 가진다.

2. 온도 점검(Temperature Check):

제안이 커뮤니티 내에서 충분한 논의와 관심을 얻으면, 오프체인 스냅샷 투표를 통해 온도 점검이 진행된다. 제안이 온도 점검 단계에서 과반수의 지지를 얻으면 다음 단계로 진행할 자격을 갖는다.

3. 제안 생성:

전체 T 토큰 공급의 최소 0.25% 이상의 투표권을 보유한 커뮤니티 구성원이 온체인 제안을 제출한다. 제안은 공식 투표가 시작되기 전 2일간의 지연 기간에 들어간다.

4. 투표 기간:

제안 투표는 10일간 열려 있다. 제안이 충분한 정족수(전체 T 공급량의 최소 1.5%)로 통과되면 다음 단계로 진행된다. 실패하면 제안은 취소된다. 제안 작성자 및 지지자는 수정된 버전을 다시 제출할 수 있으나, 이전 단계의 요건을 충족해야 하며 충분히 달라야 한다.

5. 타임락 기간:

제안이 승인되면, Governor Bravo 스마트 컨트랙트는 추가로 2일의 타임락 지연을 포함한다. 누구나 Governor Bravo 스마트 컨트랙트와 상호작용하여 승인된 제안을 타임락 컨트랙트에 규잉할 수 있다.

6. 실행:

타임락 지연이 끝난 후, 누구나 승인된 제안을 실행할 수 있다.

제안 절차의 예외 사항

• 위원회 거부권(Council veto):

온체인 단계에서 선출 위원회는 어떤 제안이든 거부(veto)할 수 있다. 이는 위험한 제안이 통과된 경우를 대비한 추가 보안 메커니즘이다.

• 늦은 정족수 방지(Late quorum prevention):

10일간의 투표 기간 중, 정족수가 마감 직전에 달성된 경우 거버넌스 공격을 방지하기 위해 자동으로 연장된다. 정족수가 마감 2일 미만 전에 달성되면, 정족수가 달성된 시점으로부터 2일 연장된다.

• 오프체인 제안(Off-chain proposals):

일부 제안은 온체인 조치를 필요로 하지 않는다(예: 위원회 및 길드 선거). 이러한 경우, 5일(일반 제안) 또는 7일(선거 제안) 동안의 Snapshot 투표가 진행되며, 온체인 제안은 포함되지 않는다.

길드(Guilds)

DAO의 주요 거버넌스 기관 외에도, 서로 다른 초점을 가진 세 개의 커뮤니티 주도 길드가 존재한다: **마케팅 길드(Marketing Guild)**, **통합 길드(Integrations Guild)**, **재무 길드(Treasury Guild)**.

각 길드는 선출된 위원회에 의해 운영되며, 정기적인 순환 선거를 통해 구성원이 교체된다.

Discord의 **#dao-contribute** 채널을 통해 길드에 참여하고, 관심 분야와 전문성에 따라 다른 Threshold DAO 구성원들과 협력하라!

재무 길드(Treasury Guild)

Threshold Treasury Guild는 Threshold DAO의 금고를 효과적으로 관리하는 역할을 담당한다. 여기에는 프로토콜 소유 유동성(POL) 확장, 최적의 금고 관리 전략 연구 및 실행, 생태계 유동성 인센티브 집행, 금고 다각화 등이 포함된다.

통합 길드(Integrations Guild)

Threshold Integrations Guild의 핵심 임무는 다른 프로토콜, DAO 및 외부 기관과 성공적이고 지속 가능한 시너지 관계를 구축하는 것이다.

마케팅 길드(Marketing Guild)

Threshold Marketing Guild는 Threshold의 전반적인 마케팅, 기여자 네트워크 확장, 신규 회원 온보딩, Threshold의 가치·서비스·사용 사례에 대한 교육 등을 담당한다.

Threshold DAO 규칙

이 공간은 DAO의 규칙, 가이드라인, 그리고 우리가 업무 방식을 개선하기 위해 추진 중인 모든 노력을 통합하기 위한 것이다.

DAO 규칙(DAO Rules)

DAO의 창립 규칙(Inaugural Rules for the DAO)

DAO 규칙은 DAO 설립 시 함께 제정되었으며, 대부분 포럼에 반영되어 있다. 초기 규칙으로는 TIP-002, TIP-007, TIP-013, TIP-020, TIP-026, TIP-032를 참조한다.

TIP-002: Threshold Network DAO 제안 – v2

Matt Luongo가 작성한 TIP-002는 DAO의 설립, 구성 기관, 그리고 구성원 간의 상호 작용 방식을 설명한다.

TIP-007: 네트워크 제네시스 시 최소 스테이크 크기 40,000 T

Arj가 작성한 TIP-007은 Threshold Network 스테이커가 네트워크 제네시스 시점에 보유해야 하는 최소 스테이크 크기 요건을 설명한다.

TIP-013: Threshold DAO 길드 부트스트래핑

Will이 작성한 TIP-013은 DAO 길드의 설립 및 내부 운영 방식을 설명한다.

TIP-020: 임시 시대 인센티브 구조: (1) 일회성 마이그레이션+스테이크 보너스 및 (2) 지속적인 안정 수익

Arj가 작성한 TIP-020은 임시 시대 동안 Threshold Network 스테이커에 대한 인센티브를 설명한다.

TIP-026: Threshold 개선 제안서(TIP): 절차 및 템플릿

Will이 작성한 TIP-026은 거버넌스 프로세스를 정의하고, 새로운 TIP을 작성할 때 따라야 할 템플릿을 만든다.

TIP-032: 위원회 결정: tBTCv2 및 PRE 간 보상 배분(총 목표 APY = 15%)

Arj가 작성한 TIP-032는 TIP-020을 대체하며, DAO 제품 간 스테이커 보상 배분을 설정한다.

길드 및 제안 관리 규칙(Rules for Guilds and Proposals Management)

2022년, DAO는 거버넌스 프로세스를 개선하기 위한 노력을 주도했고, 여러 DAO 규칙의 제정 및 투표로 이어졌다. 이 작업은 각 길드에서 3명의 자원봉사자와 DAO PM이 참여한 **규칙 소위원회(Rules Subcommittee)**에 의해 주도되었다. 결과물로 TIP-031과 TIP-034가 제정되었다.

TIP-031: 길드 위원회 선거 및 운영 규칙

규칙 위원회가 작성한 TIP-031은 DAO 길드의 선거 및 운영 규칙을 수립한다.

TIP-034: 신규 제안 규칙

규칙 위원회가 작성한 TIP-034는 TIP-026을 확장하여, DAO 제안 작성 방식에 대한 보다 구체적인 기준과 모범 사례를 제시한다.

GP-021: 통합 길드 위원회 의석 수를 5석에서 7석으로 확대

ZeroInfo가 작성한 GP-021은 통합 길드 위원회의 의석을 2석 늘리는 내용을 담고 있다.

TIP-049: 마케팅 길드 위원회 구조 조정

John Packel이 작성한 TIP-049는 마케팅 길드 위원회의 재구조화에 대해 설명한다.

추가 선거 규칙(Additional Rules for Elections)

TC-003: 제3기 위원회 선거 회고 및 교훈

Luna5가 작성한 TC-003은 3기 위원회 선거를 길드 선거와 3월로 정렬시키고, 위원회의 교차(staggered) 선거를 제거한다.

투표 위임(Vote Delegation)

DAO 거버넌스에 참여하기 위해, 토큰 보유자는 거버넌스 위임 주소를 설정해야 한다.

투표 위임은 토큰 보유자가 자신의 투표 가중치를 사용해 대리인(delegate)에게 투표 권한을 부여하는 과정이다.

대리인은 자신(self-delegation)일 수도 있고 제3자일 수도 있다. 설정된 위임자는 언제든지 변경하거나 취소할 수 있다.

위임은 자산의 수탁권 이전이 아닌, 자산이 Threshold DAO 내에서 표현하는 **투표 가중치의 위임**만을 의미한다.

제3자 위임(Third-Party Delegation)

제3자 대리인은 Threshold 거버넌스에 적극적으로 참여하며, DAO의 주요 결정에 더 큰 영향력을 행사하기를 원하는 자원봉사자다.

이들은 다른 Threshold 토큰 보유자 및 스테이커가 투표 가중치를 위임할 수 있는 ETH 주소를 제공한다.

이후 제3자 대리인은 자신에게 위임된 투표 가중치를 사용하여 Threshold 거버넌스 제안에 대해 투표할 책임을 갖는다.

거버넌스 제안, 토론, 투표에 적극적으로 참여할 의향이 없거나 관심이 없는 커뮤니티 구성원은, Threshold에 헌신을 보여준 활동적인 DAO 구성원에게 투표를 위임할 수 있다.

이를 통해 토큰 보유자와 스테이커는 일상적인 거버넌스 활동에 직접 참여하지 않고도 DAO에 간접적으로 의견을 반영할 수 있다.

대리인으로 활동하고자 하는 커뮤니티 구성원은 이곳에서 직접 자천(self-nominate)할 수 있다.

제3자 대리인의 거버넌스 참여에 대한 보상은 없다.

유동 토큰 위임 절차는 아래 섹션에 설명되어 있다.

현재 AMM 풀(예: Curve)에 LP로 예치된 토큰은 위임할 수 없지만, 이는 향후 개선될 영역이다.

유동 토큰 위임(Liquid Token Delegation)

유동 T 토큰 위임 방법

유동 T 보유자는 자신 또는 제3자에게 투표 가중치를 위임하여 거버넌스 제안에 대한 투표를 위임할 수 있다.

위임은 ETH 가스비가 필요한 온체인 트랜잭션을 통해 이루어진다.

1. <https://boardroom.io/threshold>로 이동한다.
2. 지갑을 연결한다.
3. “Set Up Delegation(위임 설정)”을 클릭한다.

4. “Delegation Type(위임 유형)”을 선택한다 — 자신 또는 제3자에게 위임할 수 있다.

5. “Delegate Address(위임 주소)”를 입력하고 “Delegate Votes(투표 위임)”을 클릭한다.

6. 트랜잭션에 서명한다.

스테이킹 및 노드 실행(Staking & Running a Node)

tBTC v2 노드 설정(tBTC v2 Node Setup)

이 문서는 tBTC v2 스테이킹 클라이언트의 기본 설치 및 설정 방법을 설명한다.
이는 자체적으로 tBTC v2 노드를 운영하고자 하는 커뮤니티 구성원을 위한 문서다.

노드 운영은 간단하지 않으며, 네트워크 가용성과 업타임을 유지하기 위한 기술적 능력과 헌신이 필요함을 명심해야 한다.
일반적인 설정 과정을 숙지하기 위해, 노드 설정을 시작하기 전에 본 문서를 전체적으로 검토하기 바란다.

중요 고려 사항(Important Considerations)

Threshold Network는 네트워크에서 실행 중인 각 노드가 특정한 역량을 갖추기를 기대한다.
이러한 역량을 충족하기 위해 다음 기준을 고려하라:

- **네트워크 가용성:**
tBTC v2 노드는 네트워크에 항상 연결되어 있어야 한다. 안정적이고 이중화된 인터넷 연결을 강력히 권장한다.
- **기계 업타임과 신뢰성:**
가상 사설 서버(VPS) 사용을 권장한다.
- **이더리움 노드 연결:**
프로덕션 수준의 자체 호스팅 또는 서드파티 이더리움 노드 배포와의 연결이 필요하다.
- **지속적이고 이중화된 스토리지:**
VM 또는 컨테이너 재시작 및 디스크 오류 발생 시에도 데이터를 보존할 수 있어야 한다.
- **고유한 오퍼레이터 계정:**
네트워크에서 실행되는 각 노드는 고유한 이더리움 오퍼레이터 계정을 필요로 하며, 해당 계정은 항상 양의 이더 잔액을 유지해야 한다.
- **고유한 IP 또는 포트:**
네트워크의 각 노드는 고유한 IP 주소 또는 동일 IP 내에서 고유한 애플리케이션 포트를 사용해야 한다.

권장 머신 유형(Recommended Machine Types)

클라이언트를 로컬 머신에서 실행하는 것도 가능하지만, 권장되지는 않는다.

최종적으로 운영 환경이 어떤 머신 유형을 선택할지 결정하게 된다. 이는 특히 여러 애플리케이션이 VM 리소스를 공유하는 컨테이너화된 솔루션을 실행하는 경우에 관련성이 높다. 아래 유형들은 tBTC v2 노드 한 인스턴스를 실행하기에 충분하다.

선호되는 OS는 Ubuntu다.

VPS Provider	VPS Type
AWS	c5.large
Azure	F2s v2
Google Cloud	n2-highcpu-2
Self-hosted	2 vCPU / 2 GB RAM / 1 GiB Persistent Storage

Ethereum API

Keep 노드는 WebSocket Ethereum API에 대한 연결이 필요하다. 서비스 제공업체(예: Alchemy, Infura, Ankr)로부터 WS API URL을 발급받거나, 자체 이더리움 노드(예: Geth)를 운영해야 한다.

Bitcoin API

버전 v2.0.0-m3부터, Keep 노드는 Electrum 프로토콜 서버를 통해 비트코인 네트워크와 상호작용한다. 공개적으로 사용 가능한 서버 중 하나를 사용하거나 자체 서버를 운영할 수 있다. 선택한 서버의 URL은 구성의 `bitcoin.electrum` 섹션에 전달되어야 한다. `bitcoin.electrum` 구성 섹션에 Electrum 서버가 명시적으로 설정되지 않은 경우, Keep 노드는 현재 실행 중인 비트코인 네트워크에 적합한 내장 서버 목록에서 무작위로 하나를 선택한다.

구성(Configuration)

클라이언트는 구성 옵션이 CLI 플래그로 전달되거나 구성 파일에 지정되기를 기대한다. 명령줄 매개변수를 사용하여 옵션을 지정한 경우, 이는 구성 파일에서 읽은 값을 재정의한다.

오퍼레이터 계정(Operator Account)

tBTC v2 스테이킹 클라이언트를 설치할 수 있도록 머신을 준비하라

클라이언트가 이더리움 체인에 연결하려면 오퍼레이터 계정의 이더리움 키 파일이 필요하다. 이 계정은 이후 단계에서 Geth(GoEthereum)를 사용하여 생성된다.

이더리움 키 파일은 비밀번호로 암호화되어야 한다. 비밀번호는 클라이언트 시작 후 프롬프트에서 제공하거나 `KEEP_ETHEREUM_PASSWORD` 환경 변수로 구성해야 한다.

오퍼레이터 계정은 항상 양의 이더 잔액을 유지해야 한다. 계정을 모니터링하고 잔액이 0.5 ETH 아래로 떨어지면 즉시 충전할 것을 강력히 권장한다.

TACo 또는 기타 애플리케이션에 사용 중인 오퍼레이터 계정을 재사용하지 말 것.

Geth(GoEthereum) 설치

새 이더리움 계정을 생성하려면 Geth(GoEthereum)를 설치하고 아래 명령을 사용해 새 계정을 생성하라. 이 계정은 이후 오퍼레이터 계정으로 언급된다.

Copy

```
geth account new --keystore /home/$USER/.operator-key
```

프롬프트가 표시되면, 오퍼레이터 키 파일을 보호하기 위한 비밀번호를 입력하라.

비밀번호 관리자를 사용하여 강력한 비밀번호를 생성하고 안전하게 보관하라. 설정 과정에서 다시 필요하다.

다음 문자를 포함하는 비밀번호는 피하라: ', ", ` , \$

이러한 문자는 구성의 일부로 해석되어, 수정에 많은 시간이 소요될 수 있는 바람직하지 않은 결과를 초래할 수 있다.

프로세스가 완료되면 공개키가 표시된다. 오퍼레이터 계정 공개키를 기록해 두라.

오퍼레이터 계정의 비밀번호를 절대 잃어버리지 말 것.

오퍼레이터 계정에 자금 공급

tBTC v2 노드의 원활한 작동과 가용성을 보장하기 위해 오퍼레이터 계정은 항상 양의 ETH 잔액을 유지해야 한다.

애플리케이션 승인 및 오퍼레이터 등록(Application Authorization & Operator Registration)

다음은 tBTC v2에 대한 애플리케이션을 승인하고 Threshold 대시보드를 통해 오퍼레이터 주소를 등록하는 방법을 보여준다.

Threshold 네트워크에서 노드를 운영하기 위한 중요한 단계는 적절한 애플리케이션 승인과 오퍼레이터 계정 등록이다. 애플리케이션 승인은 한 번만 수행하면 된다.

매우 중요: tBTC 애플리케이션과 Random Beacon 애플리케이션 **둘 다** 승인이 되어야 한다. 두 애플리케이션이 올바르게 승인되지 않으면 노드를 배포할 수 없다.

주의: 이러한 애플리케이션을 승인하면, 해당 애플리케이션에 스테이킹한 T에 대해 45일의 언본딩 기간이 발효된다. 이 냉각 기간은 언스테이크 요청을 제출한 날부터 시작된다.

애플리케이션 승인(Application Authorization)

먼저 Threshold 대시보드로 이동하여 지갑을 연결하라.

"Configure Apps"를 클릭하라.

tBTC와 Random Beacon 애플리케이션 **둘 다**를 선택하고 애플리케이션별로 스테이킹할 T의 원하는 양을 입력하라. 최소치는 40,000 T임에 유의하라.

오퍼레이터 등록(Operator Registration)

오퍼레이터 계정은 노드에서 생성된 이더리움 계정이다. 네트워크가 노드의 T 스테이크를 노드와 연계하기 위해서는, 오퍼레이터 주소를 등록해야 한다.

두 애플리케이션 승인이 완료되면, "Start Mapping"을 클릭하여 오퍼레이터 등록 절차를 시작하라.

제공된 입력란에 오퍼레이터 주소를 입력하고 "Map Address"를 클릭하라.

위 단계가 모두 성공적으로 완료되면, 노드 배포 프로세스의 다음 단계로 진행할 준비가 된 것이다.

잊지 말 것: tBTC v2 노드는 tBTC와 Random Beacon 애플리케이션을 **모두** 성공적으로 승인하고, 먼저 노드의 오퍼레이터 주소를 등록하지 않으면 배포할 수 없다.

네트워크 구성

tBTC v2 스테이킹 클라이언트를 위한 필수 네트워크 구성입니다.

필수 포트

노드는 부트스트랩 노드 및 탐색된 피어와의 연결을 설정하고 유지하기 위해 공개적으로 접근 가능해야 합니다. 노드는 네트워크 상태 모니터링 목적을 위한 메트릭 및 진단 서비스를 노출합니다. 다음 포트에 대해 애플리케이션 수준 방화벽을 포함하여 필요에 따라 방화벽 규칙을 업데이트하십시오.

Purpose	Config Property	Protocol	Default
Network	network.port	TCP	3919
Status	clientInfo.port	TCP	9601

공표 주소(Announced Addresses)

공표 주소는 피어가 사용자의 노드에 연결하는 데 사용하는 Threshold Network에 공표되는 계층화된 주소 정보(멀티어드레스/multiaddr)입니다. 예: /dns4/bootstrap-0.test.keep.network/tcp/3919 또는 /ip4/104.154.61.116/tcp/3919.

노드를 실행 중인 머신이 공용 IP를 노출하지 않는 경우(예: NAT 뒤에 있는 경우) network. AnnouncedAddresses(플래그: --network. announcedAddresses) 구성 속성을 퍼블릭이 사용자의 노드에 도달할 수 있는 주소(ip4 또는 dns4)로 설정해야 합니다.

멀티어드레스에 대한 자세한 내용은 libp2p 문서를 참조하십시오.

데이터 저장

클라이언트를 위한 영속적 데이터 디렉토리를 설정하십시오.

클라이언트는 두 개의 영속적 디렉토리를 필요로 합니다. 이 디렉터리에는 클라이언트가 생성하고 사용하는 구성 파일과 데이터가 저장됩니다. 이러한 디렉터리는 자주 백업할 것을 강력히 권장합니다. 이 데이터를 잃으면 치명적일 수 있으며 슬래싱으로 이어질 수 있습니다.

데이터 디렉터리가 지속되고 정기적으로 백업되도록 보장하는 것이 매우 중요합니다.

tBTC v2 클라이언트를 위한 폴더 생성

```
cd /home/$USER/  
mkdir keep  
cd keep  
mkdir storage config
```

tBTC v2 클라이언트는 storage 디렉터리 내에 두 개의 하위 디렉터리인 keystore 및 work를 생성합니다. 이를 수동으로 만들 필요는 없습니다.

keystore 하위 디렉터리에는 클라이언트가 생성한 민감한 키 자료 데이터가 포함됩니다. keystore 데이터를 분실하는 것은 심각한 프로토콜 위반이며 슬래싱 및 잠재적인 자금 손실로 이어집니다.

어떠한 상황에서도 keystore 데이터가 손실되지 않도록 보장하는 것은 운영자의 책임입니다.

work 디렉터리에는 클라이언트가 생성한 데이터가 포함되며, 이는 클라이언트 재시작 또는 재배포 시에도 유지되어야 합니다. work 데이터가 손실되더라도 클라이언트가 이를 재생성할 수는 있지만, 작업 완료에 시간이 필요하여 불편하며 보상 손실로 이어질 수 있습니다.

오퍼레이터 keystore 파일 복사

오퍼레이터 계정 생성 단계에서 제공된 명령으로 루트 사용자에게 대해 Geth가 설치되었다고 가정하면, operator-key 파일은 /.operator-key 디렉터리에 위치해야 합니다.

```
cd /home/$USER/.operator-key
```

operator-key 디렉터리에는 계정 키 파일(오퍼레이터 키 파일)이 포함되어 있으며, 이름은 다음과 유사합니다:

```
UTC--2018-11-01T06-23-57.810787758Z--fa3da235947aab49d439f3bcb46effd1a7237e32
```

위에서 만든 config 디렉터리로 이 계정 키 파일을 **복사**(이동 아님!) 하십시오.

```
ls -la
cp name_of_account_key_file /home/$USER/keep/config/name_of_account_key_file
```

tBTC 베타 스테이커 프로그램

tBTC 베타 스테이커 프로그램 소개

tBTC 유틸리티 부트스트래핑의 일환으로, Threshold Network는 점진적 탈중앙화 동안 시스템 연속성을 보장하기 위해 tBTC 민팅 및 상환에 참여할 수 있도록 권한 부여된 스테이커를 허용 목록에 추가합니다. 이 허용 목록에 오른 스테이커를 베타 스테이커(Beta Stakers)라고 합니다. 베타 스테이커 프로그램의 목표는 초기 성장 기간 동안 핵심 운영이 중단 없이 제대로 수행되도록 보장하는 것입니다.

이는 ‘점진적 탈중앙화’의 한 형태이지만, 더 많은 독립적인 스테이커를 허용 목록에 추가하는 방식으로 탈중앙화의 깊이를 확대할 수 있는 명확하고 단순하며 이미 배포된 경로가 있다는 점에 유의하십시오.

최신 컨트랙트 조회 기준 현재 베타 스테이커는 35명으로, 2023년 11월에 보고된 20명에서 증가했습니다. 몇몇 주목할 만한 전문 스테이킹 제공자가 이곳에서 DAO 승인을 요청한 것을 확인할 수 있습니다.

현재 베타 스테이커 수를 확인하려면 Etherscan의 컨트랙트 페이지를 방문하십시오.

베타 스테이커 노드는 BTC를 커스터디하는 tBTC 지갑을 생성하는 책임이 있는 퍼미션드 세트를 구성합니다. tBTC 베타 스테이커 노드를 운영하는 것은 상당한 커밋먼트가 필요하며 특정 요구사항이 있습니다. 이 문서는 그러한 요구사항, 기술적 권장 사항, 그리고 베타 스테이커 tBTC 노드를 운영하는 데 드는 잠재적 비용을 강조하는 것을 목표로 합니다.

현재 노드 활동 및 전체 네트워크 상태에 대한 최신 정보를 확인하려면 tbtcscan.com/operators 를 방문하거나 status.threshold.network 를 확인하십시오. 이 리소스는 노드 수, 스테이크 분포 및 운영 지표에 대한 최신 통계를 제공합니다.

일반 요구사항

베타 스테이커 노드를 운영하는 것은 장기적 커밋먼트입니다. 특정 노드가 베타 스테이커 세트에 추가되면 베타 스테이커 프로그램 종료 시점(약 12개월)까지 운영을 유지해야 합니다.

베타 스테이커 노드 운영자는 특히 소프트웨어 기여자가 요청한 업그레이드와 관련하여 매우 신속하게 대응해야 합니다. 이상적으로는 통지 후 24시간 이내에 노드를 업그레이드할 수 있어야 합니다.

베타 스테이커 노드 운영자는 기술적으로 역량을 갖추어야 합니다. 노드의 고가용성(업타임 96% 초과)과 보안을 보장할 책임이 있습니다.

기술 요구사항

베타 스테이커 노드는 표준 노드에 비해 더 계산 집약적인 작업(DKG, 임계값 서명 등)을 수행합니다. 높은 수준의 서비스를 보장하기 위해 베타 스테이커 노드는 다음 사양의 머신을 필요로 합니다:

- 4 CPUs
- 4 GB of RAM
- 1 GB of persistent disk space
- 80 Mbps of network bandwidth
- Linux OS

위 사항에 추가로:

- 기본 머신의 운영체제와 도구는 최신 보안 패치를 포함하여 최신 상태여야 합니다.
- 영속 디스크의 백업은 지속적으로 수행되어야 합니다. 이는 미션 크리티컬 데이터(예: 키 자료)의 안전을 보장하는 데 매우 중요합니다. 백업에 추가 암호화 계층을 사용하는 것을 강력히 권장합니다.
- 네트워크 계층은 노드가 외부 네트워크에서 도달 가능하도록 고유한 공용 IPv4 주소를 제공해야 합니다. 올바른 방화벽 구성이 마련되어 두 포트(통신 및 진단)로의 인바운드 트래픽만 허용하는 안전한 경계를 보장해야 합니다. 인터넷 연결은 안정적이어야 하며, 장애 조치 시나리오를 고려해야 합니다.
- 베타 스테이커 노드는 이더리움 노드에 대한 접근이 필요합니다. 개인 이더리움 스택(예: Geth + Prysm)을 설정하고 퍼블릭 제공자(예: Alchemy, Infura 등)를 페일오버로 사용하는 것을 강력히 권장합니다. 이러한 설정은 퍼블릭 제공자와 관련된 단일 장애 지점 위험을 피하는 데 도움이 되므로 네트워크 다양성과 탈중앙화에 매우 중요합니다. 베타 스테이커 운영자는 스택 구성 요소 선택에 있어 자체 판단을 사용해야 합니다. 개인 이더리움 스택의 구체적 기술 요구사항은 사용되는 소프트웨어에 따라 다릅니다. 예를 들어 Geth + Prysm 기반 스택은 4 CPU / 16 GB RAM / 2 TB SSD가 필요합니다.
- 베타 스테이커 노드는 비트코인과 상호작용하기 위해 Electrum 프로토콜 서버가 필요합니다. Electrum 서버(예: Fulcrum, ElectrumX, Electrs 등)와 비트코인 노드(예: Bitcoin Core)로 구성된 개인 스택을 설정하고 퍼블릭 서버를 페일오버로 사용하는 것을 강력히 권장합니다. 그 이유는 개인 이더리움 스택의 경우와 정확히 동일합니다. 베타 스테이커 운영자는 스택 구성 요소 선택에 있어 자체 판단을 사용해야 합니다. 개인 비트코인 스택의 구체적 기술 요구사항은 사용되는 소프트웨어에 따라 다릅니다. 예를 들어 Fulcrum + Bitcoin Core 기반 스택은 8 CPU / 16 GB RAM / 2 TB SSD가 필요합니다.
- 가시성 및 알림을 보장하기 위해 개인 모니터링 스택을 설정하는 것을 강력히 권장합니다. 모니터링 시스템은 노드 자체뿐 아니라 이더리움 및 비트코인 스택도 감독해야 합니다. 베타 스테이커 운영자는 스택 구성 요소 선택에 있어 자체 판단을 사용해야 합니다. 모니터링 스택의 구체적 기술 요구사항은 사용되는 소프트웨어에 따라 다릅니다. 예를 들어 Grafana + Prometheus 기반 스택은 2 CPU / 4 GB RAM / 20 GB HDD가 필요합니다.

비용 추정(Cost Estimation)

베타 스테이커 노드를 운영하는 실제 월간 비용은 호스팅 모델(VPS vs 자체 호스팅)과 인프라 구성에 따라 달라집니다.

다음 추정치는 대략적인 개요를 제공하기 위한 것입니다.

또한, 앞서 언급된 모든 기술적 요구사항 및 권장 사항이 고려되었다고 가정합니다.

주요 시스템 가정(Key System Assumptions)

- 베타 스테이커 노드: 4 CPU / 4 GB RAM / 1 GB HDD
- 이더리움 스택: 4 CPU / 16 GB RAM / 2 TB SSD
- 비트코인 스택: 8 CPU / 16 GB RAM / 2 TB SSD

- 모니터링 스택: 2 CPU / 4 GB RAM / 20 GB HDD
- 백업용 외부 스토리지(노드 및 보조 스택): 1 TB HDD
- 네트워크 계층: 100 Mbps 대역폭, 방화벽 및 공용 IP 포함

위 가정에 따라 비용은 다음 네 가지 범주로 나눌 수 있습니다.

1. 컴퓨팅 비용(Computing Costs):

18개의 CPU와 40 GB RAM을 실행하는 비용을 포함합니다.
여러 구성 옵션이 존재하지만, VPS 기반 모델을 예로 들면
주요 클라우드 서비스 제공업체에서 8CPU/16GB VM 3대를 운영할 경우
월 비용은 약 **\$400/월**부터 시작합니다.

2. 스토리지 비용(Storage Costs):

총 4 TB SSD 및 약 1 TB HDD 사용에 따른 비용을 포함합니다.
VPS 기반 모델에서는 일부 스토리지 비용이 VM 요금에 포함되지만,
일부 제공업체는 GB당 약 0.08(예: *Amazon EBS*)로 별도 요금을 부과합니다. 이러한 경우 스토리지 비용은 * *
200/월**부터 시작한다고 가정할 수 있습니다.

3. 네트워크 비용(Network Costs):

100 Mbps 대역폭, 방화벽, 공용 IP 등의 네트워크 관련 비용을 포함합니다.
VPS 모델에서는 대부분 기본적으로 대역폭이 제공되지만,
방화벽 및 공용 IP는 별도로 과금될 수 있습니다.
일부 제공업체는 송신(egress) 트래픽에 추가 요금을 부과할 수 있습니다.
안전하게 **\$50/월**부터 시작한다고 가정할 수 있습니다.

4. 기타 비용(Other Costs):

호스팅 모델 및 인프라 구성에 따라 달라지는 유지보수 및 기타 비용을 포함합니다.
VPS 모델에서는 OS 라이선스, 자동 백업, 관리 도구 등이 해당됩니다.
자체 호스팅 모델에서는 인터넷 요금, 전원 백업(UPS),
추가 네트워크 장비 등의 비용이 이에 포함됩니다.
이러한 비용은 전체 월간 비용에 반드시 반영되어야 합니다.

결론(Bottom Line)

요약하면, VPS 기반 모델을 사용한 베타 스테이커 노드 운영 비용은
약 **\$650/월**부터 시작합니다.

기타 비용에 대한 안전 마진을 고려하면, 기술적 요구사항 및 권장사항을 충족하는
구성의 대략적인 총 비용은 약 **\$800/월**로 추정됩니다.

자체 호스팅 모델의 일반적인 비용은 구성의 다양성 때문에 단순히 추정하기 어렵습니다.
전체 월간 비용은 VPS 모델과 유사할 수 있으나,
하드웨어 유지보수 등 추가적인 숨은 비용이 발생할 수도 있습니다.

면책(Disclaimer)

위 가정 및 수치는 인프라 비용의 일반적인 감을 제공하기 위한 참고용일 뿐이며,
각 베타 스테이커 노드 운영자는 자신의 환경에 맞추어 직접 비용을 산정해야 합니다.

마지막으로, 본 추정치는 tBTC 노드 운영과 관련된 **인프라 비용만**을 포함합니다.
인건비 및 운영 인력 비용은 포함되지 않았으며,
각 베타 스테이커 운영자는 이를 별도로 고려해야 합니다.

리소스(Resources)

T 토큰

T 토큰은 tBTC를 구동하는 ERC-20 토큰이며, Threshold Network의 가치 축적 자산(value accrual asset) 역할을 합니다. 또한 Threshold DAO의 거버넌스 토큰으로서, 커뮤니티가 네트워크 운영과 관련된 의사 결정을 집단적으로 내릴 수 있도록 합니다.

공급량(Supply)

초기 T 공급량은 DAO 출범 시 100억 T로 설정되었으며, 다음과 같이 분배되었습니다:

- 45억 T: NU 토큰 보유자에게 배정
- 45억 T: KEEP 토큰 보유자에게 배정
- 10억 T: Threshold DAO 금고에 배정

이후 인플레이션 부트스트래핑 단계에서 스테이커 및 노드 운영자 인센티브로 11.55억 T가 추가 발행되어, 최종 총 공급량은 11,155,000,000 T가 되었습니다.

공급 관련 API 엔드포인트(Supply Endpoints)

- 전체 API 엔드포인트: <https://api.threshold.network/supply/t>
- 세부 항목:
 - Total Supply: <https://api.threshold.network/supply/t/total>
 - Circulating Supply: <https://api.threshold.network/supply/t/circulating>
 - Treasury Supply: <https://api.threshold.network/supply/t/treasury>

크로스체인 배포(Cross-Chain Presence)

T 토큰은 네트워크 중립적(network-agnostic)으로 설계되어, 여러 블록체인 간 원활하게 이동할 수 있습니다. 이 멀티체인 접근 방식은 T의 DeFi 내 접근성을 확장하고, 유동성을 개선하며, 보다 견고한 생태계를 조성하는 데 기여합니다.

아래는 각 지원 체인에서의 T 토큰 공식 컨트랙트 주소입니다:

블록체인	컨트랙트 주소	탐색기
Ethereum Mainnet	0xcdf7028ceab81fa0c6971208e83fa7872994bee5	Etherscan
Base	0x26f3901ac8a79c50fb0d8289c74f0d09adc42e29	BaseScan
Optimism	0x747e42eb0591547a0ab429b3627816208c734ea7	Optimistic Etherscan
Solana	4Njvi3928U3figEF5tf8xvjLC5GqUN33oe4XTJNe7xXC	Solscan