퍼퍼(Puffer)

> *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.*

소개 (Introduction)

퍼퍼 소개
퍼퍼는 아이겐레이어 위에 구축된 탈중앙화 네이티브 리퀴드 리스테이킹 프로토콜(nLRP)입니다 🧑‍🤝‍🧑🟣

이를 통해 아이겐레이어에서 네이티브 리스테이킹을 보다 쉽게 접근할 수 있으며, 누구나 이더리움 지분증명(PoS) 검증자를 운영하면서 보상을 극대화할 수 있습니다.

퍼퍼가 제공하는 것 🍽️

프로토콜

- 🟢 퍼미션리스: 누구나 퍼퍼에서 검증자를 운영할 수 있습니다.
- 💅 네이티브 리스테이킹: 아이겐레이어 상 최초의 네이티브 리퀴드 리스테이킹 프로토콜.
- 🧢 이더리움 보호: 프로토콜은 이더리움을 보호하기 위해 자체 상한(self-cap)을 설정합니다.
- 🧑‍🌾 폭발적 성장: 검증자 대기열이 길더라도 pufETH는 가치가 성장할 수 있습니다.

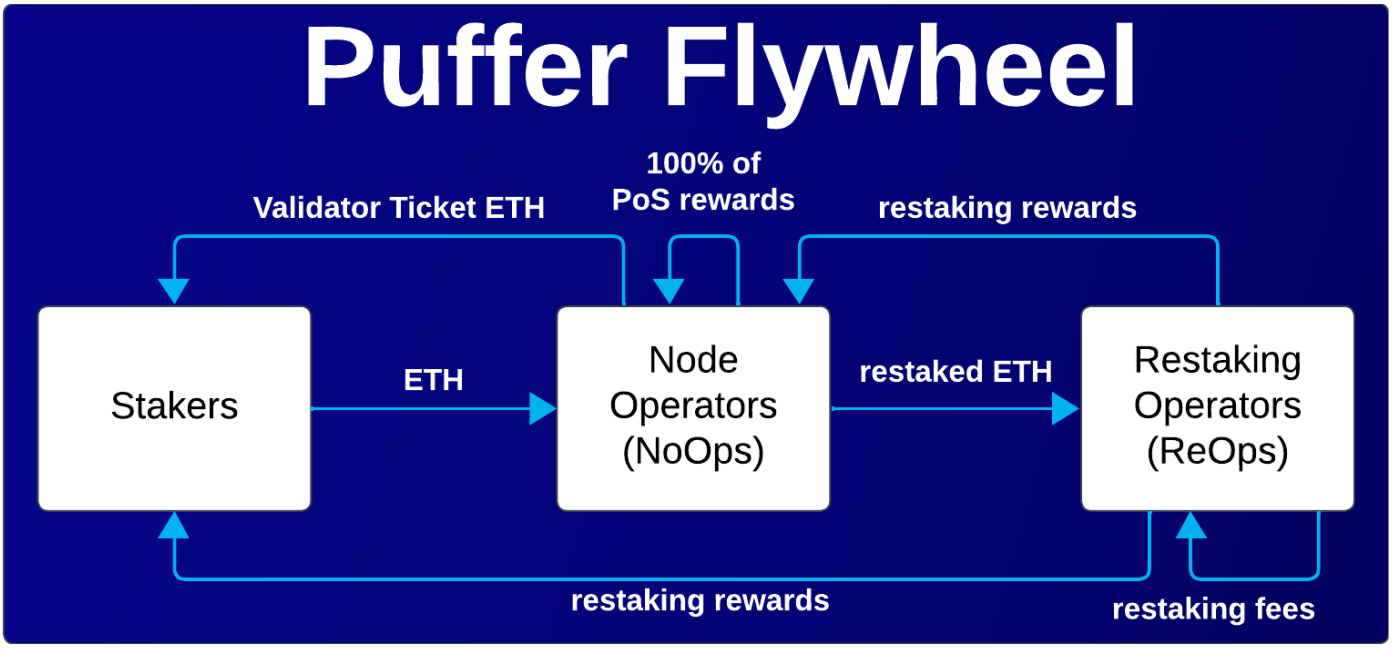
노드 운영자

- 💯 자본 효율성: 2 ETH만으로 검증자를 운영할 수 있습니다.
- 🦕 슬래시 보호: 최초의 하드웨어 기반 안티-슬래싱 지원.
- 🎲 MEV 자율성: 노드운영자(NoOps)는 자신의 MEV 전략을 선택할 수 있습니다.

보상

- 💦 리퀴드 스테이킹: 누구나 원하는 ETH 양을 스테이킹할 수 있습니다.
- 🚀 리스테이킹 보상: 아이겐레이어 통합으로 보상이 극대화됩니다.
- 🎟️ 검증자 티켓: 노드운영자 인센티브를 조정하고, MEV를 완화하며 새로운 시장을 창출합니다.
- 💧 리퀴드 보상: 노드 운영자의 실행 보상은 즉시 유동화됩니다.
- 😎 Buy and Hodl: 검증자 운영 없이도 PoS 및 리스테이킹 보상을 획득할 수 있습니다.

퍼퍼 플라이휠 🎡



스테이커와 노드 운영자는 함께 플라이휠 효과를 만들어내며, 이를 통해 퍼퍼는 기존 리퀴드 스테이킹 프로토콜보다 빠르게 성장할 수 있습니다. 그러나 **퍼퍼가 이더리움의 신뢰할 수 있는 중립성에 위협이 되지 않도록, 버스트 임계치가 검증자 세트의 22%로 제한됩니다.**

프로토콜은 **스테이커(Stakers)** 와 **노드 운영자(NoOps)** 에 의해 구동됩니다:

- **노드 운영자**는 2 ETH를 담보로 하고 검증자 티켓을 잠금으로써 어떤 퍼퍼 모듈에도 참여할 수 있습니다. 그 대가로 32 ETH 검증자를 운영하고, 티켓이 소진될 때까지 100%의 PoS 보상을 유지합니다. 또한 노드 운영자는 리스테이킹 모듈에 참여하고 검증자의 ETH를 리스테이킹 운영자에게 위임하여 리스테이킹 보상 수수료를 받음으로써 보상을 높일 수 있습니다.
- **스테이커**는 ETH를 어떤 양이든 예치하여 프로토콜의 32 ETH 노드 운영 제어 검증자를 자금 지원할 수 있습니다. 그 대가로, 프로토콜이 검증자 티켓을 발행하고 리스테이킹 보상을 받을 때 가치가 상승하는 pufETH 네이티브 리퀴드 리스테이킹 토큰 (nLRT)을 받습니다.

왜 노드 운영자가 되어야 하는가? 🤖

누구든 2 ETH만 있으면 자신만의 검증자를 운영하여 지속적인 PoS 보상을 얻고, 동시에 이더리움의 탈중앙화를 돕는 기여를 할 수 있습니다. 노드 운영자는 32 ETH가 없어도 추가 보상을 위한 리스테이킹 노출을 확보할 수 있어, 단독 검증자로서보다 몇 배 더 많은 보상을 얻을 수 있습니다.

💡 **TIP**
퍼퍼는 퍼미션리스 리퀴드 스테이킹 프로토콜 중 최고의 자본 효율성을 갖추고 있으며, 이는 리스테이킹에도 적용됩니다.

노드 운영자는 **검증자의 실행 보상 100%** 를 가질 권리가 있습니다. 이는 곧 자신이 MEV 전략을 직접 선택할 수 있음을 의미하며, 이는 이더리움의 검열 저항성을 강화하고 상당한 수익성을 가질 수 있습니다.

노드 운영자는 또한 **검증자의 합의 보상 100%** 를 받으며, 이는 검증자의 수익성이 오직 본인에게 달려 있음을 의미합니다. 이 구조는 장기적으로 뛰어난 노드 운영자 성능을 장려합니다.

⚠️ **아이겐레이어 부분 출금 증명 개선 중** 🛠️
현재 아이겐레이어에서 합의 보상을 출금하는 것은 비용이 과도하게 발생합니다. 아이겐레이어 팀은 이러한 비용을 줄이기 위해 노력 중이며, 그때까지 합의 보상 출금은 일시적으로 비활성화되어 있습니다.

노드 운영자 담보는 등록 시 pufETH로 전환되어, 그들의 약정 기간 동안 추가적인 패시브 보상을 획득할 수 있습니다.

왜 퍼퍼에 스테이킹해야 하는가? 💪

대부분의 리퀴드 스테이킹 프로토콜과 달리, 퍼퍼의 스테이커는 pufETH가 경쟁력 있는 보상을 얻기 위해 검증자가 좋은 성과를 내기를 신뢰할 필요가 없습니다. 검증자 티켓이 스테이커에게 검증자의 장기 성과와 관계없이 보장을 제공하기 때문입니다.

> ***Tip***
> *pufETH는 노드 운영자의 장기 성과와 무관하게 PoS 보상을 즉시 적립합니다.*

PoS 보상이 천천히 쌓이기를 기다리는 대신, pufETH 보유자는 검증자 티켓이 발행될 때마다 보상을 받습니다. 이 역학은 초기 스테이커에게 유리하며, 비콘 체인의 검증자 대기열이 극도로 혼잡하더라도 pufETH는 향후 발행될 모든 검증자 티켓으로부터 빠르게 가치를 높일 수 있습니다.

전통적인 리퀴드 스테이킹 토큰(LST)은 PoS 보상만 적립합니다. 그러나 nLRT인 pufETH는 PoS와 리스테이킹 보상을 모두 적립하므로, 스테이커는 복잡한 DeFi 전략 없이 더 많은 수익을 얻을 수 있습니다. 동시에 pufETH는 유동 토큰이므로 조합성을 중시하는 경우 DeFi와 100% 호환됩니다.

퍼퍼는 스테이커의 ETH 안전성을 최우선으로 합니다. 스테이킹된 ETH의 안전을 보장하기 위해 프로토콜은 다음을 요구합니다:

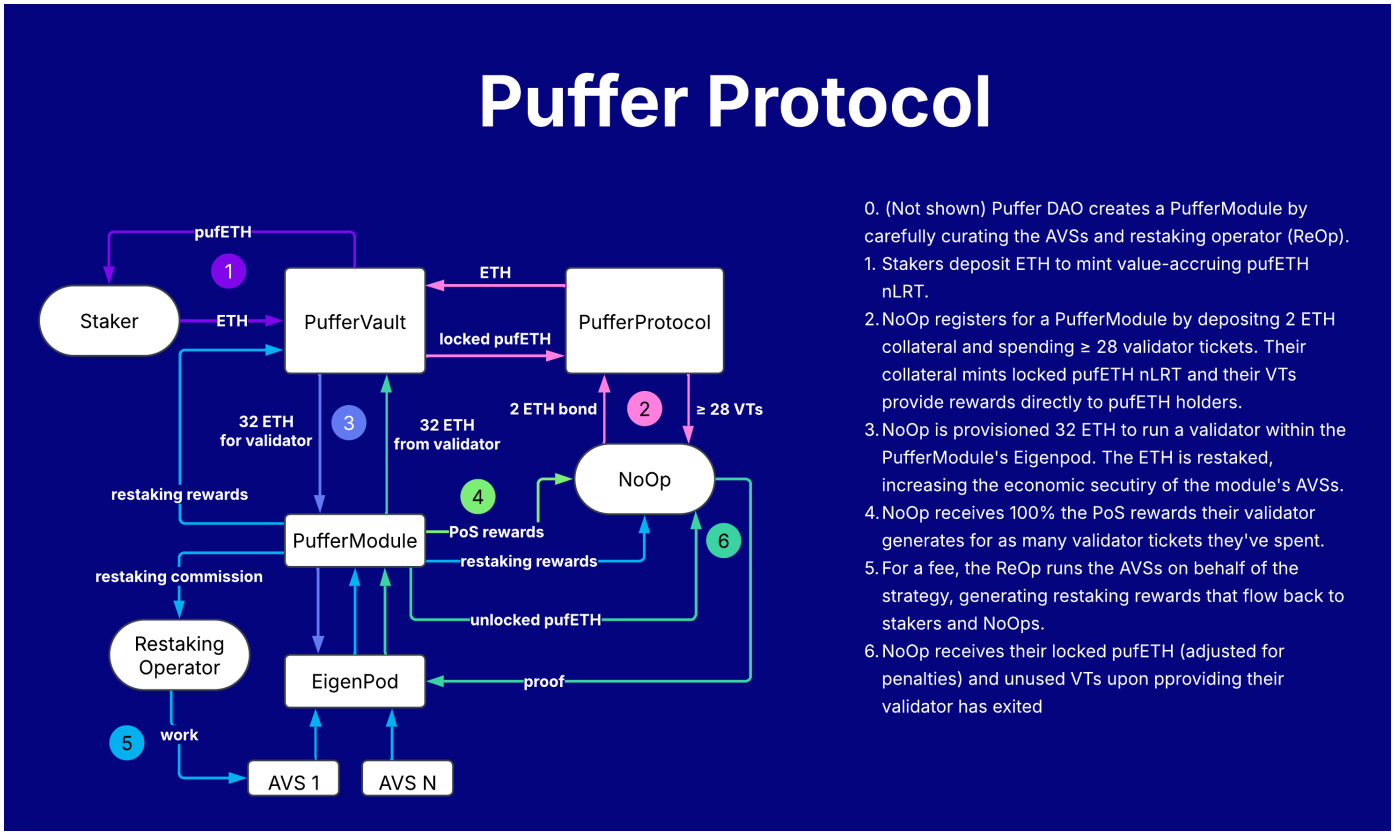
- 노드 운영자는 2 ETH 담보를 잠금
- 잔액이 너무 낮아진 검증자 퇴출
- 허용된 AVS에 대한 가드레일
- 리스테이킹 운영자가 될 수 있는 주체에 대한 가드레일

프로토콜 (Protocol)

개요 (Overview)

> ***정보***
> *퍼퍼는 리스테이킹의 잠재력을 활용하도록 설계된 네이티브 리퀴드 리스테이킹 프로토콜(nLRP) 입니다.*

퍼퍼 사용 과정 👩‍💻



0️⃣ 퍼퍼모듈(PufferModules) 생성

퍼퍼는 새로운 검증자가 프로토콜에 참여함에 따라 채워지는 여러 개의 빈 퍼퍼모듈로 시작합니다.

퍼퍼 거버넌스는 리스테이킹을 감독하는 데 중요한 역할을 하며, 여기에는 새로운 모듈 추가, 리스테이킹 운영자(RestakingOperator) 컨트랙트에 대한 위임 관리, 운영자의 AVS 약속 관리가 포함됩니다.

예를 들어, 퍼퍼프로토콜 컨트랙트에 새로운 모듈을 추가하려면 거버넌스는 다음을 수행해야 합니다:

1. 리스테이킹 운영자(Restaking Operator)를 심사하고 선택하여 RestakingOperator 컨트랙트를 대신 운영하게 합니다.
2. RestakingOperator 컨트랙트가 선택할 수 있는 아이겐레이어 AVS를 심사하고 선택합니다.
3. 모듈의 ETH를 RestakingOperator 컨트랙트에 위임합니다.

1️⃣ ETH 스테이킹

스테이커는 ETH를 예치하고 퍼퍼볼트(PufferVault) 컨트랙트를 통해 pufETH nLRT를 발행할 수 있습니다. 이는 리스테이킹된 ETH에 대한 상환 가능한 영수증 역할을 합니다. 충분한 출금 유동성이 있다면 스테이커는 퍼퍼 볼트에서 ETH를 회수할 수 있습니다. 시간이 지남에 따라 상환 가능한 금액은 검증자 티켓과 리스테이킹 보상으로 증가할 것으로 예상됩니다.

일반적인 리퀴드 스테이킹 토큰(LSTs)과 달리, pufETH는 보유자에게 더 많은 보상을 제공합니다. pufETH는 PoS 보상과 리스테이킹 보상을 모두 포함할 뿐만 아니라, 검증자 티켓 판매로 인해 가치가 빠르게 상승할 수 있습니다. 또한 스테이커의 PoS 보상은 프로토콜 검증자의 성과와 분리되어 있습니다.

2️⃣ 노드 운영 검증자 등록

새로운 검증자를 등록하기 위해 노드 운영자는 검증자 티켓과 2 ETH를 담보로 퍼퍼프로토콜 컨트랙트에 예치합니다. 그 대가로, 프로토콜은 pufETH를 발행하며 이는 검증자가 성공적으로 종료되었음이 확인될 때까지 잠금 상태로 유지됩니다. pufETH 잠금은 다음을 위해 작동합니다:

- 노드 운영자 인센티브 정렬
- 스테이커 ETH 보호
- 노드 운영자 수익 마진 확대

스테이커의 안전을 보장하기 위해, 노드 운영자는 암호화된 검증자 키셰어를 가디언(Guardians)의 엔클레이브(enclave)에 분배해야 합니다. 이를 통해 검증자 잔액이 너무 낮아지거나 검증자 티켓이 소진되면 가디언이 노드 운영자를 퇴출할 수 있습니다. 이 요구 사항은 스테이커를 보호하기 위함이며, 이더리움 프로토콜이 EIP-7002를 통해 이를 허용하면 트러스트리스 솔루션으로 업그레이드될 예정입니다.

3️⃣ ETH 할당 (Provisioning ETH)

각 RestakingModule 컨트랙트는 대기 중인 노드 운영자 등록 대기열을 포함합니다. 퍼퍼 볼트가 예치금과 보상으로부터 32 ETH 단위를 축적하면, 가디언은 라운드 로빈 방식으로 이를 노드 운영자의 대기 중인 검증자에게 할당하여 모든 모듈이 서비스되도록 합니다.

할당 단계는 EigenPod 내에서 새로운 검증자를 생성하며, 이 ETH는 아이겐레이어에서 네이티브 리스테이킹될 수 있어 등록된 AVS의 담보 역할을 합니다. 이러한 이유로, 노드 운영자의 검증자의 출금 자격 (Withdrawal Credential)이 모듈의 EigenPod 컨트랙트에 필요합니다. 할당 후 노드 운영자 검증자는 BeaconDepositContract에 32 ETH를 예치하고 활성화를 기다리게 됩니다.

4️⃣ PoS 보상

검증자가 활성화되면, 노드 운영자는 예치한 검증자 티켓 기간 동안 검증을 수행할 자격을 갖습니다. 이 기간 동안 노드 운영자는 생성된 PoS 보상의 100%를 유지합니다. 실행 보상은 즉시 지갑에 입금되며, 합의 보상은 모듈의 EigenPod에 누적되고 노드 운영자 출금 절차를 통해 출금할 수 있습니다.

노드 운영자가 자신이 생성한 PoS 보상의 100%를 받기 때문에, 그들은 검증자 성능을 최대화하도록 인센티브를 가지며, 이는 스테이커의 ETH를 보호하는 데 기여합니다.

5️⃣ 리스테이킹 보상

리스테이킹 운영자는 모듈을 대신해 AVS를 실행하며 그 대가로 수수료를 받습니다. 이 AVS에서 발생한 수수료는 pufETH의 가치를 높입니다. 이를 통해 스테이커는 일반적인 LST보다 더 높은 수익을 얻을 수 있습니다.

리스테이킹 모듈에 참여하는 노드 운영자는 담보에 대한 추가 위험을 부담합니다. 이를 보상하기 위해 그들은 리스테이킹 보상의 일부를 부여받습니다. 이 구조는 추가적인 하드웨어나 연산 자원 없이도 PoS 보상 이상을 얻을 수 있게 합니다. 이 보상은 합의 보상과 동일한 노드 운영자 출금 절차를 통해 주기적으로 접근할 수 있습니다.

6️⃣ 검증자 종료 (Exiting Validators)

노드 운영자가 프로토콜에서 나가고 싶을 때, 먼저 자신의 검증자가 비콘 체인에서 종료되었음을 확인해야 합니다. 검증자의 종료 증거를 제시하면, 컨트랙트는 검증자가 활동 중단이나 슬래싱으로 인해 발생했을 수 있는 벌금을 합산합니다. 그에 해당하는 ETH 페널티 상당의 pufETH가 노드 운영자의 잠금 담보에서 소각되며, 나머지는 노드 운영자에게 반환됩니다.

이 과정은 검증자 생애주기 동안 발생할 수 있는 ETH 손실에 대해 스테이커가 적절히 보상받을 수 있도록 보장합니다. 또한 사용되지 않은 검증자 티켓은 노드 운영자에게 반환됩니다.

Guiding Principles

> ***정보***
> *퍼퍼는 이더리움 검증을 단지 접근 가능할 뿐 아니라 수익성 있게 만드는 것을 목표로 합니다 💪🧑*

프로토콜은 이더리움 검증자 다양성을 개선하기 위해 노력합니다. 이러한 취지에서, 퍼퍼 프로토콜은 다음과 같이 설계되었습니다.

안전 우선(Safety first)

> *프로토콜은 스테이커와 그들이 지원하는 네트워크에 대해 스테이킹 및 리스테이킹 리스크를 낮춰야 합니다.*

- 퍼퍼의 노드 운영자는 슬래싱 위험을 완화하기 위해 안티-슬래싱 하드웨어를 운영하고 담보를 락업합니다.
- 퍼퍼는 장기적인 노드 운영자 인센티브가 더 우수한 독창적 검증자 담보 접근법을 도입합니다. 자세히 보기 👉 validator tickets incentives.
- 퍼퍼는 비활성화 위험을 줄이기 위해 높은 정렬을 가진 보안 위원회를 사용합니다. 자세히 보기 👉 Guardian duties.
- 퍼퍼는 리스테이킹 생태계가 발전함에 따라 허용되는 AVS에 대해 엄격한 가드레일을 둡니다. 자세히 보기 👉 restaking AVSs.
- 퍼퍼는 리스테이킹 생태계가 발전함에 따라 AVS를 운영할 수 있는 주체에 대해 엄격한 가드레일을 둡니다. 자세히 보기 👉 restaking operators.
- 퍼퍼는 프로토콜의 ETH를 다양한 아이겐레이어 AVS와 리스테이킹 운영자에 배분하여 리스크를 조정합니다. 자세히 보기 👉 allocating ETH to modules.

Ethos-aligned

> *프로토콜은 이더리움의 정체성과 부합해야 합니다.*

- 퍼퍼는 이더리움의 신뢰할 수 있는 중립성을 보호하기 위해 프로토콜 규모를 22%로 선제적 자체 상한(self-capping)합니다. 자세히 보기 👉 burst threshold to self-cap.

- 퍼퍼는 완전한 탈중앙화를 향한 로드맵으로 설계되었습니다. 자세히 보기 👉 decentralizing the Guardians.
- 퍼퍼는 노드 운영자가 장기 약정을 가지므로 이더리움 지분증명의 안정성을 높이는 데 도움이 됩니다. 자세히 보기 👉 validator tickets.
- 퍼퍼는 안티-슬래싱 기술에 대해 이더리움 재단의 그랜트를 받았습니다.

무허가(Permissionless)

> *프로토콜은 누구나 검증자를 운영할 수 있도록 해야 합니다.*

- 퍼퍼는 2 ETH 보증금(어떤 하드웨어든)으로 누구나 이더리움 검증자를 운영할 수 있게 합니다. 자세히 보기 👉 NoOp Requirements.

낮은 장벽(Low barriers)

> *프로토콜은 노드 운영자를 유치하기 위해 자본 효율적이어야 합니다.*

- 퍼퍼는 이더리움 검증자가 되기 위해 필요한 ETH를 최소 2 ETH까지 낮춰 더 많은 참여를 유도합니다. 자세히 보기 👉 validator tickets.
- 퍼퍼는 32 ETH 미만으로도 노드 운영자에게 리스테이킹 노출을 제공합니다. 자세히 보기 👉 modules.

수익성 있는(Profitable)

> *프로토콜은 노드 운영자를 유치하기 위해 수익성이 있어야 합니다.*

- 퍼퍼는 아이겐레이어 리스테이킹 노출을 통해 노드 운영자가 이익 마진을 높일 수 있게 합니다. 자세히 보기 👉 modules.

확장 가능한(Scalable)

> *프로토콜은 중앙화된 리퀴드 스테이킹 프로토콜과 경쟁할 수 있을 만큼 확장 가능해야 합니다.*

- 퍼퍼는 스테이커가 어떤 양의 ETH든 가져올 수 있도록 하여 프로토콜 성장을 돕습니다. 자세히 보기 👉 minting pufETH.
- 퍼퍼는 리스테이킹 노출을 통해 pufETH 보유자의 보상을 극대화합니다. 자세히 보기 👉 nLRTs.
- 퍼퍼는 검증자 대기열이 매우 길더라도 pufETH가 가치 성장을 지속할 수 있도록 설계되었습니다. 자세히 보기 👉 validator tickets.

- 퍼퍼 스테이커는 프로토콜의 검증자가 부진하더라도 보상을 획득합니다. 자세히 보기 👉 NoOp incentives.

네이티브 유동성 리스테이킹 토큰(native Liquid Restaking Tokens (nLRTs))

> ***정보***
> *nLRT는 LST의 2.0 버전이라고 생각해 보세요* 🤯

LST란 무엇인가요?

유동성 스테이킹 토큰(LST)은 비콘 체인에 락업된 ETH를 토큰화된 형태로 표현하여, 스테이커에게 유동성을 제공하는 동시에 보유 기간 동안 PoS 보상을 수동적으로 획득할 수 있게 합니다. LST를 통해 스테이커는 검증자를 운영할 필요 없이 PoS 보상을 수취합니다. 이러한 토큰은 다음과 같은 여러 이점을 제공합니다:

- **유동성**: ETH를 스테이킹하면 다양한 DeFi 활동에 사용할 수 있는 거래 가능한 토큰을 받습니다.
- **사용 용이성**: 스테이커의 별도 조치 없이 LST에 보상이 자동으로 적립됩니다.
- **유연성**: LST를 통해 사용자는 다양한 DeFi 프로토콜에 참여하여 잠재 수익 기회를 다각화할 수 있습니다.

네이티브 유동성 리스테이킹 토큰에 대한 소개 (nLRTs)

이더리움의 끊임없이 진화하는 스테이킹 환경은 새로운 토큰 모델, 즉 **네이티브 리퀴드 리스테이킹 토큰 (nLRT)**을 탄생시켰습니다. 이 현대적 리퀴드 스테이킹 방식은 전신인 LST 대비 독보적 이점을 제공합니다.

> 💡 ***Tip***
> *기본적으로, nLRT는 전통적인 PoS 보상을 제공하면서 여기에 추가 리스테이킹 보상을 더하는 LST입니다.*

nLRT와 LRT의 차이는 무엇인가요?

nLRT는 이더리움 PoS 검증자 ETH가 스테이킹 자산인 아이겐레이어에서의 네이티브 리스테이킹을 통해 리스테이킹 보상을 생성합니다. 이것이 LRT와의 차별점입니다. LRT는 리퀴드 리스테이킹 프로토콜(LRP) 내에서 리스테이킹된 LST를 토큰화합니다. LRP는 리스테이킹 서비스에서 보상을 창출하지만, 이는 PoS 보상과는 구별됩니다.

핵심 개념은 LST와 일치하지만, LRT는 리스테이킹 서비스에서 나오는 보상에만 초점을 둡니다. 퍼퍼는 LRT가 이더리움에서 LST와 관련된 탈중앙화 문제를 심화시킬 수 있다고 관찰해 왔습니다. 반면, nLRT는 PoS에 새로운 검증자를 통합하면서 그 수익성을 높여 탈중앙화를 적극 촉진합니다. 중요하게도, 이러한 이유로 퍼퍼는 첫날부터 퍼미션리스 검증자 세트로 출시하는 데 전념해 왔습니다.

pufETH

pufETH는 최적의 DeFi 호환성을 위해 Compound의 cToken 설계를 따르는 리워드 보유형 ERC20 토큰으로 구현되었습니다. 이는 리퀴드 스테이킹 영역에서의 새로운 접근으로, 스테이커의 보상과 DeFi 프로토콜과의 상호작용을 향상시키는 여러 기능을 도입합니다.

향상된 보상 잠재력

pufETH를 포함한 nLRT는 다변화된 보상 흐름을 제공합니다. 전통적인 이더리움 PoS 보상을 포괄할 뿐만 아니라, 리스테이킹 서비스에서 나오는 보상까지 허용합니다. 이러한 이원적 보상 구조는 nLRT 보유자가 LST 보유자보다 더 높은 수익을 얻을 가능성을 높입니다.

검증자 티켓을 통한 가치 가속

pufETH는 검증자 티켓을 활용하여 가치 성장을 가속화합니다. 이더리움 PoS 보상을 프런트로딩함으로써, pufETH 토큰의 즉시 청구 가치를 높일 뿐 아니라 단·장기 참여 모두에 매력적인 인센티브를 창출합니다.

검증자 성과로부터의 디커플링

연계된 검증자 성과에 보상이 밀접히 의존하는 LST와 달리, pufETH는 하나의 차단막을 제공합니다. 이는 스테이커가 검증자 성과와 무관하게 PoS 보상을 수취하도록 보장하여, 더 안정적이고 예측 가능한 수익을 제공하고 잠재적 부진의 영향을 완화합니다.

강화된 단순성과 매끄러운 디파이 통합

확장 중인 LSDeFi 생태계에서, 다양한 프로토콜과 매끄럽게 맞물리는 스테이킹 메커니즘의 적응성은 매우 중요합니다. LST가 DeFi 호환성의 표준을 제시해 왔다면, pufETH는 이 경험을 한 단계 끌어올립니다.

리스테이킹 보상을 얻기 위해 LST를 보유한 뒤 LRP에 다시 리스테이킹하는 2단계 절차와 달리, pufETH는 한 단계로 이를 달성합니다. pufETH를 보유하기만 해도, 사용자는 본질적으로 리스테이킹 보상에 접근합니다. 이 간소화는 스테이커가 전통적 LST가 디파이에서 제공하는 유연성과 기회를 훼손하지 않으면서도 스테이킹 자산의 효용과 보상을 극대화하도록 보장합니다.

pufETH 작동 방식

스테이커는 퍼퍼 볼트 컨트랙트에 ETH를 예치하여 pufETH nLRT를 민트합니다. 프로토콜 초기에는 pufETH의 전환율이 1:1이지만 시간이 지나며 증가할 것으로 예상됩니다. 즉, 프로토콜이 잘 수행되어 벌점보다 보상이 더 많이 누적되면 pufETH로 상환 가능한 ETH 양이 증가합니다.

전환율 계산

전환율은 다음과 같이 간단히 계산할 수 있습니다:

$$\text{conversion rate} = \frac{\text{deposits} + \text{rewards} - \text{penalties}}{\text{pufETH supply}} \tag{1}$$

- 스테이커가 ETH를 예치해 pufETH를 민트하면 `deposits`와 `pufETH supply`가 비례하여 증가하므로 `conversion rate`에는 영향이 없습니다.
- 리스테이킹 운영자가 AVS를 실행하고 검증자 티켓이 발행될 때마다 `rewards`가 증가합니다.
- 검증자가 PoS에서 담보인 1 ETH를 초과하여 슬래시될 경우(이는 비인센티브 행위입니다) `penalties`가 누적됩니다. 또한 리스테이킹 운영자가 AVS를 운영하다 슬래시될 경우에도 벌점이 누적될 수 있으므로, 퍼퍼는 초기 단계에서 리스테이킹 운영자 참여를 제한하고 있습니다.

예시

프로토콜 초기, Bob은 10 ETH를 스테이킹하고 10 pufETH를 받습니다. 이후 일정 시간이 지나, 프로토콜이 검증자 티켓 발행과 리스테이킹으로 2 ETH의 보상을 벌었다고 합시다. 이제 Bob의 10 pufETH는 12 ETH로 담보되며, 전환율은 $\frac{10+2-0}{10} = 1.2$ ETH/pufETH가 됩니다.

Charlie가 1 ETH를 스테이킹하기로 했다면, 전환율 상승으로 인해 $\frac{1}{1.2} = 0.83$ pufETH를 민트하게 됩니다. Charlie의 예치는 보상을 추가한 것이 아니라 예치이므로, 전환율은 $\frac{11+2-0}{10.83} = 1.2$ ETH/pufETH로 변함이 없습니다.

퍼퍼 볼트에 충분한 유동성이 있고 일일 출금 한도에 도달하지 않았다면, Bob은 자신의 10 pufETH를 $10 \times 1.2 = 12$ ETH로 상환할 수 있습니다.

퍼퍼 모듈

> ***정보***
> *퍼퍼는 검증자가 네이티브 리스테이킹 노출을 통해 전통적인 리퀴드 스테이킹 프로토콜이나 솔로 스테이킹보다 더 많은 보상을 얻을 수 있도록 합니다.*

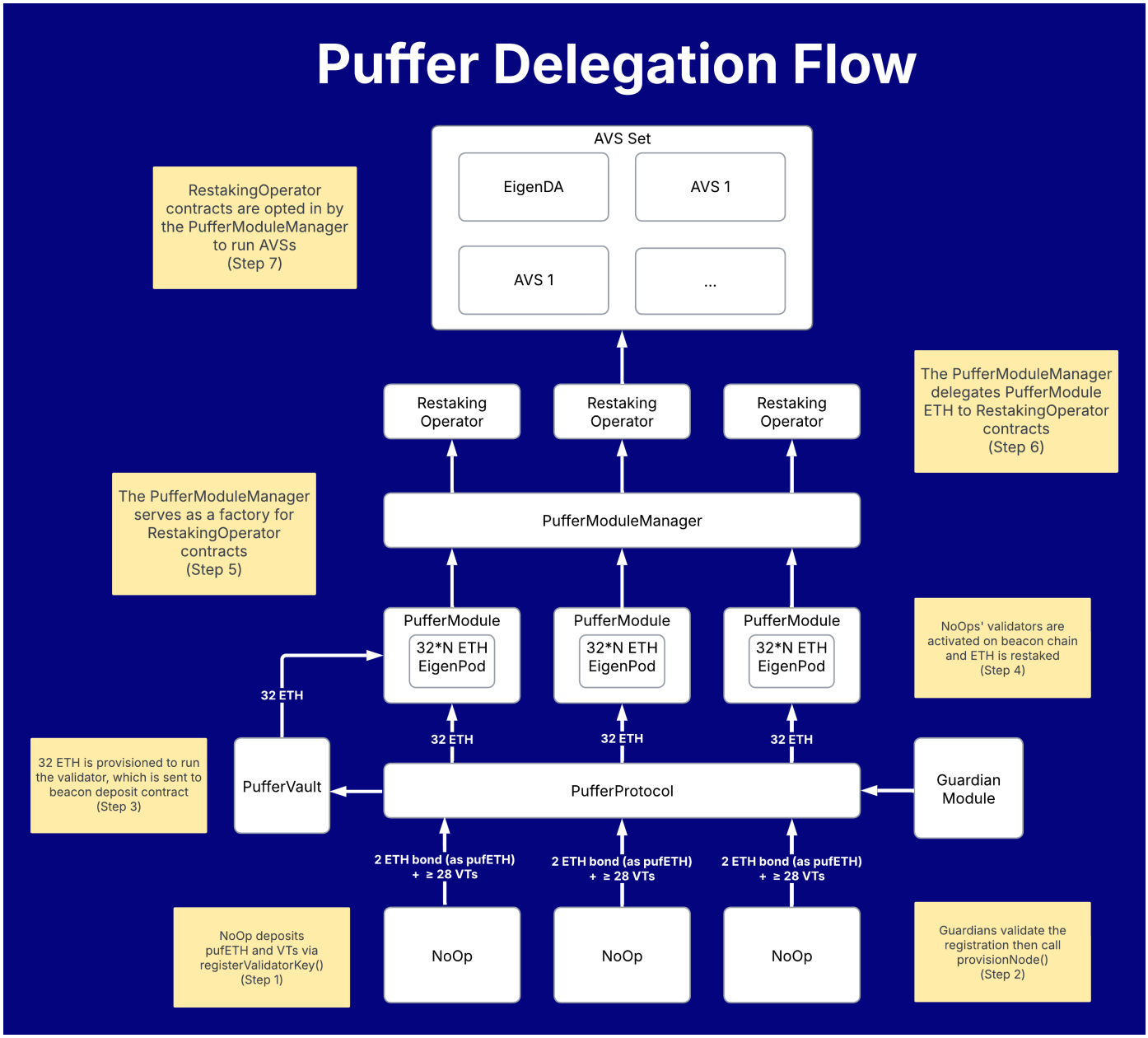
네이티브 리스테이킹 💪

네이티브 리스테이커__는 자신의 32 ETH를 리스테이킹하여 아이겐레이어 AVS를 운영하는 이더리움 PoS 검증자입니다. 네이티브 리스테이커는 서비스 대가로 AVS 수수료를 받지만, AVS 규칙을 위반하면 페널티를 받습니다. 네이티브 리스테이킹을 수행하려면 검증자는 자신의 출금 자격(Withdrawal Credentials)을 EigenPod 컨트랙트에 지정해야 하며, 이 컨트랙트가 리스테이킹을 선택(opt-in)하고 AVS를 선택합니다.

네이티브 리스테이킹은 검증자가 ETH 자본과 하드웨어를 더 잘 활용하여 PoS 보상을 보충할 수 있게 합니다. 그러나 32 ETH 요구사항은 대부분의 사용자에게 너무 높은 장벽이며, 일부 AVS는 PoS보다 훨씬 더 높은 연산 자원을 필요로 할 수 있습니다. 퍼퍼는 이를 **퍼퍼모듈(PufferModules)**을 통해 해결하고자 합니다.

퍼퍼 모듈 🐡

퍼퍼 프로토콜의 핵심은 여러 개의 **퍼퍼모듈** 컨트랙트 모음입니다. 각 모듈은 하나의 네이티브 리스테이커처럼 작동하는 EigenPod를 제어하지만, 실제로는 다수의 노드 운영자가 운영하는 검증자로 구성됩니다.



모듈은 노드 운영자 검증자로 채워지며, 이들의 유일한 임무는 이더리움 PoS 검증을 수행하는 것입니다. 검증자의 ETH는 이후 리스테이킹되어 아이겐레이어 AVS의 담보로 사용됩니다. 퍼퍼의 초기 단계에서는, AVS 운영 책임이 DAO가 선정한 **리스테이킹 운영자(Restaking Operator, ReOp)**에게 위임되며, 이들은 생성된 AVS 수수료 일부를 대가로 서비스를 제공합니다.

프로토콜은 어떤 AVS에 모듈이 배정될지 결정하여, 리스테이킹된 ETH가 프로토콜의 위험 성향에 따라 AVS에 배분되도록 합니다. 위임 위험을 감안하여, 노드 운영자는 AVS 수수료의 일부를 커미션으로 받고 나머지는 프로토콜로 반환되어 pufETH 가치를 성장시킵니다. 이를 통해 노드 운영자는 단 2 ETH로 네이티브 리스테이킹 보상을 받을 수 있습니다.

> 💡 ***tip***
> *노드 운영자가 자신의 검증자를 퍼퍼 모듈에 배치하면 자동으로 리스테이킹 보상 커미션을 얻게 됩니다.*

리스테이킹 운영자 (Restaking Operators)

리스테이킹 운영자(ReOps)는 특정 모듈을 대신하여 모든 필요한 AVS 업무를 수행하는 역할을 맡습니다. ReOps는 자신의 모듈 또는 다른 모듈에서 노드 운영자일 수도 있습니다. ReOps는 본인의 이익뿐만 아니라 모듈 내 노드 운영자 및 pufETH 보유자에게 최대한의 리스테이킹 보상을 제공하기 위해 성과를 최적화해야 합니다.

퍼퍼 프로토콜에서 ReOps는 RestakingOperator 컨트랙트를 통해 운영되며, 거버넌스는 PufferModuleManager 컨트랙트를 통해 그들의 AVS 선택을 결정합니다.

모듈 참여 👈

이더리움의 철학과의 정렬을 유지하기 위해, 노드 운영자가 모듈에 참여하여 이더리움 검증자를 배치하는 것은 **항상 퍼미션리스**입니다.

> 💡 ***tip***
> *노드 운영자는 검증자를 모듈에 퍼미션리스하게 배치할 수 있습니다.*

참여하기 위해, 노드 운영자는 2 ETH 담보와 검증자 티켓을 잠금합니다. 티켓은 모듈 내 검증자를 운영하겠다는 장기적 약속을 나타냅니다. 담보는 pufETH로 잠기며, 이후 32 ETH가 공급되어 모듈의 EigenPod 컨트랙트에 검증자가 배치됩니다.

노드 운영자는 이제 자신의 검증자가 생성하는 모든 PoS 보상(합의 및 실행)을 가질 권리가 있으며, 퍼퍼 모듈에 참여한 노드 운영자는 리스테이킹 보상도 받습니다.

리스테이킹 위험과 완화 🚧

리스테이킹 개념은 유망하지만, 스테이커와 노드 운영자 모두에게 내재적 위험을 수반합니다. 이는 주로 스마트 컨트랙트 취약성과 잠재적 AVS 슬래싱 위험을 중심으로 합니다.

> 💡 ***tip***
> *퍼퍼는 리스테이킹이 성숙해짐에 따라 보수적 접근을 통해 이러한 위험을 완화하려고 합니다.*

리스테이킹이 제공할 수 있는 지속 가능한 보상 덕분에, 이는 현재 완전 중앙화를 향해 가고 있는 리퀴드 스테이킹 시장의 역학을 재편할 수 있습니다.

ReOps 제한

리스테이킹 세계로의 안전한 전환을 보장하기 위해, 퍼퍼는 초기 단계에서 거버넌스가 리스테이킹 자격을 더 중점적으로 결정하도록 할 것입니다. 이 시기에는 거버넌스를 통해 선정된 뛰어난 성과의 신뢰할 수 있는 ReOps만이 특정 모듈을 대신하여 AVS를 운영할 수 있습니다.

아이겐레이어, AVS, 그리고 퍼퍼의 안티-슬래싱 메커니즘이 성숙해지면, 입증된 노드 운영자는 DAO 승인 없이도 ReOps가 될 수 있는 옵션을 갖게 됩니다.

AVS 제한

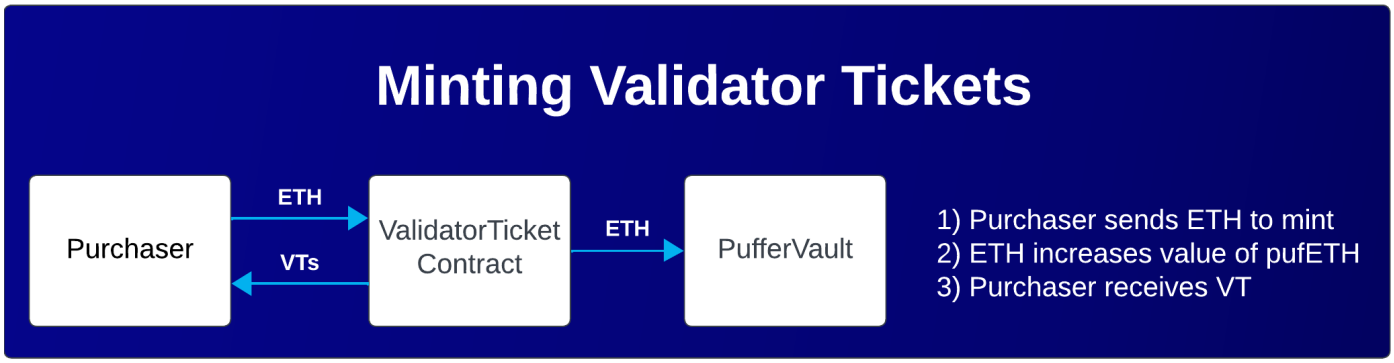
아이겐레이어는 누구나 AVS를 배포할 수 있는 오픈 플랫폼입니다. 따라서 PufferModules이 모든 AVS를 서비스할 수 있도록 허용한다면 스테이커와 노드 운영자는 과도한 슬래싱 위험에 노출될 것입니다.

이 위험을 완화하기 위해, 퍼퍼는 DAO가 새로운 모듈을 온보딩하고, 허용되는 AVS를 신중히 심사하며, 모듈을 AVS에 배분하도록 요구합니다.

검증자 티켓(Validator Tickets)

> ***정보***
> *Validator Tickets는 LST 검증자 라이프사이클에 퍼퍼가 새롭게 도입한 개념입니다.*
> ***Validator Tickets**는 퍼퍼의 초기 연구 협력인 "Smoothing Commitment"(Justin Drake과 공동 연구)에서 발전한 것이며, 최근 이더리움 로드맵에 추가된 "Execution Tickets" 제안과 밀접한 관련이 있습니다.*

개요 (Overview)



핵심 아이디어는 단순하지만 강력합니다:

- **pufETH**: 사람들이 ETH를 스테이킹하면 퍼퍼 프로토콜 내 스테이킹된 ETH를 나타내는 pufETH를 받으며, 이는 이더리움 검증자 자금을 조달하는 데 사용됩니다.
- **Validator Tickets (VTs)**: VTs는 보유자에게 스테이커가 자금을 댄 이더리움 검증자를 하루 동안 운영할 권리를 부여하는 ERC20 토큰입니다. VTs는 ETH 예치로 발행되며, 이 ETH는 검증자를 자금 조달한 pufETH 보유자를 보상하는 데 쓰입니다.
- **검증자 운영**: 검증자를 운영하려면 노드 운영자는 VTs를 잠그고, 2 ETH 상당의 pufETH를 담보로 잠가야 합니다.
- **VT 가격**: VT 가격은 검증자 운영으로 기대되는 하루 수익에 따라 책정됩니다. 이 가격은 pufETH 예상 APR에 직접적으로 영향을 줍니다.
- **혜택**: VTs는 새로운 거래 기회를 창출하고, "러그 풀링" 문제를 해결하며, 성과를 높이도록 인센티브를 제공합니다. pufETH 보유자는 VTs 구매 시 즉시 보상을 받습니다. VTs를 사용한 노드 운영자는 검증자의 모든 수익을 100% 가져갑니다.

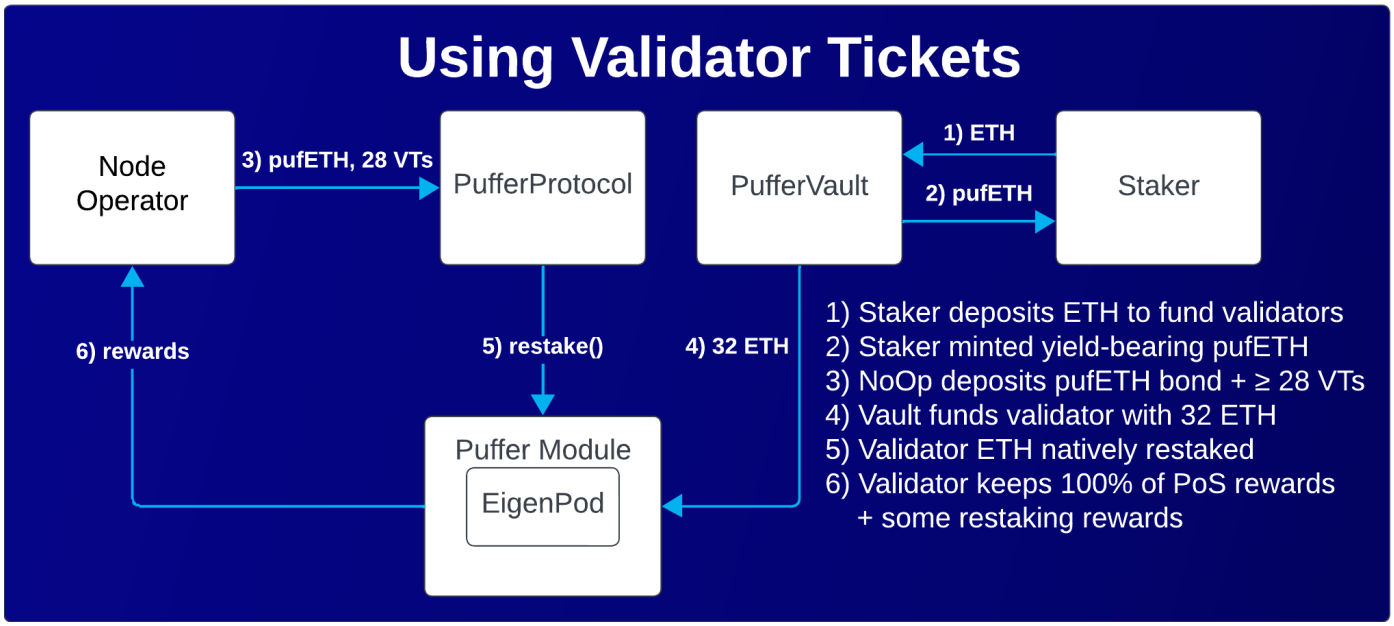
현행 모델 (The status quo)

일반적으로, 리퀴드 스테이킹 프로토콜(LSPs)은 검증자 운영에 두 가지 모델을 사용합니다:

- **언본디드(Unbonded) 모델**: 검증자는 담보를 잠글 필요가 없습니다. 성장에는 유리하지만, 페널티가 스테이킹 풀에 직접 영향을 주며, 종종 특별히 승인된 검증자(퍼미션드 / KYC 필요)를 요구합니다.
- **본디드(Bonded) 모델**: 검증자는 운영 기간 동안 담보를 잠급니다. 더 안전하며 모든 검증자가 참여할 수 있지만, 검증자당 많은 ETH를 선납해야 하므로 LSP 성장 속도가 느려집니다.

퍼퍼는 *본디드 모델*을 채택하되, VTs를 추가해 기존 단점을 보완합니다.

VTs는 어떻게 사용되는가?



Validator Tickets는 검증자 본드(bond)를 보완합니다. 검증자를 등록할 때 노드 운영자는 2 ETH 상당의 pufETH를 본드로 잠그고, 최소 28 VTs를 예치합니다.

그 대가로 32 ETH가 할당되어 검증자를 운영할 수 있으며, 노드 운영자는 자신이 예치한 VTs 일수만큼 발생하는 PoS 보상을 100% 가져갑니다. 즉, 노드 운영자는 검증자를 운영하기 위해 pufETH 보유자에게 ETH를 선지급하는 셈입니다.

각 VT는 1일(검증자 1일차)의 PoS 보상을 나타냅니다. VTs 발행 시 지불된 금액은 pufETH 보유자에게 직접 지급되어 강력한 성장 동력을 만듭니다. 이는 스테이커에게 유리하며, 자본 효율적이고, 노드 운영자 성과를 최적화하도록 유도합니다. 검증자가 종료될 때, 활동 일수에 해당하는 VT가 소각되며, 사용되지 않은 VTs는 노드 운영자가 되찾을 수 있습니다.

왜 필요한가? ~ 노드 운영자 인센티브

LSP의 성공은 노드 운영자의 성과에 크게 의존합니다. 전통적으로 노드 운영자에게 담보를 예치하도록 요구하는 것은 프로토콜 목표와의 정렬을 보장하는 방법이었습니다. 담보를 걸면 오프라인, 슬래싱, MEV 도둑질("러그 풀링") 같은 행위를 억제할 수 있습니다.

그러나 이 담보 방식은 성과 향상에 강한 인센티브를 주지 못합니다. 예를 들어, "게으른" 노드 운영자는 온라인과 오프라인을 번갈아 유지해 잔액을 32 ETH에 맞춰둘 수 있습니다. 이 경우 LSP는 보상을 얻지 못하지만 노드 운영자도 담보를 잃지 않습니다.

퍼퍼는 VTs를 통해 이 인센티브 구조를 바꿉니다. 노드 운영자는 VTs를 이미 구매했기 때문에, 성과가 부진하면 초기 비용을 회수할 방법이 없습니다. 따라서 수익을 내려면 최소한 평균 검증자 수준의 성과를 내야 하며, 성과가 뛰어난 경우 더 많은 수익을 올릴 수 있습니다.

추가적으로, 퍼퍼는 스테이커 ETH를 보호하기 위해 2 ETH 담보를 요구합니다.

이 접근 방식은 두 가지 전통적 문제를 해결합니다:

- **러그 풀링**: 노드 운영자가 자신이 생성한 MEV를 100% 가져가기 때문에, 더 이상 러그 풀링을 감시하거나 처벌할 필요가 없습니다.
- **게으른 노드 운영자**: 스테이커는 VTs 발행 시 PoS 보상을 선지급 받기 때문에, 노드 운영자가 부진하더라도 영향을 받지 않습니다.

요구사항 (Requirements)

PoS 안정성과 노드 운영자 인센티브 정렬을 위해, 등록 시 2 ETH 상당의 pufETH와 최소 28 VTs를 예치해야 합니다. 기간은 검증자가 비콘 체인에서 활성화되는 순간 시작되며, 각 VT는 1일 또는 255 에폭(epoch)을 나타냅니다.

28 VTs를 예치했다면, 28일 검증 후 노드 운영자 검증자는 자동으로 퇴출되며, 32 ETH는 프로토콜로 반환되고 본드는 돌려받습니다. 더 연장하려면 언제든 추가 VTs를 예치할 수 있습니다. 사용되지 않은 VTs(예: 100 VTs 예치 후 28일 사용 시 72 VTs)는 프로토콜에서 회수할 수 있습니다.

Validator Tickets 가격 산정

Validator Tickets의 가격은 RedStone Oracles에 의해 제공·게시됩니다. VT 오라클 모듈은 완전 자동화되어 있으며, MEV 지급액 10% 또는 합의 보상 5% 이상 편차가 발생하거나 12시간마다 데이터를 업데이트합니다.

퍼퍼 Phase 1 동안, VT 가격은 가디언이 게시합니다. 가격은 아래 공식으로 계산됩니다. 여기서 $R_{expected}$는 합의 및 실행 보상 이력에 기반한 하루 예상 검증자 수익, D는 할인율입니다:

$$P_{VT} = R_{expected} \times (1 - D) \tag{2}$$

예시

- 연간 예상 합의 보상 + 실행 보상이 $5\% \times 32 = 1.6$ ETH라면,
- 단순화된 $R_{expected} = 1.6/365 = 0.00438$ ETH.
- 할인율 $D = 10\%$라면, $P_{VT} = 0.00438 \times 90\% = 0.00394$ ETH.
- 노드 운영자가 VT를 소비하면 하루 동안 평균 0.00438 ETH를 벌 수 있으며, 이는 0.000438 ETH의 기대 이익을 의미합니다.
- 실제 수익은 노드 운영자 성과, 검증자 세트 크기, MEV 상황에 따라 달라질 수 있습니다.

장단점 (Pros and Cons)

장점 (Pros):

- **자본 효율성**: 단 2 ETH(본드 + VTs)만으로 검증자를 운영할 수 있어 기존 LSP보다 진입 장벽이 낮습니다.

- **성장 촉진**: VT 모델은 검증자 대기열이 길더라도 LSP가 보상을 계속 획득할 수 있도록 보장합니다.
- **러그 풀링 감독 불필요**: 노드 운영자가 100% 실행 보상을 가져가기 때문에 러그 풀링을 감시·처벌할 필요가 없습니다.
- **게으른 노드 운영자 억제**: VTs는 선불 구조이므로 성과가 부진한 노드 운영자는 이익을 얻을 수 없습니다.
- **MEV 로터리 참여**: 노드 운영자는 32 ETH를 잠그지 않고도 MEV 기회에 참여할 수 있습니다.

단점 (Cons):

- **새로움**: VTs는 업계에서 새로운 개념이므로 신뢰 구축이 필요합니다.
- **추가 자본 요구**: 본드만 있는 구조보다 더 많은 ETH가 선납되지만, 퍼퍼는 모든 퍼미션리스 LSP 중 최저치인 2 ETH만 요구하기 때문에 상대적으로 부담이 적습니다.
- **가격 변동성**: PoS 보상은 비교적 안정적이지만, 실행 보상 및 검증자 세트 크기 변화에 영향을 받습니다. 그러나 VT는 하루 단위이며 매일 재가격되므로 변동성은 완화됩니다. 또한 VTs는 유동적이며 2차 시장에서 거래될 수 있습니다.

보상(Rewards)

> ***정보***
> *네이티브 리스테이킹 덕분에 스테이커와 노드 운영자는 더 많은 수익을 얻을 수 있습니다.*

보상 개요 (Rewards Overview)

프로토콜은 검증자를 운영하기 위해 발행된 검증자 티켓과, 리스테이킹 운영자가 AVS를 운영하면서 생성한 리스테이킹 보상으로부터 보상을 수취합니다. 이 두 가지 보상이 합쳐져 pufETH를 담보하는 ETH 규모를 늘려, 둘 사이의 전환율을 높이고 결과적으로 pufETH의 가치를 증가시킵니다. 이 섹션에서는 프로토콜 참여자 간 보상이 어떻게 분배되는지 개요합니다.

누가 보상을 받나요? (Who Gets Rewards?)

Stakers

- pufETH nLRT를 보유함으로써 PoS 보상과 리스테이킹 보상을 획득합니다.

노드 운영자

- 자신들의 검증자가 생성한 모든 PoS 보상을 받습니다.

- pufETH 보유 및 검증자를 퍼퍼 모듈에 배치함으로써 추가 수익을 얻습니다.

Restaking Operators

- PufferModules을 대신해 AVS를 운영한 대가로 수수료를 받습니다.

가디언

- 업무 수행에 대한 수수료와 가스 비용 보전을 받습니다.

퍼퍼 프로토콜

- 성장 지원과 거버넌스 토큰의 유틸리티 강화를 위해 프로토콜 수수료를 받습니다.

보상 구성 (Rewards Breakdown)

합의 보상 (Consensus Rewards)

검증자 티켓 덕분에, **노드 운영자는 합의 보상의 100%를 수령합니다.** 이러한 합의 보상은 출금 자격으로 지정된 곳—이 경우 모듈의 EigenPod—으로 향합니다. 다만 이 보상은 즉시 출금할 수 없습니다. 일정 지연 후, 노드 운영자는 머클 리워드 트리를 사용하여 합의 보상을 출금할 수 있습니다.

> *EigenLayer Partial Withdrawals Proofs 개선 중🚧*
> *현재 EigenPods에서 합의 보상을 출금하는 것은 비용이 과도하며, 아이겐레이어 팀이 비용 절감을 위해 작업 중입니다. 그때까지 합의 보상 출금은 일시적으로 비활성화되어 있습니다.*

실행 보상 (Execution Rewards)

검증자 티켓 덕분에, **노드 운영자는 실행 보상의 100%도 수령합니다.** 이 구조는 노드 운영자에게 MEV-Boost 같은 필수 소프트웨어 제약 없이 MEV(Maximal Extractable Value) 전략에 대한 완전한 통제권을 부여하여, 잠재적으로 더 높은 검열 저항성을 가능하게 합니다. 실행 보상은 노드 운영자가 지정한 `fee_recipient` 주소를 사용해 자동으로 해당 지갑으로 라우팅되므로 즉시 유동화됩니다.

리스테이킹 보상 (Restaking Rewards)

리스테이킹 보상은 AVS 운영에서 발생하는 수수료입니다. EigenDA처럼 ETH로 지급하는 프로토콜은 관리가 간단하지만, 다른 일부는 ERC20 토큰으로 지급할 수 있습니다. 이러한 경우, 이 ERC20 보상은 퍼퍼 프로토콜 참여자에게 분배되기 전에 ETH로 변환되어야 합니다.

> *주의: 아이겐레이어 스펙이 아직 확정되지 않음🚧*
> *아이겐레이어는 활발히 개발 중이며, AVS 지급에 관한 더 자세한 정보가 곧 제공될 예정입니다.*

Validator Tickets

Validator Tickets는 발행(민팅)에 ETH 비용이 들며, 다음과 같이 배분됩니다:

- 정직한 행동을 유도하고 가스비를 보전하기 위해 가디언에게 수수료가 지급됩니다.
- 프로토콜 수수료로 국고(treasury)에 일부가 할당됩니다.
- 나머지는 스테이커에게 퍼퍼 볼트로 예치됩니다.

가디언

> ***정보***
> *퍼퍼 프로토콜의 가디언은 프로토콜의 안정적 운영을 보장하도록 신뢰받는 퍼미션드 노드들로 구성됩니다. 이들의 존재는 중요한 기능을 수행하지만, 이더리움 생태계가 발전하고 특정 EIP가 도입됨에 따라 궁극적으로는 불필요해지도록 설계되어 있습니다.*

가디언은 누구인가요?

가디언은 이더리움의 원칙과 가치에 깊이 공감하는 존중받는 커뮤니티 구성원들의 집합입니다. 이들은 탈중앙화 자율 조직(DAO)으로 기능하며, 프로토콜의 성공과 이더리움 생태계의 광범위한 이익에 이해관계를 가지고 있습니다. 커뮤니티에서의 명성은 그들이 최고 수준의 성실성으로 운영되도록 하는 안전장치로 작용합니다.

가디언의 역할은 무엇인가요?

가디언은 퍼퍼 프로토콜에서 세 가지 핵심 책임을 집니다:

1. **검증자 퇴출(Ejecting validators)**: **EIP-7002**가 구현되기 전까지, 특정 조건에서 검증자를 퇴출시키는 역할을 가디언이 수행합니다. 이들은 퇴출 서명에만 사용되도록 설계된 특수 엔클레이브에 보관된 암호화된 검증자 키셰어를 사용합니다. 다음 경우 검증자는 퇴출됩니다:
    - 비콘 체인 잔액이 DAO 임계치 아래로 떨어진 경우.
    - AVS 위반으로 모듈이 슬래시된 경우.
    - 검증자 티켓을 모두 소진했음에도 갱신하지 않은 경우.
    - pufETH 출금 요청을 충족하기 위해 프로토콜이 ETH 유동성이 필요한 경우(검증자는 무작위로 선택).

2. **검증자 할당 또는 건너뛰기(Provisioning or skipping validators)**: 노드 운영자가 검증자를 등록하면, 가디언은 32 ETH를 할당하기 전에 등록을 심사합니다. 등록이 유효하지 않은 경우(예: 잘못된 출금 자격 사용, 잘못된 포크 버전으로 서명, 이미 존재하는 검증자) 또는 가디언을 위한 키 암호화가 제대로 되지 않은 경우, 해당 등록은 건너뜁니다. 노드 운영자의 등록이 건너뛰어지면 본드는 전액 반환되지만, 프로토콜을 괴롭히는 행위를 방지하기 위해 검증자 티켓의 일부가 페널티로 차감됩니다.
3. **종료 시 본드 반환(Returning validator bonds on exit)**: 검증자가 비콘 체인과 아이겐레이어에서 완전히 종료되면, 가디언은 본드를 반환하고 소비된 검증자 티켓을 소각하며, 온체인 회계에서 활성 검증자 수를 업데이트합니다. 이 단계는 퍼퍼가 보다 실시간에 가까운 pufETH 전환율을 가능하게 하는 "지연형 준비금 증명(lazy proof of reserves)"을 수행하도록 해줍니다. 자세한 내용은 기술 문서를 참조하세요.

중대한 조치를 취하기 위해서는 가디언 다수(예: 8명 중 7명)의 합의가 필요합니다.

탈중앙화를 향한 로드맵 (Roadmap to Decentralization)

완전한 프로토콜 레벨의 탈중앙화는 퍼퍼의 최종 목표입니다. 이는 프로토콜이 코어 팀, 제3자, 외부 주체에 대한 의존 없이 운영된다는 뜻입니다. 이 목표에 중요하게 기여하는 여러 이더리움 개선 제안(EIP)이 있습니다:

- **EIP-7002**: 구현되면, 스마트 컨트랙트에서 검증자 퇴출 트리거가 가능해져 가디언의 퇴출 감독 역할이 불필요해집니다.
- **EIP-4788**: 많은 Guardian 작업을 ZKP로 대체할 수 있게 해줍니다.
- **EIP-2537**: BLS 프리컴파일을 통해 온체인에서 검증자 등록 메시지 검증이 가능해져 가디언에 대한 신뢰를 줄여 줍니다.

이러한 EIP가 완전히 채택될 때까지 가디언은 과도기적 장치로서 기능합니다. 이들은 퍼퍼 프로토콜이 안전하게 성장하고 이더리움을 탈중앙화할 수 있도록 하며, 그 사이 스테이커가 위험과 불확실성으로부터 보호받도록 합니다. 현재는 중요한 역할이지만, 가디언의 역할은 스테이커 자산을 보호하고 이더리움의 끊임없이 변화하는 환경에서 프로토콜 성장을 보장하기 위한 임시적 장치입니다.

버스트 임계치 (Burst Threshold)

퍼퍼는 이더리움 검증자 세트에서 자사의 검증자 점유율을 22\%로 자체 상한할 것을 약속하며, 이를 프로토콜의 'Burst Threshold' 라고 부릅니다. 버스트 임계치에 도달했다고 해서 스테이킹과 노드 운영자 등록을 갑작스레 중단하는 대신, 퍼퍼는 임계치에 접근할수록 스테이커 수요를 자연스럽게 감소시키는 메커니즘을 도입합니다.

프로토콜이 22\%에 도달하면, 발행 가능한 검증자 티켓 수를 줄여 기존 검증자만 유지할 수 있고 신규 검증자는 추가되지 않도록 합니다.

이 약속은 이더리움의 안정성을 위협하는 33\%의 위험한 합의 임계치를 퍼퍼가 절대 넘지 않도록 보장하는 데 필수적입니다. 우리는 버스트 임계치가 프로토콜이 수익화된 이후가 아니라, 첫날부터 포함되어야 한다고 확신합니다.

노드 운영자(Node Operators)

우리 프로토콜은 퍼미션리스이므로 누구나 퍼퍼 노드 운영자가 될 수 있습니다!

퍼퍼 노드 운영자가 되려면 검증자를 운영해야 합니다. 노드 운영자는 환불 가능한 pufETH 본드를 잠그고, 검증자 티켓을 잠가야 하며(검증자 운영 일마다 소각됨), 그렇게 하면 검증자를 운영하기 위한 32 ETH가 할당됩니다.

본드와 검증자 티켓 (Bond and Validator Tickets)

본드는 슬래싱 및 비활성화에 대한 보험 역할을 합니다. 잠긴 검증자 티켓은 인센티브 정렬의 역할을 합니다. 잠근 검증자 티켓의 양이 노드 운영자가 검증자를 운영할 수 있는 기간을 결정합니다. 검증자 티켓에 대해서는 여기에서 더 알아보세요. ETH 본드는 최종적으로 pufETH로 전환되므로, 노드 운영자는 본드를 pufETH로 대체 예치할 수도 있습니다. 어느 경우든, 검증자가 비콘 체인에서 최소 32 ETH로 종료하고 슬래시되지 않았다면, 노드 운영자는 본드를 전액 반환받습니다. 슬래시는 없었지만 잔액이 32 ETH보다 적다면, 그 차액은 노드 운영자의 본드에서 차감됩니다.

> *검증자가 슬래시되면, 노드 운영자는 본드 전액을 몰수당합니다.*

노드 운영자 요구사항 요약 (NoOp Requirements Summary)

- 2 ETH 본드
- 최소 28개의 검증자 티켓
- 리스테이킹 모듈 선택
- 검증자

검증자 요구사항 (Validator Requirements)

- CPU: 쿼드 코어(또는 듀얼 코어 하이퍼스레딩) CPU

- 메모리: >= 16GB RAM
- 스토리지: 전체 노드용 2 TB SSD(NVMe SSD 권장)
    - 전체 아카이브 노드를 실행하려면 13.5 TB 이상 필요
    - 참고: 이더리움 블록체인이 성장함에 따라 주당 약 14GB의 추가 스토리지가 필요
- 대역폭: 다운로드 속도 >= 25 Mbps

자세한 내용은 Geth 하드웨어 요구사항을 참고하세요.

고지사항 (Disclaimers)

> *주의 : **EigenLayer Partial Withdrawals Proofs 개선 중***
> *현재 EigenPods에서 합의 보상을 출금하는 것은 비용이 과도하며, 아이겐레이어 팀이 비용 절감을 위해 작업 중입니다. 그때까지 합의 보상 출금은 일시적으로 비활성화되어 있습니다.*

노드 운영자 보상 (Node Operator Rewards)

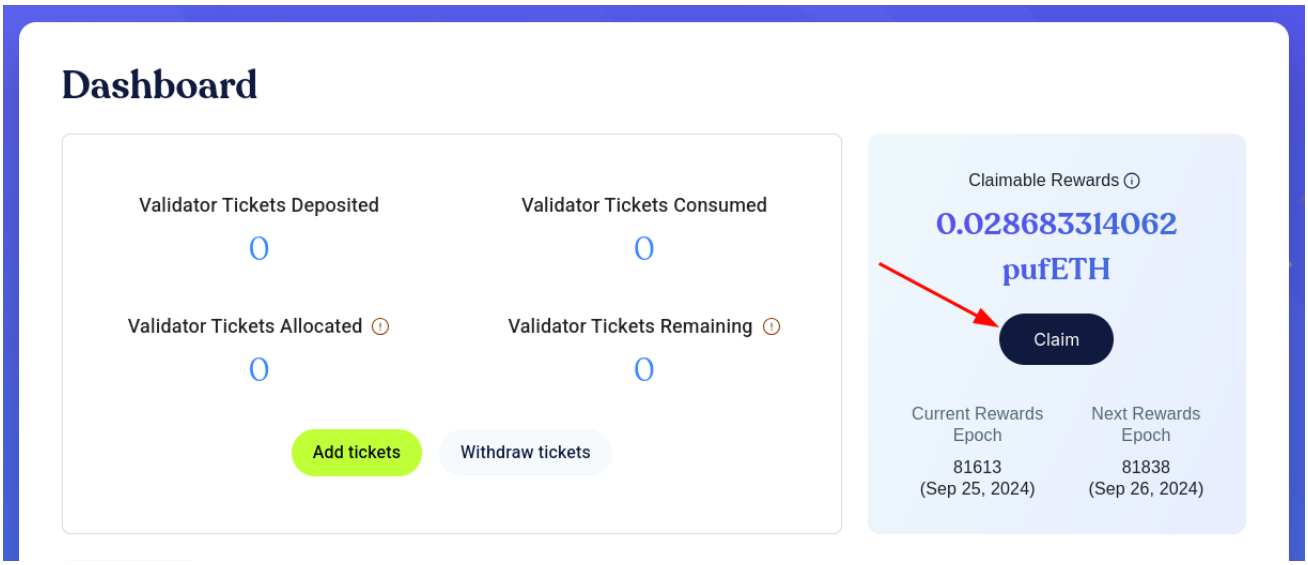
합의 레이어 보상 출금 (Withdrawing Consensus Layer Rewards)

노드 운영자는 다른 이더리움 검증자와 동일한 방식으로 보상을 받습니다. 다만 실행 레이어 보상은 정상적으로 획득되어 Beacon Node 클라이언트에서 설정된 수수료 수령자(fee recipient) 주소로 전송되는 반면, 합의 레이어 보상은 아이겐레이어 컨트랙트를 통해 흐르며 일반적으로 지연이 발생합니다.

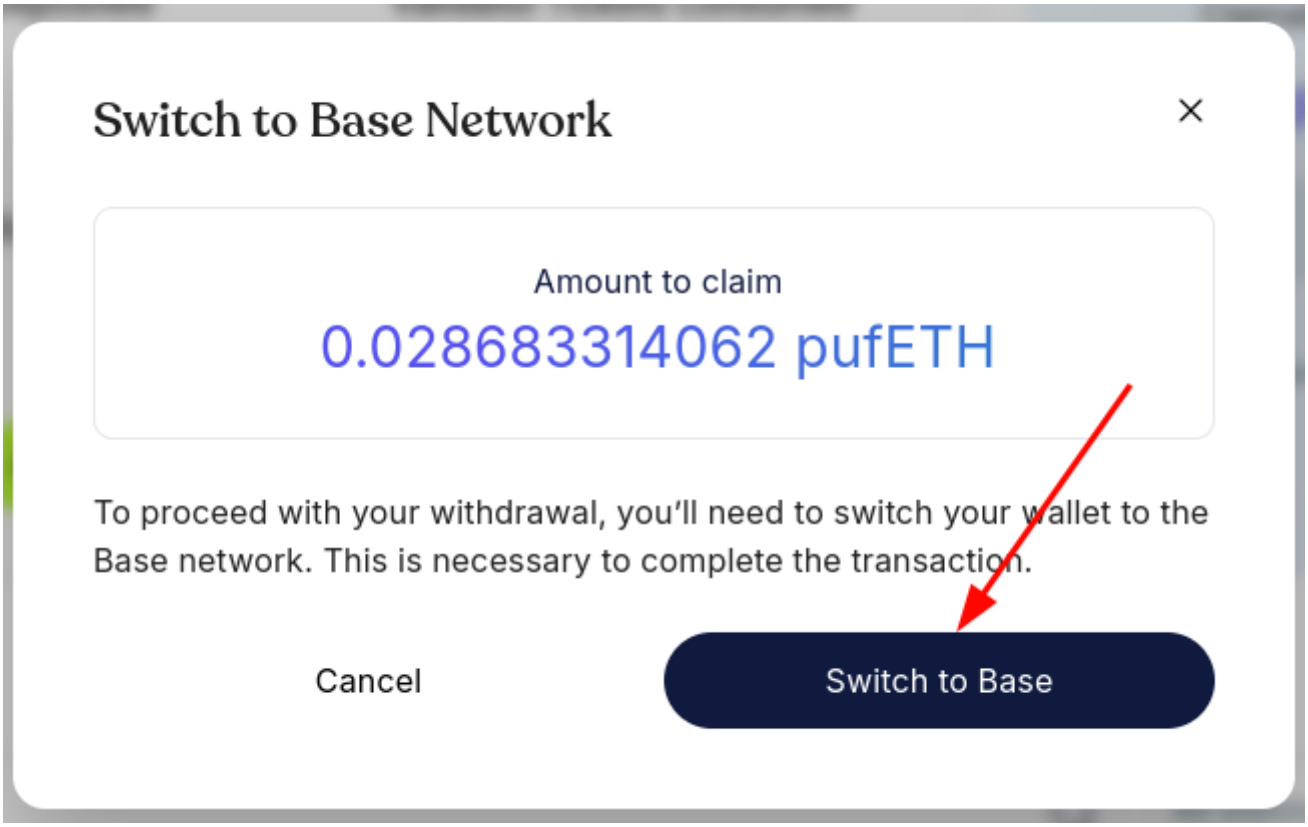
보상 출금 과정을 빠르고 가스 효율적으로 만들기 위해, 퍼퍼는 Base L2에서 보상을 출금할 수 있는 방식을 마련했습니다. 이 방식은 최소한의 가스로 출금이 가능하며, 검증자가 보상을 가능한 한 신속하게 그리고 필요한 만큼 자주 수령할 수 있도록 합니다. 노드 운영자의 합의 레이어 보상은 Everclear를 사용해 자동으로 Base L2로 브리징되며, 검증자는 이를 pufETH 형태로 출금할 수 있습니다.

보상을 출금하려면, 노드 운영자는 Puffer Dashboard에서 다음 단계를 따라 Base에서 트랜잭션에 서명해야 합니다:

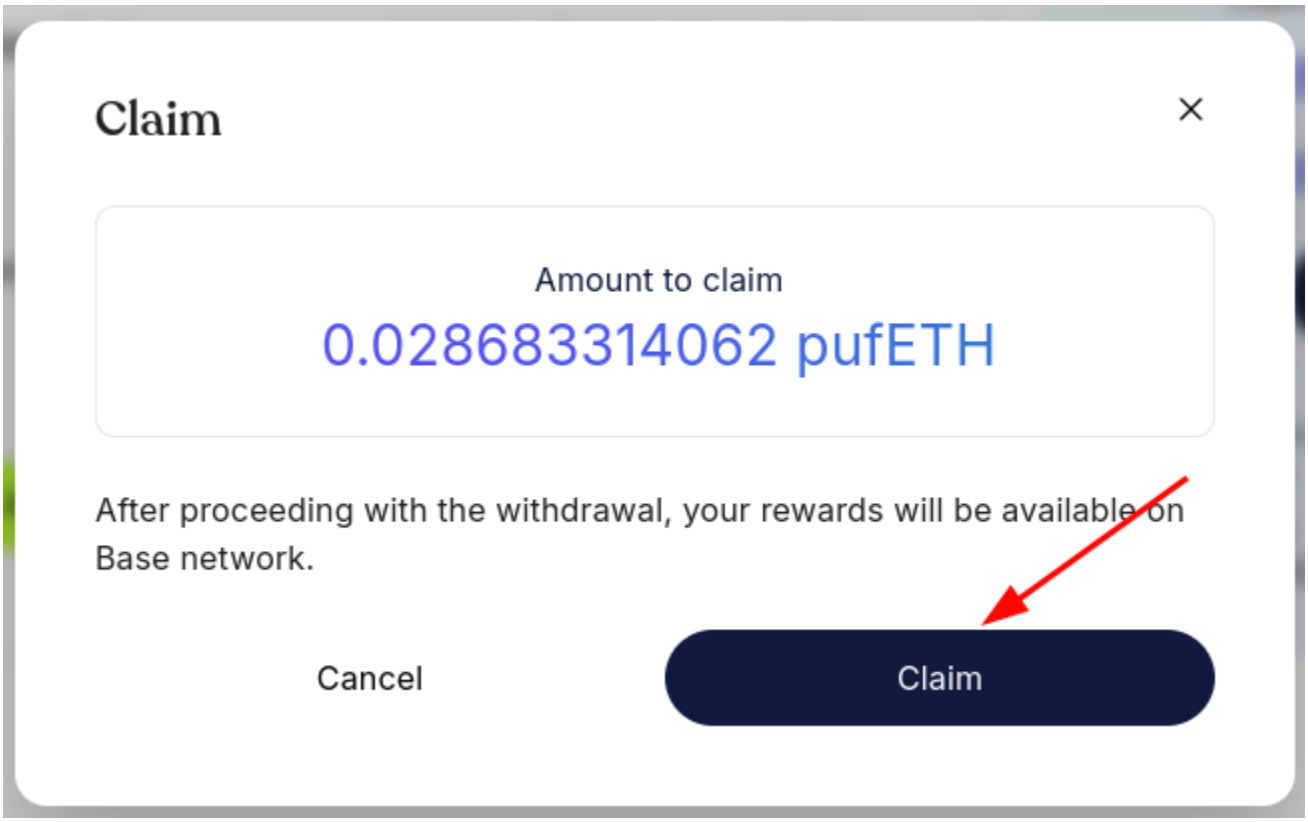
1. "Claim" 버튼 클릭



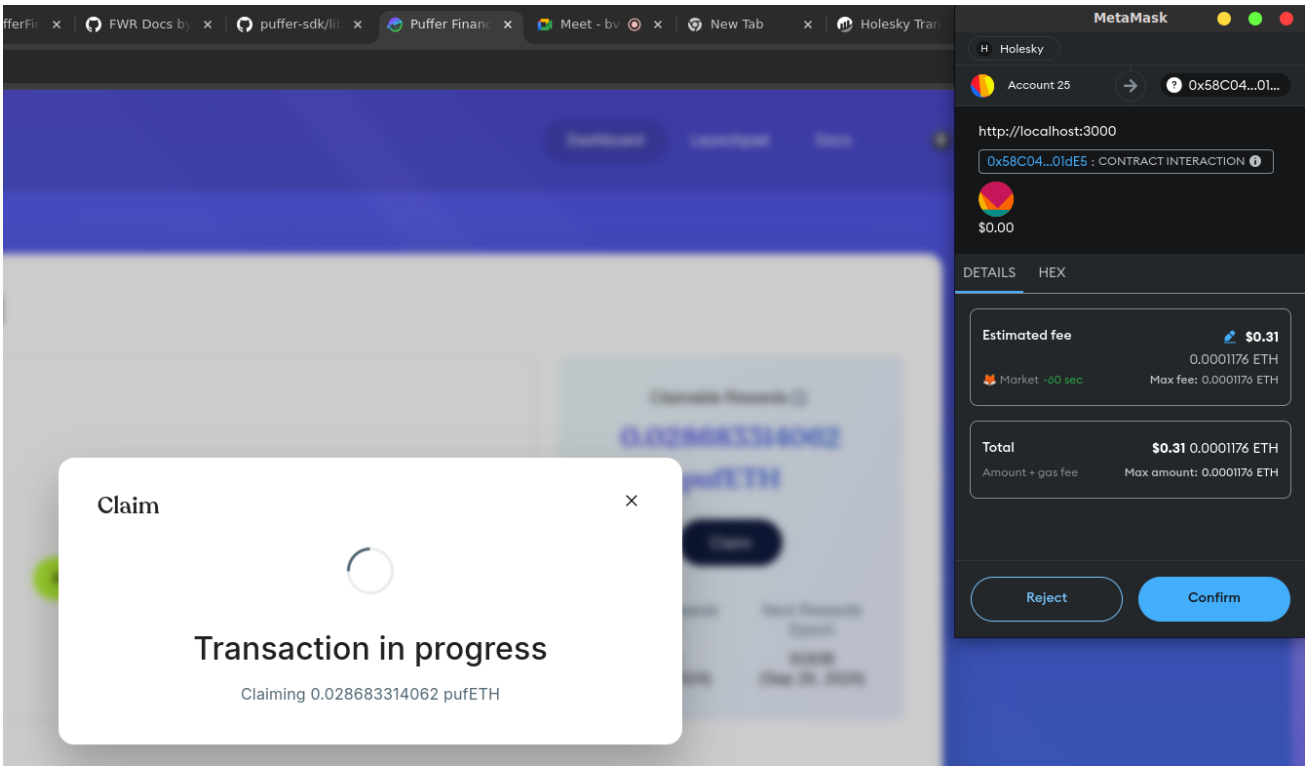
2. 지갑 네트워크를 Base로 전환 (청구 과정은 Base에서 진행되므로 필수). 가스를 위한 ETH가 충분히 있는지 확인.



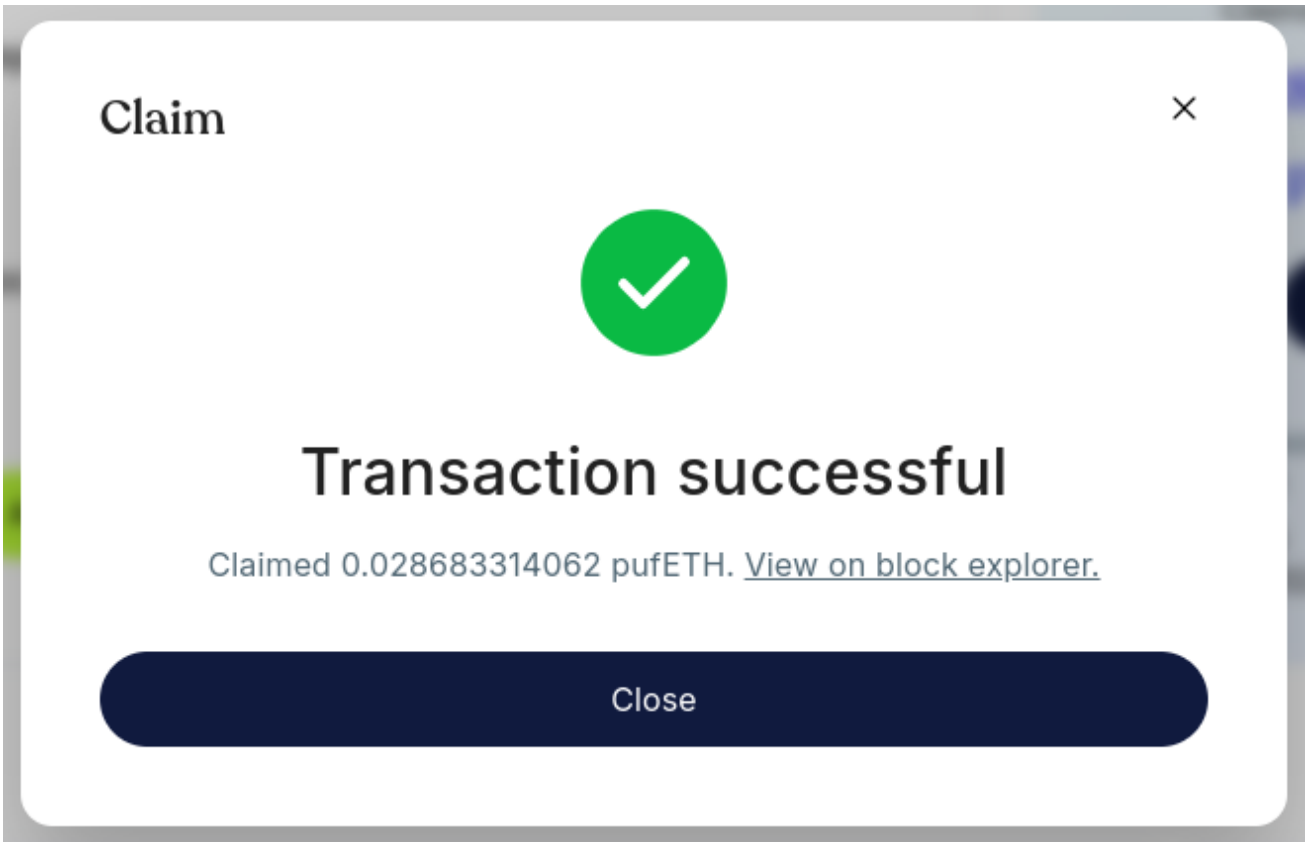
3. "Claim" 버튼 다시 클릭



4. 트랜잭션 세부정보를 검토 후 지갑으로 서명



5. 트랜잭션 확인 대기 → 확인되면 보상이 Base에서 수령됨



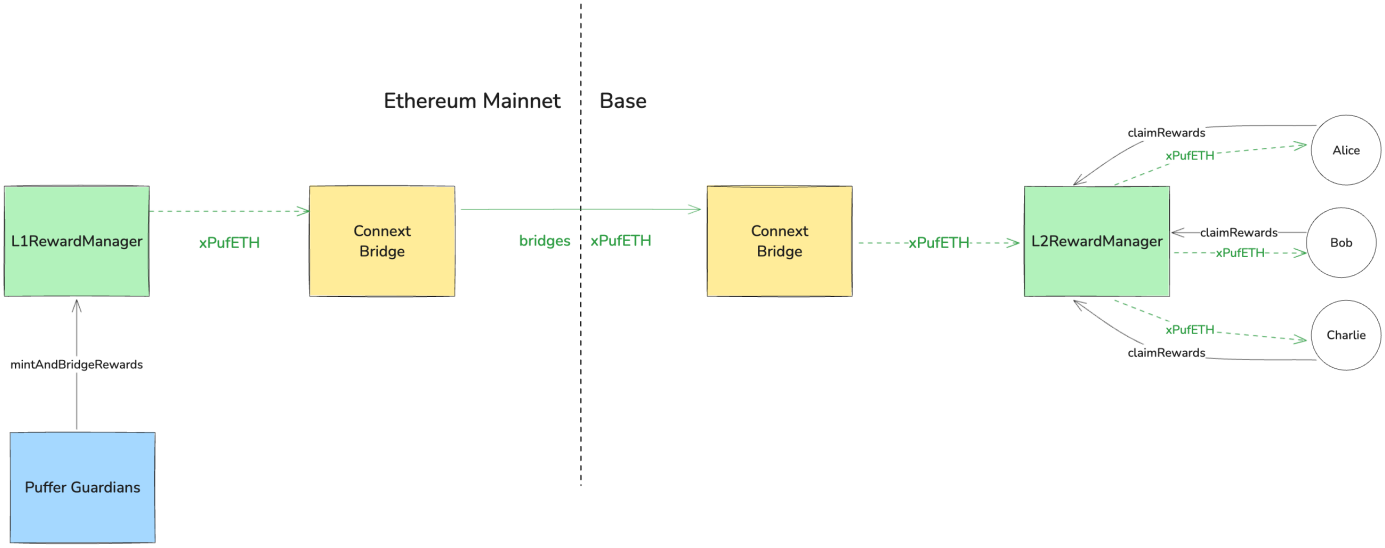
보상 청구 후, 노드 운영자는 이를 Ethereum L1으로 다시 브리징하거나 Base L2에서 활용할 수 있습니다.

보상 계산 방식 (How Rewards Are Calculated)

보상은 주 단위로 분배되며, 최초 분배는 퍼퍼 메인넷 출시 이후 누적된 모든 보상을 포함합니다.

각 주기마다 퍼퍼의 가디언은 다음 단계를 수행합니다:

1. 각 노드 운영자의 개별 보상 계산 (해당 검증자 전체 합산)
2. 이전 주기의 총 보상 합산
3. 보상에 대한 머클 트리를 생성 및 게시하고 AWS S3에 저장
4. pufETH 토큰을 민트해 Base L2 네트워크로 전송
5. 보안 취약 시 되돌릴 수 있도록 강제 대기 기간 설정
6. 대기 기간 종료 후, 노드 운영자는 Base의 L2RewardManager 컨트랙트를 통해 Puffer Dashboard에서 보상 청구 가능



보상 에포크와 회계 (Rewards Epochs and Accounting)

- **현재 보상 에포크(Current Rewards Epoch)**: 보상이 계산되어 Base에 게시된 시점까지의 에포크
- **다음 보상 에포크(Next Rewards Epoch)**: 다음 회계 이벤트에서 보상이 계산될 시점까지의 에포크

회계는 매주 월요일에 자동 실행되지만, 추후 변경될 수 있습니다.

> *퍼퍼는 Beacon Chain에서 검증자가 성공적으로 출금한 보상만 Base로 민트하고 전송합니다.*

보상 계산 검증 방법

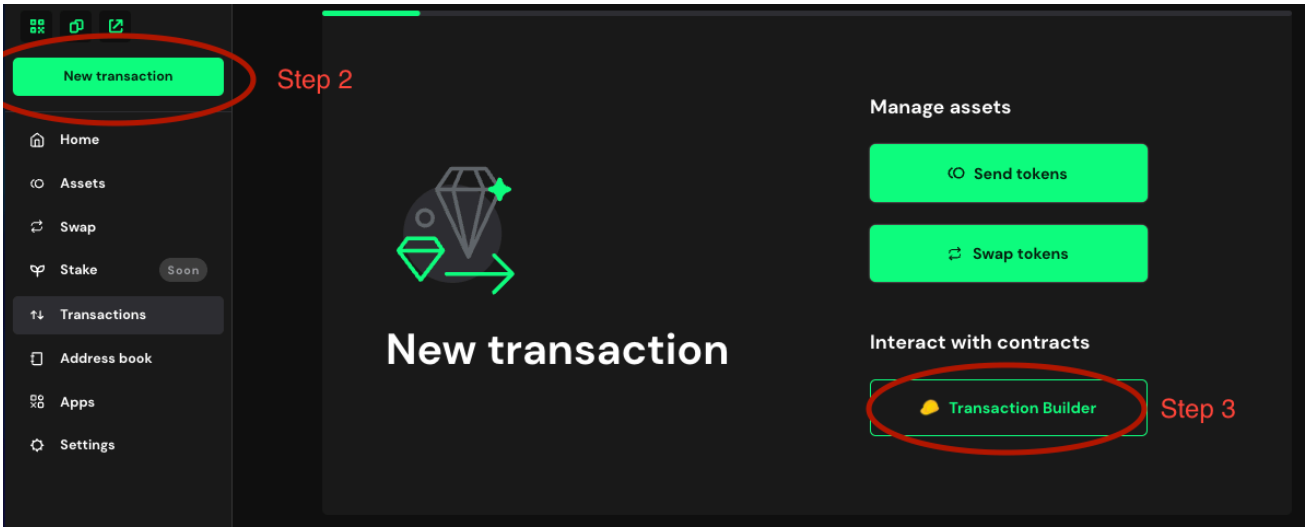
1. 대시보드에서 현재 보상 에포크를 확인합니다.
2. beaconcha.in (또는 유사 사이트)에서, 해당 에포크 이전까지의 검증자 출금을 확인합니다. 시작 시점은 마지막 퍼퍼 보상 청구 이후입니다.
3. 이 출금들을 모두 합산합니다.
4. 이 합계가 예상 ETH 보상이며, Step 1의 에포크에서의 환율로 변환해야 합니다.

보상 수령 주소 변경 (Changing Your Rewards Recipient Address)

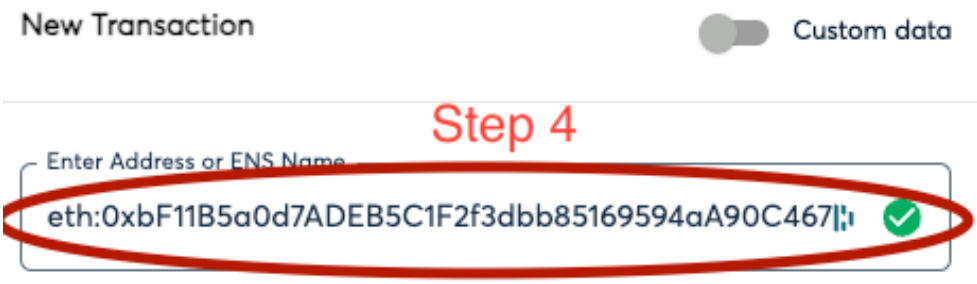
> *이더리움 메인넷에서 검증자를 등록할 때 멀티시그 지갑 같은 스마트 컨트랙트를 사용한 노드 운영자는, Base에서 특정 보상 청구 주소를 반드시 설정해야 합니다. 그렇지 않으면 Base에서 보상을 청구할 수 없습니다. 이유는 메인넷 주소와 Base 주소가 자동으로 매칭되지 않기 때문입니다. 따라서 Base에서 보상을 청구할 수 있는 주소를 명시적으로 지정해야 합니다.*

보상 청구 주소를 Base에서 변경하려면, 노드 운영자는 다음 단계를 따라야 합니다:

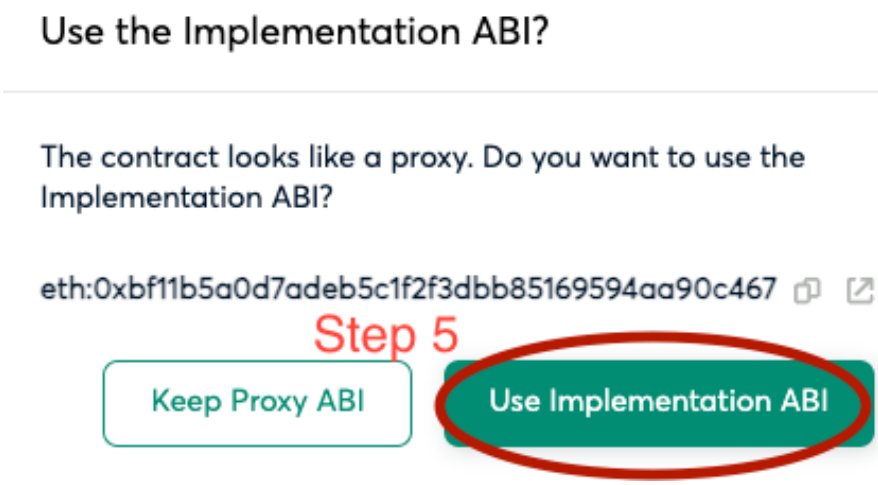
1. SAFE 계정으로 이동
2. `New transaction` 선택
3. `Transaction Builder` 선택



4. L1RewardManager 컨트랙트 프록시 주소 입력: 0x157788cc028Ac6405bD406f2D1e0A8A22b3cf17b

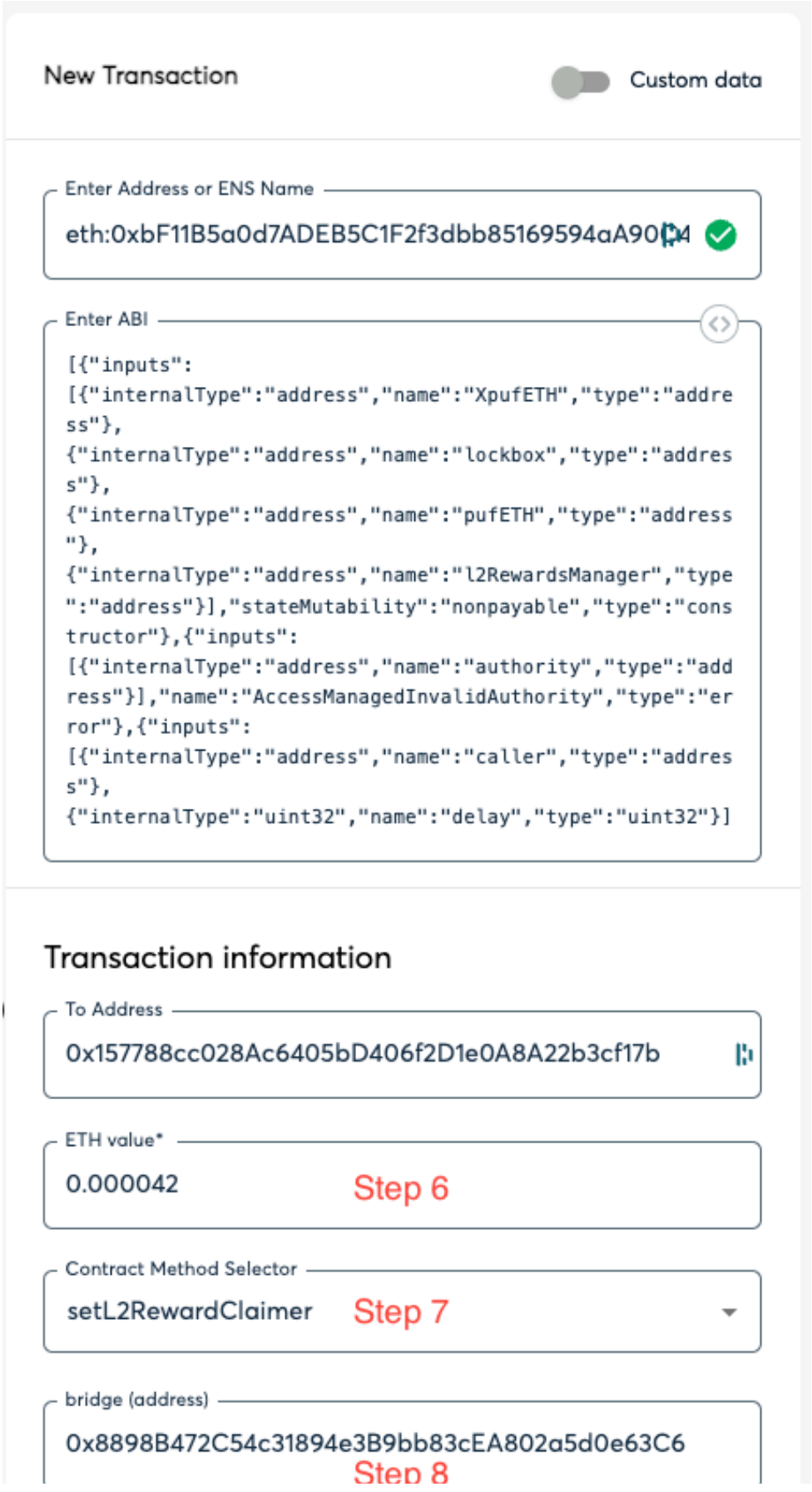


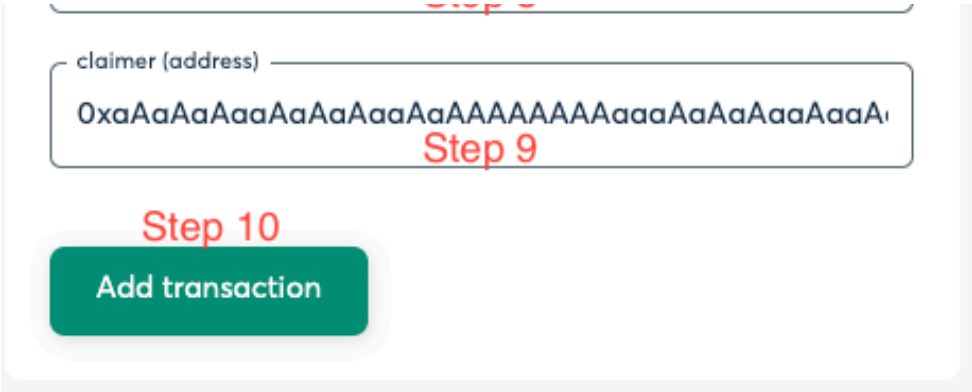
5. `Use Implementation ABI` 선택



6. `ETH value`를 소액(예: `0.000042`)으로 설정 → 트랜잭션을 Base로 브로드캐스트하는 브리지(relayer) 수수료
7. `Contract Method Selector`를 `setL2RewardClaimer`로 설정

8. `bridge (address)`를 Everclear 브리지 주소로 설정: 0x8898B472C54c31894e3B9bb83cEA802a5d0e63C6
9. Base에서 제어하는 새로운 보상 청구 주소 입력
10. `Add transaction` 클릭 후 SAFE 트랜잭션 서명





> ***note***
> *`To Address` 필드가 자동 입력되지 않으면, L1RewardManager 프록시 주소로 수동 입력해야 합니다: [0x157788cc028Ac6405bD406f2D1e0A8A22b3cf17b](0x157788cc028Ac6405bD406f2D1e0A8A22b3cf17b).*

11. 트랜잭션이 Ethereum Mainnet에서 Base L2로 브리징될 때까지 대기 (일반적으로 3~6시간, relayer 수수료 부족 시 더 오래 걸릴 수 있음).
12. 트랜잭션이 Base에서 확인되면, 노드 운영자는 지정한 보상 청구 주소를 사용해 보상을 청구할 수 있습니다.

> *Externally Owned Accounts(EOAs)는 이 단계를 수행할 필요가 없습니다. EOAs의 경우, 보상은 이더리움 메인넷에서 검증자를 등록한 동일한 주소로 자동 전송됩니다.*

거버넌스 (Governance)

미션 (Mission)

우리의 비전 (Our Vision)

퍼퍼는 사용자를 강화하고, 혁신을 촉진하며, 이더리움의 핵심 원칙을 지키는 탈중앙화 금융 생태계를 지향합니다. 퍼퍼는 항상 이더리움의 가장 중요한 가치인 **탈중앙화**를 보존하기 위해 노력해 왔습니다. 이러한 이유로 우리의 생태계는 퍼미션리스 검증자 운영을 촉진하는 데 중점을 두었습니다.

이러한 탈중앙화의 원칙을 우리 프로토콜 내에서 구현하기 위해, 우리는 탈중앙화 자율 조직(DAO)으로 전환하고 있습니다. 이는 퍼퍼의 미래가 중앙화된 권위가 아니라 토큰 보유자와 생태계 참여자로 이루어진 커뮤니티에 의해 결정되도록 합니다. DAO를 통해 우리는 단순히 탈중앙화를 주장하는 것을 넘어, 그것을 실제로 실현하며, 우리의 거버넌스가 이더리움 생태계에서 추구하는 가치와 동일하게 반영되도록 합니다.

우리의 생태계 (Our Ecosystem)

현재 퍼퍼 생태계는 다음을 포함합니다:

- Puffer LRT: 대표적인 리퀴드 리스테이킹 프로토콜
- Puffer UniFi: 우리의 베이스드 롤업 스택
- UniFi AVS: 최초의 베이스드 롤업 사전확인(preconfirmation) 서비스

우리의 약속 (Our Commitment)

성장 과정에서 우리는 퍼퍼를 다음과 같이 구축하겠다는 약속을 지켜왔습니다:

- 신뢰 불필요한 프로토콜 (Trustless protocol)
- 탈중앙화 인프라 (Decentralized infrastructure)
- 커뮤니티 거버넌스 생태계 (Community-governed ecosystem)

퍼퍼 재단 (The Puffer Foundation)

커뮤니티의 비전에 맞춰 성장을 보장하기 위해, 우리는 퍼퍼 재단을 설립했습니다. 그 임무는 다음과 같습니다:

- 초기 가이드 제공
- 투명한 거버넌스 촉진
- 완전한 커뮤니티 통제로의 전환 지원

커뮤니티 거버넌스 (Community Governance)

퍼퍼 토큰은 우리의 거버넌스 모델의 초석으로, 커뮤니티가 다음을 할 수 있도록 합니다:

- 주요 의사결정에 참여
- 퍼퍼 생태계의 미래를 형성
- 모든 활동에서 이더리움의 핵심 원칙을 지킴

포용적 참여 (Inclusive Participation)

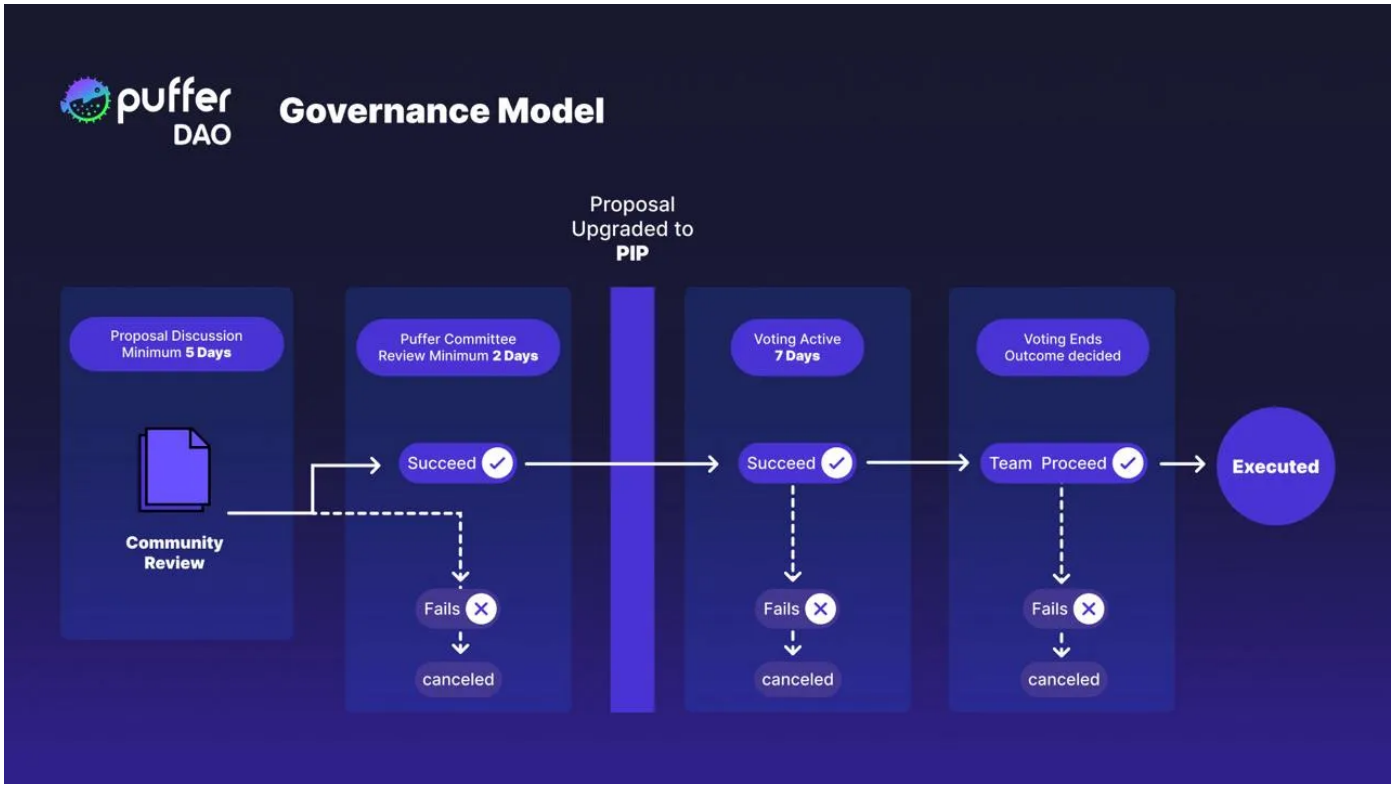
우리는 다양한 관점의 힘을 믿습니다. 따라서:

- 퍼퍼의 미션에 관심 있는 모든 이들에게 대화와 아이디어 기여를 환영합니다.
- 투표권은 토큰을 잠근 vePUFFER 보유자에게 주어지지만, 우리는 커뮤니티 전체의 의견을 소중히 여깁니다.
- 토큰 보유 여부와 관계없이, 여러분의 목소리는 프로토콜을 형성하고 이더리움 생태계에 기여하는 데 중요합니다.

우리는 단순히 프로토콜을 구축하는 것이 아니라, 이더리움 위에서 탈중앙화 금융의 미래를 만들어가고 있습니다.

거버넌스 이해하기 (Understanding Governance)

이 글에서는 거버넌스가 어떻게 작동하는지, 그리고 제안이 처음 생성되는 단계에서 커뮤니티와 퍼퍼 팀의 토론 및 검토를 거쳐 최종 투표 단계로 이동하는 과정을 설명합니다.



제안 생성 (Proposal creation)

우리는 누구나 제안을 만들 수 있는 생태계를 구축하여 거버넌스 과정을 민주화하고 있습니다. 제안은 먼저 퍼퍼 거버넌스 포럼의 해당 카테고리에 게시되며, 이후 거버넌스 관리 팀에 의해 PIP(Puffer Improvement Proposal)로 업데이트됩니다. 제안이 성공적으로 업데이트되려면 지정된 제안 템플릿을 사용하고 다음 세부사항을 반드시 포함해야 합니다:

- 포괄적 설명
- 명확한 근거
- 기대되는 이점
- 잠재적 위험

제출된 제안은 커뮤니티 검토를 위해 포럼에 게시됩니다. 향후에는 제출 수수료가 있는 퍼미션리스 제출 시스템 등 개선이 도입될 수 있습니다.

제안 토론 (Proposal Discussion)

최소 5일의 토론 기간 동안 커뮤니티 구성원들은:

- 피드백 제공
- 제안의 장단점 토론
- 개선 사항 제안

퍼퍼 거버넌스 포럼은 이러한 토론의 주요 플랫폼으로, 모든 제안의 평가가 투명하고 협력적으로 진행되도록 보장합니다.

제안 검토 (Proposal Review)

퍼퍼 거버넌스 검토 위원회는 제안의 준비 상태를 평가하는 중요한 역할을 합니다. 위원회는 다음 기준에 따라 제안을 평가합니다:

- 커뮤니티 피드백
- 퍼퍼의 장기적 목표와의 정렬
- 실행 가능성

최소 2일의 검토 과정을 거쳐 품질 높은 제안만이 투표 단계로 나아갑니다. 위원회는:

- 승인된 제안을 최종화하여 투표 준비
- 추가 개선 필요 시 제안자에게 피드백 전달
- 거부된 제안은 사유를 문서화하여 아카이브

승인된 제안은 다음 투표 에포크에 맞춰 큐잉됩니다.

제안 투표 (Proposal Voting)

거버넌스 과정의 마지막 단계는 투표이며, 이는 vePUFFER 보유자만 참여할 수 있으며 퍼퍼 투표 플랫폼을 통해 진행됩니다. 주요 투표 지침은 다음과 같습니다:

- 7일간의 투표 에포크
- 격주 목요일 0시(UTC)에 시작
- 정족수는 제안 유형에 따라 다름

    - 일반 제안은 단순 과반으로 통과
    - 인센티브 게이지의 경우, 프로토콜들이 투표를 두고 경쟁하며 사용자 인센티브가 배분됨
- 투표 종료 후 결과는 집계되어 거버넌스 포럼 및 공식 채널을 통해 공유

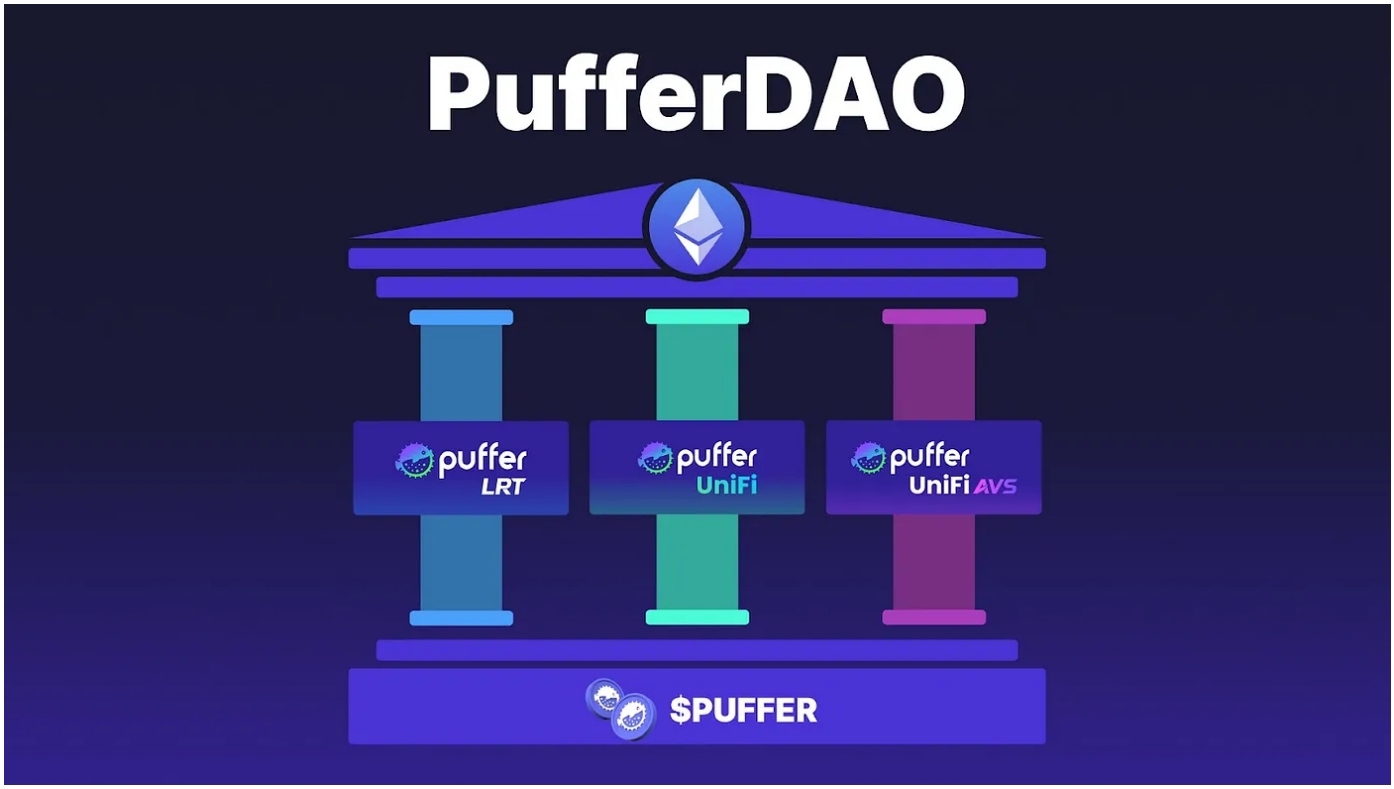
각 투표 에포크는 7일 동안 지속되며, 격주 목요일 0시(UTC)에 시작됩니다.

투표에 대한 자세한 내용은 Voting 문서를 참고하세요.

PUFFER 토큰

PUFFER 토큰은 퍼퍼 프로토콜과 UniFi 생태계의 네이티브 거버넌스 토큰입니다.

PUFFER의 역할



Puffer LRT

- 주요 프로토콜 파라미터(수수료, 한도, 본드 요건) 거버넌스
- 가디언과 리스테이킹 운영자 선택
- 지원 AVS 큐레이션

- 미래 기능: ETH를 다양한 운영자와 AVS에 할당하는 데 기여 (세부사항 추후 공개)

UniFi AVS

- 수수료 구조 관리
- AVS 지원을 위한 신규 롤업 화이트리스트
- AVS 보안 파라미터 감독
- 신규 사전확인(preconf) 및 제안자 약속(proposer commitment) 서비스 통합 가이드

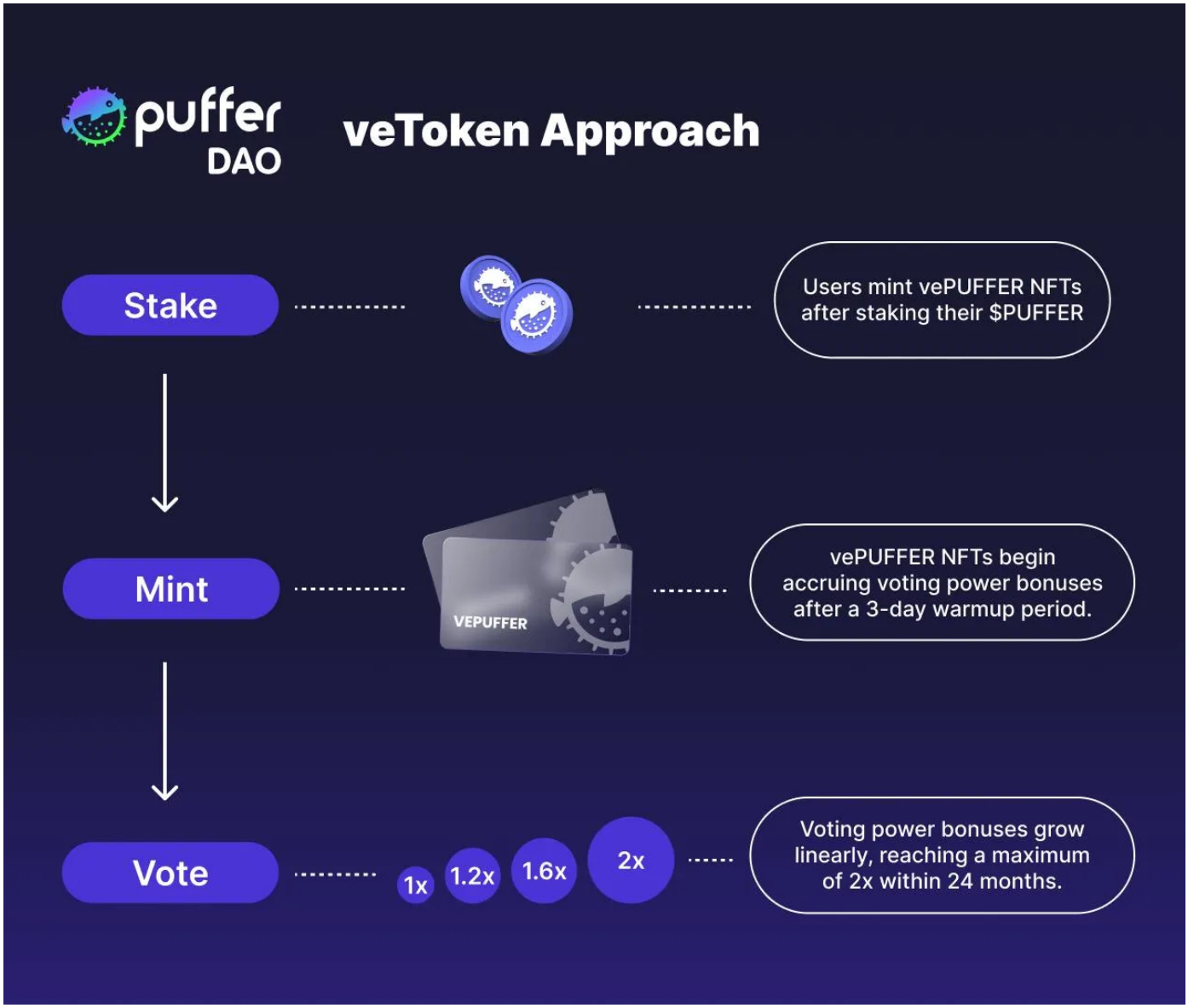
UniFi 롤업

- 롤업 트랜잭션 수수료 파라미터 설정
- 채택 촉진을 위한 생태계 보상 지시
- 장기적 지속 가능성을 위한 국고 자금 관리
- 롤업 업그레이드 결정 및 기능 우선순위 설정

---

vePUFFER

vePUFFER란?



vePUFFER는 Aragon과 협력해 개발된 ERC-721 기반의 새로운 ve(voting escrow) 거버넌스 메커니즘입니다. 이는 생태계 내에서 가치 정렬과 장기적 약속을 촉진한다는 퍼퍼의 장기적 목표에 맞춰 설계되었습니다.

주요 특징은 다음과 같습니다:

- 사용자가 PUFFER 토큰을 스테이킹하여 vePUFFER NFT를 발행 (예치 확인용)
- PUFFER가 vePUFFER로 스테이킹되어 있는 한, 시간이 지남에 따라 투표권이 축적
- 고정된 락업 기간 없음
- 사용자는 언제든 PUFFER를 언스테이킹할 수 있으며, 원래의 스테이킹된 PUFFER를 수령

다른 ve 토큰과 다른 점

vePUFFER는 Curve, Prisma 등 프로토콜의 교훈을 바탕으로 하되 몇 가지 핵심 혁신을 도입합니다:

- **유연한 스테이킹:** 기존 ve 토큰과 달리 락업 기간을 지정할 필요가 없음

- **동적 투표권:** 시간이 지남에 따라 투표권이 증가, 장기 참여를 보상
- **리셋 메커니즘:** 언스테이킹 시 축적된 투표권 초기화 → 장기 인센티브와 유연성 균형 유지
- **NFT 기반:** ERC-721로 구현되어 독창적 거버넌스 참여 가능성 제공
- **장기 참여 인센티브:** 지속적인 참여를 보상하는 투표권 누적 시스템
- **유연한 스테이크 관리:** 개인적/시장 상황에 따라 스테이킹 조정 가능

vePUFFER 활용

vePUFFER는 생태계 내 투표에 사용됩니다. 거버넌스에 참여하려면, 사용자는 PUFFER를 스테이킹하여 vePUFFER NFT를 발행하고, 주 단위로 투표권이 누적됩니다. 웜업 기간 이후 투표를 시작할 수 있으며, 이를 통해 사용자는 Puffer 생태계의 미래를 직접 형성할 권한을 가집니다.

---

vePUFFER 초기 파라미터

이 파라미터는 초기값이며, 향후 거버넌스 제안을 통해 커뮤니티가 변경할 수 있습니다.

카테고리	이름	설명	값
Voting Power Curve	Max Multiplier	무기한 스테이킹 시 달성되는 최대 부스트 배율	2x
Voting Power Curve	Max Duration	선형적으로 증가하여 최대 배율에 도달하는 데 걸리는 시간	2년
Voting Power	Warmup Period	스테이킹 후 최소 경과 시간(vePUFFER 활성화 및 투표 가능 시점)	3일
Voting Power	Cutoff Time	해당 투표 에포크에서 vePUFFER가 활성화되기 위한 스테이킹 마감 시간	매주 일요일 23:59:59 UTC
Voting Epoch	Epoch Period	투표가 진행되는 기간	7일
Voting Epoch	Start Time	모든 투표 시작 시간(vePUFFER는 이 시점에 최소 3일 이상 되어야 활성화됨)	목요일 00:00:00 UTC
Exit Queue	Cooldown	출금 대기열에 들어간 후 실제 출금까지 걸리는 기간. 이 기간 동안 투표권 없음	1개월
Exit Queue	Min Lock	출금 절차를 시작하기 전 최소 보유 기간	1개월
Exit Queue	Exit Fee Percent	출금 시 부과되는 세금 비율	0%
Escrow	Minimum Deposit	최소 예치 PUFFER 수	70 PUFFER

PUFFER 토큰 분배 (Allocations)



PUFFER 토큰은 총 공급량이 1,000,000,000개로 고정되어 있으며, 현재 초기 유통량은 102,300,000개 (10.23%)입니다.

아래 표는 PUFFER 토큰이 생태계 전반에 어떻게 배분되는지 보여줍니다.

분배 대상	비율	설명
생태계 및 커뮤니티	40%	활발한 생태계 구축, 커뮤니티 지원 보상, 지속 성장 보장. 향후 에어드랍 시즌, 커뮤니티 인센티브, 초기 거래소 유동성 제공에 사용.
에어드랍 시즌 1	7.5%	Crunchy Carrot Quest 시즌 1 에어드랍에 할당. 초기 서포터 보상. 첫날 65% 지급, 나머지는 6개월 동안 베스팅.
에어드랍 시즌 2	5.5%	Crunchy Carrot Quest 시즌 2 참여자에 할당. 시즌 1 스냅샷 이후(2024년 10월 5일) 시작.
투자자	26%	커뮤니티를 위한 제품 개발 자원 및 지원 제공. 3년간 베스팅(1년 클리프, 이후 2년 베스팅).
초기 기여자 & 고문	20%	퍼퍼 핵심 팀 및 고문에 할당. 3년간 베스팅(1년 클리프), 생태계 장기적 비전 실현을 보장.
Protocol Guild	1%	Protocol Guild Pledge에 따라 이더리움 코어 개발 지원. 4년에 걸쳐 베스팅. 이더리움 보안 및 확장성 강화 기여.

퍼퍼 거버넌스 로드맵

완전한 커뮤니티 거버넌스로의 전환은 단계적으로 이루어지며, 이는 원활하고 안전하며 효과적인 구현을 보장합니다. 프로토콜 발전에 따라 로드맵과 타임라인은 변경될 수 있습니다.

모든 단계에서 우리는 다음에 대한 약속을 유지합니다:

- 논의와 의사결정에 대한 폭넓은 커뮤니티 참여 촉진
- 모든 거버넌스 과정의 투명성 유지
- 혁신과 보안, 안정성 간 균형 유지
- 이더리움의 탈중앙화 및 퍼미션리스 원칙 준수

Phase 0: 초기 배분 및 오프체인 투표

- PUFFER 토큰 출시
- vePUFFER 민팅 도입
    - 사용자는 즉시 PUFFER를 잠가 vePUFFER NFT 민팅 가능
    - 이로써 미래 거버넌스 참여를 위한 투표권 축적 시작
- 커뮤니티 토론을 위한 거버넌스 포럼 개설
- 초기 커뮤니티 의견을 위한 오프체인 투표 메커니즘 도입
- AVS 화이트리스트 제안 초기 실행

Phase 1: vePUFFER 유틸리티 확장

- Aragon과 협력하여 vePUFFER 모델 전면 구현
- vePUFFER 보유자에게 향상된 유틸리티 제공:
    - 락업 기간 기반 투표권 강화
    - AVS 할당 게이지
    - 추가 프로토콜 보상/혜택 가능성
- 초기 인센티브 게이지 출시
- 초기 거버넌스 프로세스 롤아웃
- 커뮤니티 피드백 기반 거버넌스 메커니즘 개선
- UniFi 생태계 내 크로스-프로토콜 거버넌스 기회 탐색

Phase 2: 온체인 투표

- 오프체인에서 온체인 투표로 전환
- 거버넌스 제안 및 투표용 스마트 컨트랙트 구현
- 위임(Delegation) 탐색
- 점진적 거버넌스 범위 확대:
    - Puffer LRT: 프로토콜 파라미터, 수수료, 한도 조정
    - UniFi AVS: 수수료 구조 관리 및 신규 롤업 화이트리스트
    - UniFi 롤업: 수수료 파라미터 설정 및 생태계 보상 지시
- 복잡한 거버넌스 의사결정 프로세스 도입
- UniFi 보조금 프로그램 런칭 → 커뮤니티 주도 프로젝트 지원

Phase 3: 프로토콜 고착화 (Protocol Ossification)

- 완전 자율적이고 자급자족하는 거버넌스 모델로 전환
- 거버넌스 프로세스와 스마트 컨트랙트를 고착화

UniFi AVS 소개 (Introduction to UniFi AVS)

> ***UniFi AVS에 대한 정보***
> *UniFi AVS는 이더리움의 사전확인(preconfirmation, preconf) 생태계의 문제를 해결하기 위해 아이겐레이어 기반으로 구축된 솔루션입니다. 이는 퍼미션리스 검증자 참여, 온체인 레지스트리, 책임성을 위한 슬래싱 메커니즘을 제공합니다. 아이겐레이어 위에 구축되고 Commit-Boost와 통합된 UniFi AVS는 베이스드 롤업을 위한 빠르고 안전하며 중립적인 사전확인을 제공하여, 이더리움의 탈중앙화와 보안 원칙을 유지하면서 확장성을 강화합니다.*

UniFi AVS의 기능 🚀

프로토콜 기능

- 🟢 퍼미션리스: 아이겐레이어에서 리스테이킹된 모든 검증자가 참여 가능
- 📊 온체인 레지스트리: 투명하고 검색 가능한 사전확인자(preconfer) 레지스트리
- ⚖️ 슬래싱 메커니즘: 사전확인 약속에 대한 책임성 부과
- 🔗 아이겐레이어 통합: 자본 효율성 향상
- 🌟 혁신 촉진자: 이더리움 코어 프로토콜을 변경하지 않고도 빠른 혁신 가능

사전확인 서비스

- ⚡ 빠른 확인: 거의 즉시 수준(~100ms)의 트랜잭션 확인
- 🔒 보안: 경제적 보안으로 뒷받침된 이더리움 검증자의 강력한 보증
- 🌐 중립성: 편향 없는 운영에 대한 약속
- 💪 구속력 있는 약속: 중앙화된 시퀀서와 달리, 사전확인은 실질적 경제적 결과에 의해 보장

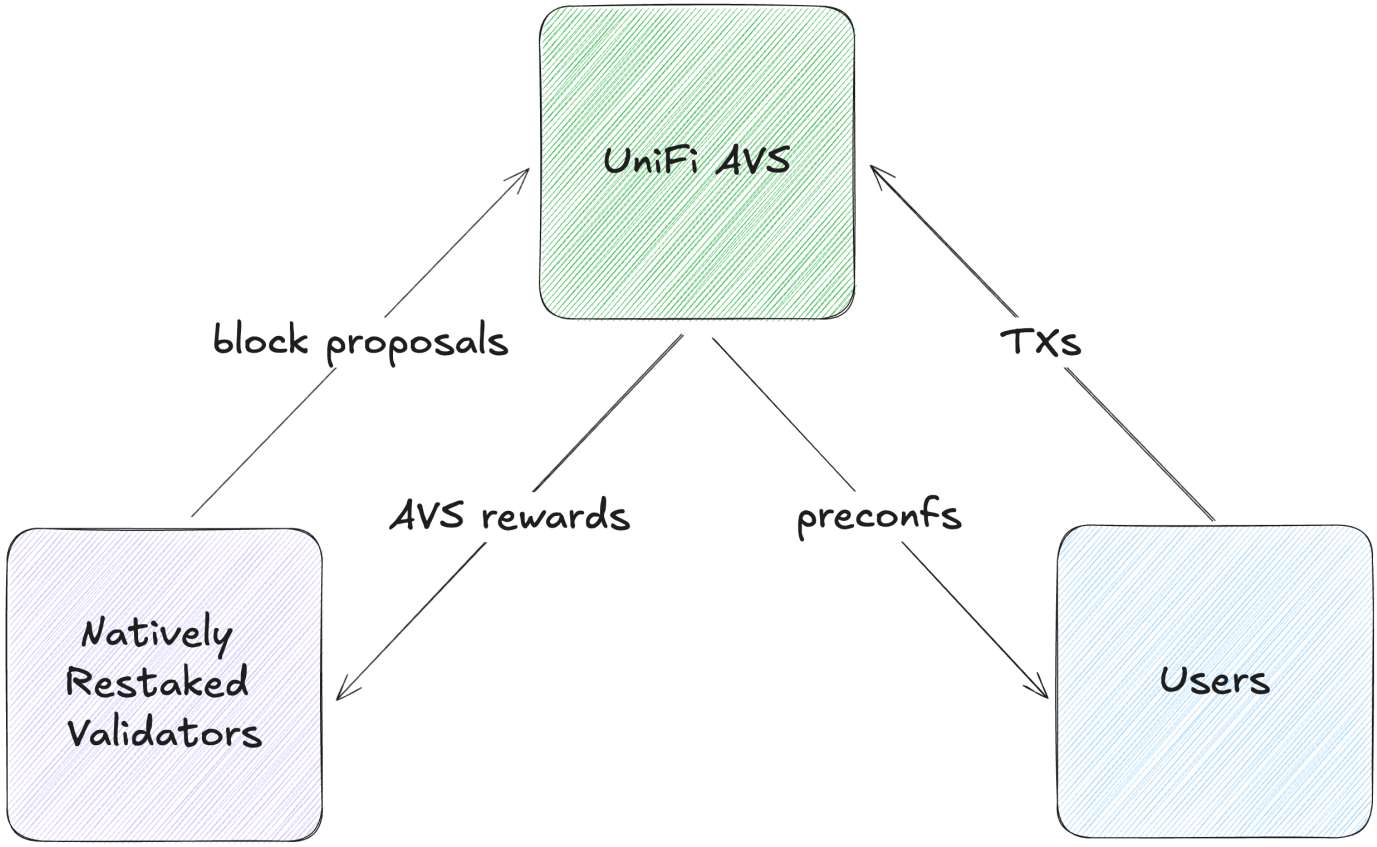
베이스드 롤업 실현

- 🔄 라이브니스 보장: 이더리움 L1의 강력한 라이브니스 상속
- 🛡️ 단순성과 보안: 기존 이더리움 인프라 활용
- 💰 경제적 정렬: MEV가 이더리움 L1로 환류
- 🤝 동기적 조합성: 다양한 베이스드 롤업 간 상호작용 가능
- ⚡ 속도 향상: 긴 L1 블록 타임의 한계 극복

Commit-Boost

- 🌟 오픈소스: 퍼블릭 굿으로 개발
- 🔧 표준화: 검증자 소프트웨어와의 손쉬운 통합 촉진

UniFi AVS 생태계 🌐



UniFi AVS는 이더리움의 핵심 원칙을 훼손하지 않으면서 이더리움의 역량을 강화하는 견고한 생태계를 만듭니다. 이는 검증자, 사용자, 그리고 더 넓은 이더리움 커뮤니티를 하나로 모아 더 빠르고, 더 안전하며, 더 효율적인 트랜잭션 처리를 제공합니다.

이 생태계는 **검증자(Validators)** 와 **사용자(Users)** 가 주도합니다:

- **검증자(Validators)** 는 EigenPod를 보유하고 Commit-Boost 소프트웨어를 실행함으로써 UniFi AVS에 참여할 수 있습니다. 그들은 사전확인(preconfirmation) 서비스를 제공하고, 네트워크의 보안과 효율성에 기여하는 동시에 추가 보상을 얻습니다.
- **사용자(Users)** 는 L1 트랜잭션과 베이스드 롤업 트랜잭션 모두에서 거의 즉시(~100ms) 트랜잭션 확인 혜택을 누립니다. 이는 사용자 경험을 크게 개선하여, 대체 L1 블록체인과 동등하거나 그 이상이 되게 합니다.

왜 UniFi AVS의 검증자가 되어야 하나요? 🤖

검증자는 이미 리스테이킹된 ETH를 활용하여 UniFi AVS에 참여할 수 있으며, 다음과 같은 이점을 제공합니다:

- 💰 추가 보상: 사전확인 서비스를 제공하여 추가 보상을 획득합니다.
- 🔒 자본 효율성: 추가 예치 없이 리스테이킹된 ETH를 사전확인 담보로 사용합니다.
- 🌐 네트워크 기여: 이더리움의 트랜잭션 속도와 사용자 경험 향상에 핵심 역할을 합니다.
- 🚀 혁신 참여: 이더리움 생태계의 최첨단 발전에 동참합니다.

> ***Tip***
> *UniFi AVS는 리스테이킹된 ETH 이외의 추가 담보 없이 검증자가 사전확인에 참여할 수 있도록 합니다. 이미 아이겐레이어에서 검증자를 운영 중이라면, 이 새로운 기회를 시작하기에 완벽한 위치에 있습니다!*

왜 UniFi AVS를 사용해야 하나요? 🚀

사용자와 개발자에게 UniFi AVS는 다음과 같은 중요한 이점을 제공합니다:

- ⚡ 속도: 거의 즉시(~100ms)의 트랜잭션 확인을 경험합니다.
- 🔒 보안: 경제적 보안에 의해 뒷받침되는 강력한 보증의 혜택을 누립니다.
- 🌐 생태계 개선: 더 효율적이고 사용자 친화적인 이더리움 생태계에 기여합니다.
- 🔗 호환성: 확장성을 강화하기 위해 베이스드 롤업과 원활하게 통합합니다.
- 🏗️ 구축 기회: 번개처럼 빠른 확인과 통합된 유동성을 갖춘 차세대 롤업을 구축하기에 완벽한 플랫폼입니다.

> ***Tip***
> *UniFi AVS는 보안이나 탈중앙화를 희생하지 않고 이더리움에 대체 L1의 속도를 제공합니다. 이는 단순한 개선이 아니라, 이더리움을 위한 혁신입니다!*

UniFi AVS는 이더리움 생태계의 보안성과 효율성을 최우선으로 합니다. 이를 보장하기 위해, 프로토콜은 다음을 수행합니다:

- 검증자가 EigenPods를 보유하고 Commit-Boost 소프트웨어를 실행하도록 요구합니다.
- 책임성을 위한 슬래싱 메커니즘을 구현합니다.
- 참여에 거버넌스 토큰 요구 사항을 두지 않음으로써 중립성을 유지합니다.

배경 (Background)

이더리움 확장성 과제 🏗️

이더리움은 제한된 트랜잭션 처리량과 높은 가스비 때문에 확장성 문제에 직면했습니다. 이로 인해 L2를 사용하여 이더리움을 확장하는 데 초점을 맞춘 롤업 중심 로드맵이 개발되었습니다.

롤업의 역할

롤업은 트랜잭션을 오프체인에서 처리한 후 결과를 배치로 이더리움 메인넷에 제출하여 이더리움의 트랜잭션 처리량을 높이는 것을 목표로 합니다. 그러나 전통적인 롤업은 다음과 같은 과제에 직면합니다:

- 🦕 느린 파이널리티: 이더리움 블록 확인에 최소 12초, 파이널리티에 12분이 필요합니다.
- 🔒 보안 상충: 일부 솔루션은 속도를 위해 보안을 타협합니다.
- 🌐 단편화된 유동성: 서로 다른 롤업은 유동성과 사용자가 분리되어 있습니다.
- 🎯 중앙화: 중앙화된 시퀀서는 롤업의 단일 실패 지점이 될 수 있습니다.

베이스드 롤업: 한 단계 도약 ⚡

베이스드 롤업은 이러한 많은 과제에 대해 유망한 해결책을 제공합니다.

베이스드 롤업의 핵심 특징

베이스드 롤업은 다음과 같은 특성을 가진 롤업입니다:

- 🔄 이더리움 검증자가 트랜잭션을 시퀀싱합니다.
- 🔗 이더리움의 보안을 직접 상속합니다.
- 🤝 서로 다른 베이스드 롤업 간 동기적 조합성을 가능하게 합니다.
- 💰 경제적 인센티브를 이더리움 L1과 정렬합니다.

베이스드 롤업의 속도 과제

장점에도 불구하고, 베이스드 롤업은 중요한 문제에 직면해 있습니다:

- ⏳ 느린 확인 시간: 베이스드 롤업은 이더리움의 블록 타임(12초)에 의해 제한되며, 많은 애플리케이션이 원하는 것보다 느린 트랜잭션 확인을 야기합니다.

사전확인(Preconfirmations): 레이턴시 해법 🚀

베이스드 롤업의 속도 제한을 해결하기 위해 사전확인(preconfirmations) 개념이 도입되었습니다.

사전확인이란?

사전확인은 이더리움 검증자 네트워크를 활용하여 거의 즉시의 트랜잭션 보증을 제공합니다. 동작 방식은 다음과 같습니다:

- ⚡ 약 ~100ms의 트랜잭션 확인을 제공하여 대기 시간을 급격히 줄입니다
  - 검증자는 유입되는 트랜잭션을 빠르게 처리하고 서명합니다
  - 이 서명은 L1에 블록이 게시되기 전 즉각적인 보증 역할을 합니다

- 🛡️ 이더리움 검증자의 경제적 보안으로 뒷받침됩니다
  - 검증자는 담보로 ETH를 스테이킹하여 정직한 행동을 보장합니다
  - 사전확인 약속을 위반하면 스테이킹 자산 슬래싱으로 이어질 수 있습니다
- 🌐 중립성과 탈중앙화를 유지합니다
  - 다수의 검증자가 참여해 단일 실패 지점을 방지합니다
  - 개방형 참여로 중앙 권위가 과정을 통제하지 못하도록 합니다
- 🔄 트랜잭션 제출과 블록 확인 사이의 간극을 메웁니다
  - 사용자는 트랜잭션 유효성에 대한 신속한 피드백을 받습니다
  - 롤업은 L1 파이널리티 전에도 자신 있게 트랜잭션을 처리할 수 있습니다

사전확인 프로토콜 요구사항 🛠️

베이스드 롤업을 위한 효과적인 사전확인 프로토콜을 구축하려면, 여러 핵심 요구사항을 충족해야 합니다:

1. **검증자 네트워크**: 🌐
   - 사전확인에 참여하려는 이더리움 검증자 네트워크
   - 적격한 검증자 누구나 참여할 수 있는 개방형 시스템
2. **경제적 인센티브**: 💰
   - 정직한 참여를 보상하는 시스템
   - 악의적 행위(안전성 결함) 또는 불이행(라이브니스 결함)에 대한 페널티(예: 슬래싱)
3. **보안 보증**: 🔒
   - 검증자 커밋에 대한 암호학적 증명
   - 사전확인의 무결성을 보장하는 메커니즘
4. **표준화**: 🔧
   - 참여 검증자의 온체인 레지스트리
   - 검증자 소프트웨어를 위한 공통 인터페이스
5. **자본 효율성**: 💼
   - 추가 자본 잠금 없이 검증자가 참여할 수 있는 메커니즘
   - 리스테이킹 프로토콜과의 통합 가능성

이러한 요구사항을 충족함으로써, 사전확인 프로토콜은 베이스드 롤업에 대해 거의 즉시이면서도 안전한 트랜잭션 확인을 가능하게 하는 필수 인프라를 제공하여, 이더리움 생태계의 사용자 경험과 효율성을 크게 향상시킬 수 있습니다.

UniFi AVS: 사전확인의 개척자 🦄

UniFi AVS는 베이스드 롤업을 위한 사전확인 프로토콜의 첫 구현체로 나섭니다.

아이겐레이어의 리스테이킹 역량과 Commit-Boost의 표준화를 결합함으로써, UniFi AVS는 베이스드 롤업을 위한 견고하고 효율적이며 안전한 사전확인 시스템을 구축합니다.

이 독특한 조합을 통해 UniFi AVS는 다음을 제공합니다:

1. 🟢 퍼미션리스 검증자 참여
2. 📊 투명성을 위한 온체인 레지스트리
3. ⚖️ 책임성을 위한 슬래싱 메커니즘
4. 🔗 베이스드 롤업과의 원활한 통합
5. ⚡ 거의 즉시이면서도 안전한 트랜잭션 확인

다음 섹션에서 그 방법을 알아보세요 👉

UniFi AVS 프로토콜

개요 (Overview)

UniFi AVS는 사전확인(pre-conf) 작업을 처리하는 오프체인 소프트웨어와, 등록·보상·패널티를 처리하는 온체인 AVS 스마트 컨트랙트로 구성됩니다.



정의 (Definitions)

UniFi AVS 생태계에는 몇 가지 핵심 구성 요소와 주체가 있습니다:

- **사용자(Users)**: 사전확인을 위해 트랜잭션을 제출하는 개인 또는 애플리케이션.
- **운영자(Operators)**: UniFi AVS 프로토콜의 일부로 이더리움 검증자를 제어하는 주체.
- **UniFiAVSManager**: 운영자 및 검증자 등록을 관리하고 전체 상태를 유지하는 온체인 컨트랙트.
- **Gateway**: 사용자와 운영자 사이에서 사전확인 요청을 중개하는 오프체인 엔티티.
- **Beacon Node**: 비콘 체인의 현재 상태(검증자 세트, 다가오는 블록 제안자 등)를 제공하는 검증자 스택의 일부.
- **Commit-Boost**: 검증자와 다양한 커밋 모듈 간 인터페이스를 표준화하는 오픈소스 소프트웨어.
- **RewardsManager**: 참여도와 성과에 따라 운영자, 검증자, Gateway에 보상을 분배하는 온체인 컨트랙트.

프로토콜 아키텍처 (Protocol Architecture)

UniFi AVS 사전확인 플로우 (Preconf Flow)

UniFi AVS의 사전확인 플로우는 여러 상호작용으로 구성됩니다:

1. 운영자는 자신의 delegate key를 Gateway로 지정
2. Gateway는 Beacon Node에 질의해 다가오는 블록 제안자 목록(lookahead window)을 확인
3. Gateway는 다가오는 제안자 중 자신에게 위임된 검증자가 있는지 확인
4. 사용자는 Gateway의 preconf RPC/라우터에 트랜잭션을 전송
5. Gateway는 사용자에게 서명된 사전확인을 반환
6. Commit-Boost는 블록 제안 시점에 Gateway로부터 L1 블록을 요청
7. 검증자가 Ethereum 네트워크에 L1 블록을 제안
8. RewardsManager를 통해 보상이 분배

무엇이 사전확인되는가? (What is being preconfed?)

UniFi AVS는 향후 다양한 proposer commitment 유형을 지원할 수 있는 유연하고 일반적인 프로토콜로 설계되었습니다. 초기에는 **L2 실행 사전확인(L2 execution preconfirmation)** 에 초점을 맞춥니다. 이는 베이스드 롤업 사용자에게 강력한 보장을 제공합니다.

L2 실행 사전확인은 다음과 같이 작동합니다:

1. **트랜잭션 보장**: 사용자는 자신의 트랜잭션이 L2 블록에 포함되고 사전확인된 대로 실행됨을 보장받습니다.
2. **즉시 확인**: L1 블록 제안까지 수 분이 남아 있어도, 사용자는 L2 트랜잭션(예: 스왑)을 제출하고 즉시 확인을 받습니다.
3. **결과 확약**: 사용자는 특정 결과(예: 스왑 결과)에 대한 사전확인을 즉시 수령합니다.
4. **실행 보장**: 나중에 블록 제안자가 L1 블록을 제안하고 L2 상태를 커밋할 때, 해당 트랜잭션은 사전확인된 대로 정확히 실행됩니다.
5. **경제적 보안**: 사전확인 약속을 위반할 경우, 검증자는 슬래싱되어 경제적 인센티브가 정직한 실행을 보장합니다.

이 개념은 L2 블록이 L1에서 최종 확정되기 몇 분 전에도 포함과 실행에 대한 강력한 보장을 가능하게 하며, 사용자 경험을 대폭 향상시키면서도 이더리움 롤업의 보안성과 탈중앙화를 유지합니다.

향후 UniFi AVS는 추가적인 사전확인 유형을 지원해, 이더리움 생태계 내에서 그 활용도를 더욱 확장할 수 있습니다.

온체인 구성요소 (On-Chain Components)

UniFi AVS는 여러 스마트 컨트랙트를 활용하여 운영을 관리합니다:

1. **UniFiAVSManager**: 운영자 및 검증자 등록을 포함한 AVS 등록 관리
2. **RewardsManager**: 운영자, 검증자, Gateway에 대한 보상 분배 관리
3. **DisputeManager**: 부정행위 검증자를 처벌하는 슬래싱 메커니즘 구현

등록 프로세스 (Registration)

UniFi AVS는 운영자와 검증자를 위한 **이중 옵트인(double opt-in) 등록 절차**를 구현하여 보안성과 유연성을 확보합니다:

1. **운영자 온보딩 (Operator Onboarding)**
    - 운영자는 먼저 아이겐레이어의 위임 시스템에 등록
    - 이후 UniFi AVS에 옵트인 → 참여 의사 표시
    - 등록은 아이겐레이어의 AVS 디렉토리에 기록됨

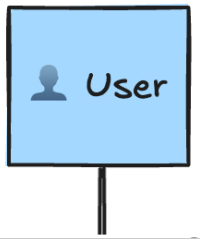
2. **커밋 선언 (Commitment Declaration)**
    - 운영자는 서비스 파라미터 지정:
        - 사전확인 서명을 위한 delegate key
        - 지원 베이스드 롤업 체인 ID
    - 두 단계 프로세스(변경 시작 → 지연 후 최종화)를 통해 안전성 보장
3. **검증자 등록 (Validator Enrollment)**
    - 운영자는 EigenPod에 연결된 검증자를 등록
    - 시스템은 EigenPod의 위임 적절성, 검증자 활성 상태 확인
    - 검증자의 BLS 공개 키 해시로 등록 완료
4. **단일 키 관리 (Unified Key Management)**
    - 하나의 delegate key가 운영자의 모든 등록 검증자를 대표
    - 향후 다양한 키 타입 지원
5. **체인 지원 선언 (Chain Support Declaration)**
    - 운영자는 256비트 비트맵을 사용해 지원하는 체인을 표시
    - 각 비트가 특정 체인 ID를 나타냄

보상 분배 (Rewards Distribution)

UniFi AVS는 검증자에게 매력적이면서도 안정적인 인센티브를 제공하기 위해 보상 분배 메커니즘을 설계했습니다:

1. **사전확인 수수료**
    - 사용자들이 지불하는 실행 사전확인 수수료가 주요 보상원
    - 수익 변동성과 개별 검증자 보상 빈도 불규칙 가능
2. **MEV 스무딩 (MEV-Smoothing)**
    - 보상을 시간에 따라 고르게 분배
    - 변동성과 불규칙성을 완화
    - 안정적이고 예측 가능한 수익 흐름 제공
    - 대규모 운영자 독점 완화
3. **ETH 지급**
    - 모든 보상은 ETH로 지급
    - 유동성과 단순성 보장
    - 비유동적 또는 비네이티브 토큰 문제 방지

4. **경쟁력 있는 수익**
    - 전통적인 PBS(Proposer-Builder Separation)보다 더 많은 수익 가능성
    - 검증자의 참여를 유도하는 강력한 경제적 인센티브 제공



보상 청구 (Claiming Rewards)

- 보상은 L2에서 각 검증자 단위로 분배됨
- 검증자는 자신의 BLS 키로 EIP-712 해시 서명을 통해 보상 컨트랙트에 청구자 주소를 설정 가능
- 미청구 보상은 누적되며, 언제든 한 번의 트랜잭션으로 전액 청구 가능
- 추가로 아이겐레이어 AVS에서도 일부 보상이 분배될 수 있으며, 운영자는 이를 아이겐레이어 인터페이스에서 직접 청구 가능

슬래싱 메커니즘 (Slashing Mechanism)

UniFi AVS는 **DisputeManager** 컨트랙트를 사용하여 슬래싱을 처리하고 운영자의 정직한 행동을 인센티브화합니다:

1. **안전성 위반 (Safety Faults)**: 실행 사전확인 보증 위반 시 패널티
2. **라이브니스 위반 (Liveness Faults)**: 사전확인 서명 후 블록 제안을 누락했을 경우 패널티
3. **러그 풀링 (Rug Pulling)**: 보상 스무딩을 무시하고 블록 보상을 탈취한 경우 패널티

> ***주의 (caution)***
> *슬래싱 메커니즘의 구체적 구현은 아직 확정되지 않은 아이겐레이어의 슬래싱 설계에 따라 달라집니다.*



퍼퍼 기관용 스테이킹 솔루션 (Institutional Staking Solution)

퍼퍼 기관 솔루션

퍼퍼는 기관이 자산에 대한 완전한 통제권을 유지하면서도 수익을 최적화할 수 있도록 설계된 안전하고 맞춤형 스테이킹 및 리스테이킹 플랫폼을 제공합니다.

🚀 소개

퍼퍼의 기관 솔루션은 조직이 스테이킹 수익을 극대화하는 방식에서 패러다임 전환을 제공합니다. 전통적인 고정 수익 스테이킹 모델과 달리, 퍼퍼는 **리스테이킹 메커니즘**을 통해 추가적인 수익원을 창출할 수 있게 합니다. 아이겐레이어를 활용하여, 기관은 여러 AVS를 동시에 보호하면서도 강력한 보안과 통제를 유지할 수 있습니다.

플랫폼은 유연한 아키텍처를 제공하여 기관이 위험 성향과 재무 목표에 맞게 전략을 조정할 수 있습니다. 예를 들어, 일부 ETH는 안정적 수익을 위해 전통적 스테이킹에 배분하고, 나머지는 리스테이킹에 참여하여 추가 수익을 창출할 수 있습니다.

🧩 핵심 구성 요소 (Core Components)

퍼퍼 자산매니저(AccessManager) 스마트 컨트랙트

- 볼트 접근 권한과 관리 권한을 통제하는 핵심 보안 프레임워크
- OpenZeppelin 기반으로 구축, 다중서명(Multisig) 지갑 또는 EOA로 구성 가능
- 기능: 업그레이드 제어, 세분화된 권한 관리

퍼퍼 기관 컨트랙트 볼트(Institutional Contract Vault)

- 기관 ETH 및 검증자 운영을 안전하게 관리하는 중심 컨트랙트
- OpenZeppelin 기반 맞춤형 보안 컨트랙트
- 기능: 검증자 배포, 리스테이킹 운영, 보상 분배
- 전통적 스테이킹과 리스테이킹을 동시에 관리하되 자산과 보상을 명확히 분리

퍼퍼 리스테이킹 운영자(Restaking Operator)

- EOA 형태로 구현
- 다양한 AVS 등록 및 리스테이킹 보상 관리 담당

보안 프레임워크 (Security Framework)

- **AccessManager**: OpenZeppelin의 사전 감사 템플릿 사용
- **볼트 컨트랙트**: 선도 보안 기업들의 종합 감사 완료
  - BlockSec 감사 보고서
  - SpearBit 감사 보고서
- **EigenLayer 통합**: 자체 감사 프레임워크로 추가 보안 레이어 제공