SOOHO.IO

BLOCKCHAIN SECURITY INCIDENT BULLETIN

KelpDAO rsETH / LayerZero 브릿지 보안 사고 정보 알림

2026년 4월 18일 발생한 약 USD 292M 규모의 cross-chain 브릿지 유출 사고에 대한 공개 자료 기반 사실관계 및 기술 구조 정리

발행일

2026-04-24

문서 유형

정기 보안 알림 (Bulletin)

작성

SOOHO.IO Security Research

버전

v1.3 · 2026-04-24

SUMMARY

집행 요약

2026년 4월 18일 17:35 UTC, **KelpDAO**가 발행한 유동성 리스테이킹 토큰(LRT) **rsETH**의 cross-chain 브릿지 경로에서 약 **116,500 rsETH (미화 약 290–294M)**가 정상적인 원천 체인 소각 절차 없이 Ethereum 체인 Escrow 컨트랙트에서 공격자 지갑으로 전송되는 사고가 발생하였습니다.

공개된 자료에 따르면 이번 사고는 스마트 컨트랙트 코드 자체의 취약점이 아니라, **브릿지 메시지를 검증하는 단일 검증자 (DVN) 구성**과 **검증자가 참조하는 블록체인 노드 (RPC) 인프라에 대한 공격**이 결합되어 발생한 것으로 분석되고 있습니다. 본 문서는 해당 사고의 사실관계·기술 구조·자금 흐름을 공개자료 기준으로 정리한 정보 알림입니다.

직접 유출	공급량 대비
~294M USD	**~18%**
116.5K rsETH	rsETH 순환공급량 약 630K 기준
2차 피해 예상 금액	**방어 확보액**
~236M USD	**~71M USD**
Aave V3 등 대출 프로토콜	Arbitrum 거버넌스 강제 이관

SECTION 01

사고 이해를 위한 기본 개념

본 절에서는 사고의 맥락을 파악하는 데 필요한 5개 개념을 순서대로 정리합니다.

1.1 LRT (Liquid Restaking Token) 이란?

스테이킹(Staking)은 이더리움 등 블록체인 네트워크에 자산을 예치하고 네트워크 검증 대가로 보상을 받는 구조입니다. **리스테이킹(Restaking)**은 이미 스테이킹된 자산을 재활용하여 추가 네트워크 검증에 활용하고 추가 보상을 얻는 방식으로, EigenLayer 등의 프로토콜이 대표적입니다.

LRT(Liquid Restaking Token)는 사용자가 예치한 ETH가 리스테이킹되어 락업되는 동안, 그 포지션을 대신 나타내는 유동화 토큰을 발행해 다른 DeFi 서비스에서 활용할 수 있게 한 금융상품입니다. 전통 금융으로 비유하면, **정기예금에 맡긴 자금에 대한 증권**을 발행해 그 증권 자체를 담보로 다시 대출을 받거나 매매할 수 있게 한 구조입니다.

1.2 KelpDAO · rsETH는 무엇인가

KelpDAO는 LRT를 발행하는 주요 프로토콜 중 하나이며, 이들이 발행한 토큰이 **rsETH**입니다. 사용자가 KelpDAO에 ETH(또는 ETH 계열 자산)를 예치하면, KelpDAO는 그 자산을 EigenLayer에 리스테이킹하고 사용자에게 rsETH를 발행해 줍니다. 사용자는 rsETH를 Aave · Spark 등 대출 프로토콜에 담보로 예치하거나, 탈중앙화 거래소에서 (DEX) 매매하는 등 자유롭게 활용할 수 있습니다.

1.3 LayerZero OFT — 크로스체인 토큰 구조

rsETH는 Ethereum 메인넷에서 발행되지만, 사용자가 다른 블록체인(L2·사이드체인)에서도 사용할 수 있어야 시장성이 확보됩니다. 이를 위해 사용되는 기술이 **LayerZero OFT(Omnichain Fungible Token)** 구조입니다. 작동 원리는 다음과 같습니다.

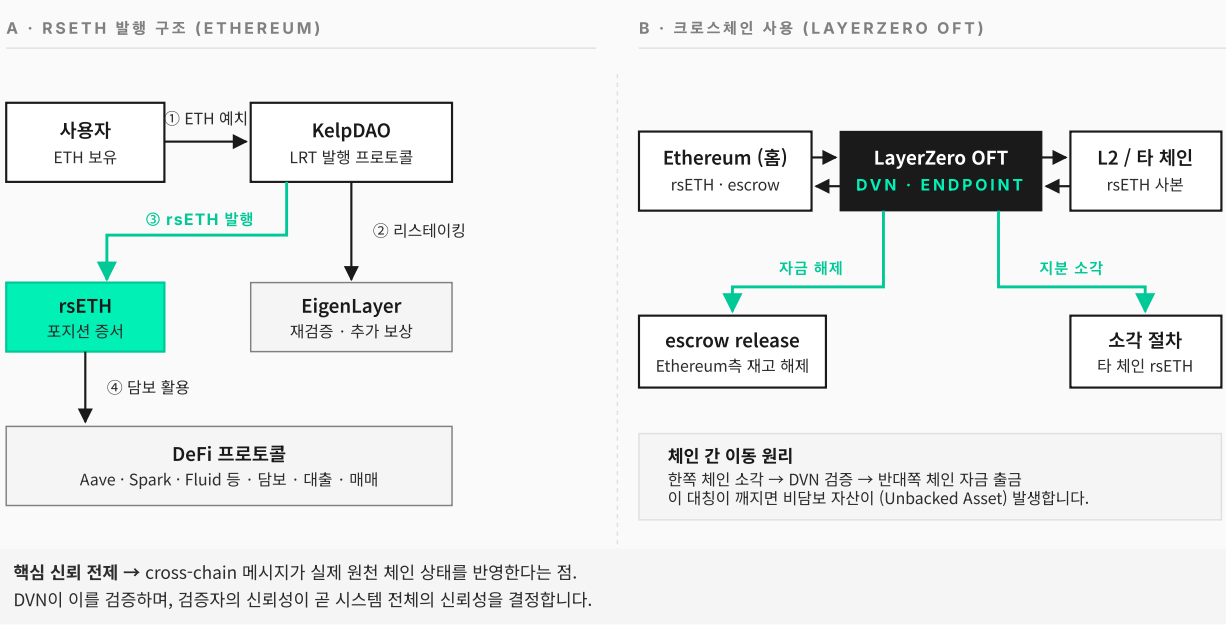
- 사용자가 한 체인(예: Unichain)에서 rsETH에 대한 **소각 절차**를 수행하면, 다른 체인(예: Ethereum)의 보관 컨트랙트에서 동일 수량이 **release(해제)**되어야 합니다.
- 양 체인 사이에 **"소각 절차가 실제로 수행되었다"**는 사실을 전달하는 메시지가 필요하며, 이 메시지는 LayerZero가 중개합니다.
- 메시지의 진위는 **DVN (Decentralized Verifier Network)**이라는 오프체인 검증자 네트워크가 확인합니다.

1.4 DVN — 브릿지의 오프체인 검증자

DVN은 양 체인의 상태를 모두 관찰하고, "A 체인에서 실제로 소각 절차가 수행되었으니 B 체인에서 release해도 된다"는 사실을 서명 형태로 증명하는 오프체인 검증자입니다. 전통 금융의 결제·청산 시스템에서의 **확인 기관**에 비유할 수 있습니다.

DVN은 여러 개를 동시에 요구할 수 있으며, 이를 **정족수 (Quorum)**이라고 합니다. 예를 들어 **2-of-3** 정족수는 3개 DVN 중 2개 이상이 동의해야 메시지가 유효한 구조이고, **1-of-1** 정족수는 단 하나의 DVN 서명만으로 메시지가 유효한 구조입니다.

1.5 시스템 개요 (도식)



도식 1 · rsETH 및 LayerZero OFT 시스템 개요. *사용자가 ETH를 KelpDAO에 예치하면 rsETH가 발행되고, KelpDAO는 원본 ETH를 EigenLayer에서 리스테이킹합니다 (좌). 발행된 rsETH는 LayerZero OFT를 통해 여러 체인에서 사용할 수 있으며, 체인 간 이동은 한쪽 소각 절차 · 다른 쪽 자금 해제 절차를 DVN이 검증하는 방식으로 동작합니다 (우).*

SECTION 02

사고 타임라인

본 사고는 exploit 발생일보다 훨씬 이전부터 동일 리스크 구조에 대한 공개 경고가 외부 보안 연구자 그룹에 의해 제기되어 있었다는 점과, 사고 발생 이후 프로토콜 · 거버넌스 차원의 대응이 복수 주체에 의해 전개되었다는 점이 특징적입니다. 아래 타임라인에서 공격 이벤트는 붉은 마커로, 최초 인지 및 대응 시점은 강조 마커로 구분하였습니다.

2025 · JANUARY — T–15M

외부 보안 감사자 · 연구자 그룹의 공개 경고 사전 경고

Aave 거버넌스 포럼에서 외부 보안 감사자 · 연구자 성격의 개발자 그룹 (Yearn Finance 핵심 기여자 `@banteg` 등)이 KelpDAO의 단일 검증자 DVN LayerZero OFT 구성을 **단일 장애 지점**으로 지적하며 최소 2-of-3 이상의 multi-DVN 구성이 필요하다고 경고. 해당 경고는 KelpDAO · LayerZero 양측이 참여하는 **공개 거버넌스 포럼**에 15개월간 기록된 상태로 존재했으며, 사고 시점까지 DVN 구성은 변경되지 않았습니다.

2026-04-18 17:35 UTC

Exploit 트랜잭션 발생 — 116,500 rsETH release 공격 발생

Ethereum mainnet에서 LayerZero **EndpointV2**의 `lzReceive()`가 호출되어 Kelp rsETH OFTAdapter로 메시지가 발송되었습니다. 이 악성적으로 만들어진 패킷은 실제 수행된 적이 없는 Unichain 소각 증명을 포함하였으나, 단일 DVN이 정상 서명을 제공하여 EndpointV2는 이를 유효 메시지로 처리하게 되어, 116,500 rsETH가 비담보 상태로 해제되어 탈취되게 됩니다.

17:35 – 18:21 UTC · 46 MIN

공격자의 후속 이동 — Aave 등에서 담보 차입 공격 진행

탈취한 rsETH가 Aave V3 등 lending 프로토콜에 담보로 예치되고 WETH 등 유동성 자산이 차입됩니다. 이 구간 동안 약 USD 236M 규모의 잠재 2차 피해가 형성되게 됩니다. 이 46분이 **공격 탐지까지의 공백 구간**에 해당합니다.

2026-04-18 18:21 UTC

KelpDAO 비상 멀티시그 — Pause 및 Blacklist 공격 인지 · 최초 대응

이 시점이 공격 발생을 최초 인지하고 대응이 개시된 분기점입니다. 보안 사고 발생과 약 46분의 간격이 있었고, 그 사이 공격자는 이미 Aave 등에서 담보 차입을 상당 부분 완료한 상태였습니다. KelpDAO 비상 대응 지갑은 핵심 스마트 컨트랙트에 대해 비상정지 함수를 (pause) 호출하고 공격자 주소를 블랙리스트에 등록, 이 조치로 추가 자금 탈취 시도 2건(각 ~40K rsETH)이 거부되어 잠재 피해가 추가로 억제되었습니다.

2026-04-18 18:52 UTC

Aave Guardian, rsETH / wrsETH 마켓 동결 시장 대응

Aave는 여러 배포망에서 rsETH 및 wrsETH 마켓을 동결. 다만 동결 시점은 보안 사고 발생 후 약 1시간 17분이 경과한 시점이며, 공격자는 그 이전에 차입 이동을 상당 부분 완료한 상태였습니다.

2026-04-19 / 20

LayerZero Incident Statement 공개 공식 성명

LayerZero는 공식 블로그를 통해 ① 단일 DVN 구성은 KelpDAO의 선택이었으며, ② 공격은 DVN이 참조하던 RPC 인프라의 오염으로 발생, ③ LayerZero 프로토콜 자체의 취약점은 아니라는 입장을 공개하였습니다.. 동시에 1-of-1 DVN 앱 대상 추가 서명 중단 및 multi-DVN으로 수정 정책을 공지하였습니다.

2026-04-21 ~

Arbitrum Security Council의 비상 동결 조치 거버넌스 개입

Arbitrum Security Council이 비상 시스템 트랜잭션으로 공격자 지갑 관련 약 **30,766 ETH(≈ USD 71M)**를 거버넌스 통제 주소로 강제 이관하였습니다.

2026-04-21 ~ PRESENT

자금세탁 및 추적 진행 추적 진행

남은 ETH 상당 부분이 THORChain(ETH→BTC swap), Umbra mixer, BitTorrent 등으로 자금 세탁이 진행중입니다.

SECTION 03

기술적 분석 — 어떻게 공격이 이루어졌는가

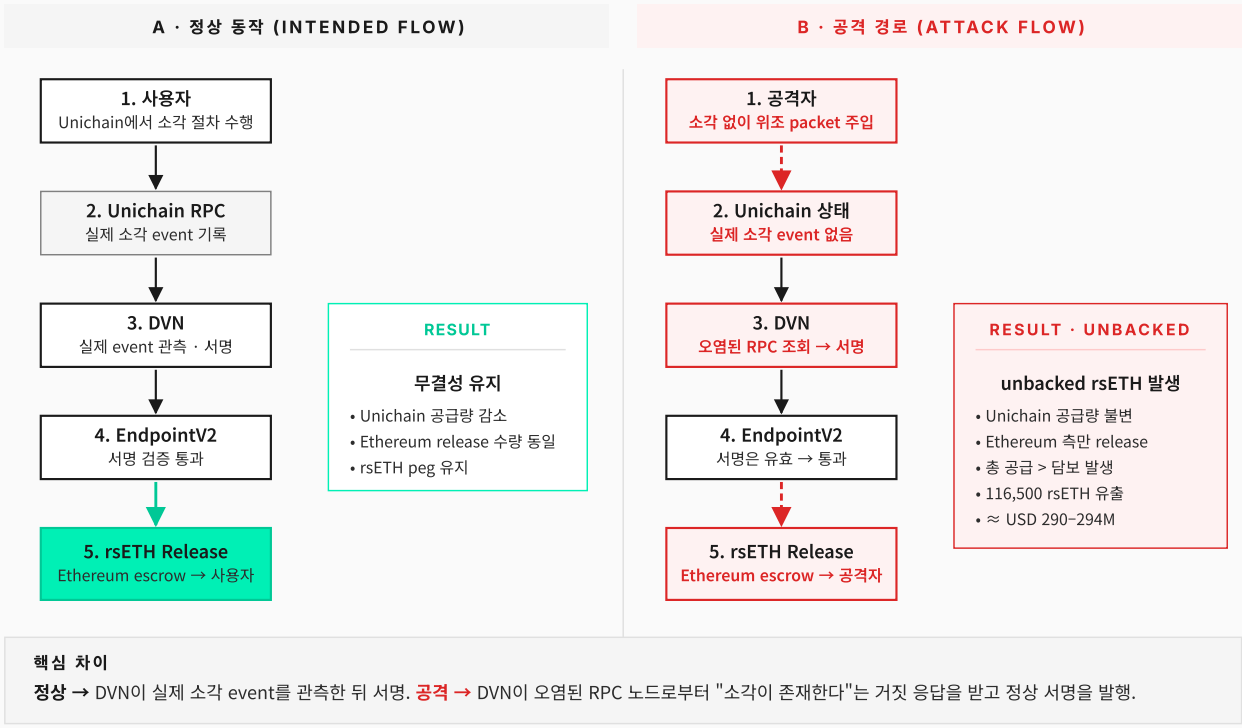
본 사고를 이해하려면 ① **정상적인 OFT 브릿지가 어떻게 동작하는가**, ② **이번 공격이 정상 흐름의 어느 지점을 어떻게 우회했는가**를 대비해서 보는 것이 가장 명확합니다. 아래 두 개 소절은 동일 시스템의 정상 흐름과 공격 흐름을 나란히 추적합니다.

> **핵심 전제 · 스마트 컨트랙트 취약점은 없음**
>
> 본 사고에 관련된 스마트 컨트랙트 — LayerZero **EndpointV2**, Kelp rsETH **OFTAdapter**, KelpDAO core contracts — 의 코드 자체에는 취약점이 확인되지 않았습니다. 공격은 이들 컨트랙트가 **신뢰 전제로 삼는 오프체인 구성 요소**(DVN 및 그 기반 RPC 인프라)에 대해 이루어졌으며, 스마트 컨트랙트 관점에서는 모든 검증 단계가 설계대로 통과되었습니다. 따라서 이번 사고의 기술적 분석은 **코드 감사 영역 밖**의 구성·인프라 영역에 집중됩니다.

3.1 정상 동작 흐름과 공격 흐름의 차이

정상 동작 흐름. 사용자가 Unichain에서 보유한 rsETH에 대한 **소각 절차**를 수행하면, Unichain 체인 상태에 해당 이벤트가 기록됩니다. LayerZero DVN은 블록체인 노드(RPC)를 통해 이 이벤트를 관측한 뒤, "이 소각 절차가 실제로 수행되었다"는 사실을 자신의 키로 서명하여 증명합니다. Ethereum 측의 EndpointV2 컨트랙트는 이 서명을 검증하고 유효하다고 판단되면, Kelp rsETH OFTAdapter에 메시지를 전달해 예탁 컨트랙트에 보관되어 있던 rsETH를 동일 수량만큼 전달합니다. 전체 신뢰 체인의 핵심은 **DVN이 관측한 사실이 실제 체인 상태와 일치한다**는 전제입니다.

공격 흐름의 분기점. 이번 사고에서 공격자는 Unichain에서 실제로 소각 절차를 수행하지 않은 상태로, 위조된 정보를 패킷을 통해 LayerZero 메시지 경로에 주입했습니다. 공격자가 노린 표적은 EndpointV2나 OFTAdapter 같은 스마트 컨트랙트 단이 아니라 **DVN의 관측 과정 자체**였습니다 — DVN이 Unichain 체인 상태를 조회할 때 사용하는 RPC 노드 일부가 오염되어, 실제로는 존재하지 않는 소각 이벤트가 마치 존재하는 것처럼 DVN에 보고되도록 조작되어 있었기 때문입니다. DVN은 이 응답을 신뢰하여 위조 정보에 대해 **정상 서명**을 발행했고, EndpointV2는 해당 서명을 암호학적으로 검증한 뒤 메시지를 통과 처리했습니다. 결과적으로 스마트 컨트랙트 로직 관점에서는 **모든 검증 단계가 정상적으로 통과**되었기 때문에, 코드 감사만으로는 이 공격을 사전에 구별할 수 없는 구조였습니다.

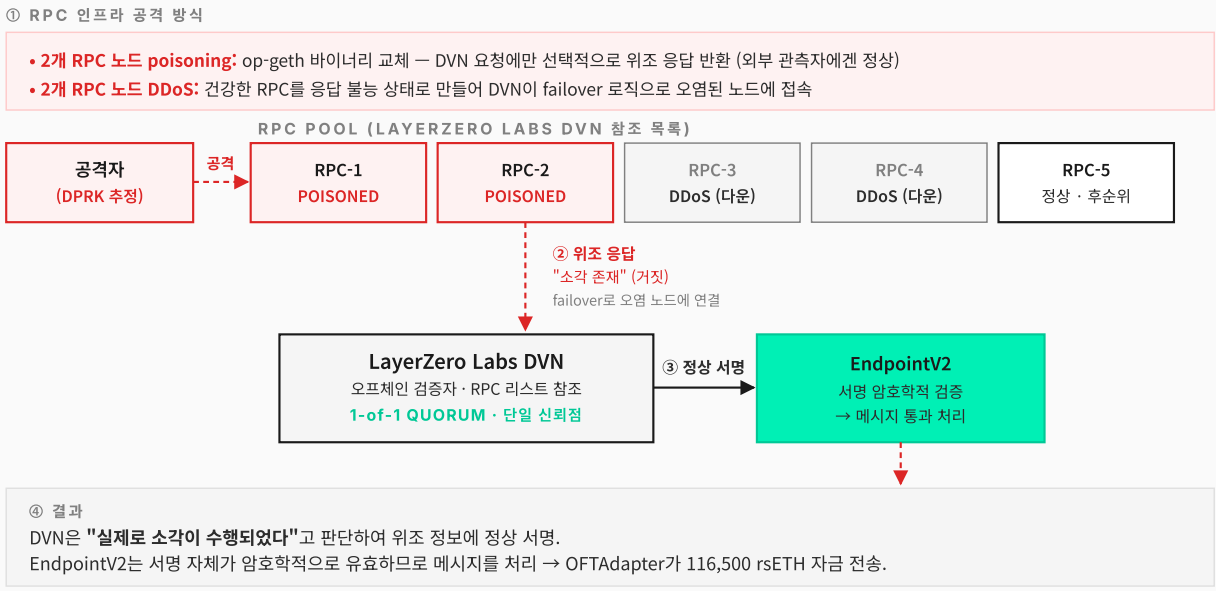


도식 2 · 정상 OFT 동작과 공격 경로 비교. *스마트 컨트랙트(EndpointV2 · OFTAdapter)는 설계대로 동작하였으나, 오프체인 검증자(DVN)가 잘못된 세계 상태를 신뢰하고 정상 서명을 발행함으로써 Ethereum 측에서 실제 원천 체인 소각 절차 없이 rsETH가 release되는 결과가 발생한 점이 핵심입니다.*

3.2 DVN이 속은 과정 — Poisoned RPC + DDoS Failover

DVN의 작동 원리. DVN은 오프체인에서 실행되는 검증 노드로, 각 체인의 상태를 확인하기 위해 여러 개의 블록체인 노드(RPC) 엔드포인트 리스트를 참조합니다. 단일 RPC에 장애가 나도 검증 서비스가 중단되지 않도록 **장애 전환** 로직이 내장되어 있어, 최상위 RPC가 응답하지 않으면 자동으로 차순위 RPC로 쿼리를 넘깁니다. 이 구조는 운영 안정성을 위한 상식적 설계이지만, 이번 공격에서는 오히려 공격 벡터로 활용되었습니다.

공격 구성. 공격자는 LayerZero Labs DVN이 참조하는 RPC 리스트를 파악한 뒤 다음 두 가지를 병행했습니다. 첫째, RPC 풀 중 일부 노드의 `op-geth` 바이너리를 교체하여 **DVN 쿼리에만 선택적으로 위조 응답을 반환**하도록 심어두었습니다 — 다른 관측자(일반 사용자 · 외부 모니터링)에게는 정상 응답을 반환했기 때문에 외부에서는 노드 상태만으로 이상을 감지할 수 없었습니다. 둘째, 건강한 상태의 우선순위 RPC들에 DDoS 공격을 가해 응답 불능 상태로 만들었습니다. 그 결과 DVN은 장애 전환 로직에 따라 자연스럽게 오염된 RPC로 쿼리를 넘겼고, "실제로는 존재하지 않는 소각 이벤트가 존재한다"는 응답을 수신하게 되었습니다.



도식 3 · DVN RPC Poisoning + DDoS Failover의 세부 공격 경로. *오염된 노드는 DVN 쿼리에만 선택적으로 위조 응답을 반환했기 때문에, 외부 관측자에게는 정상 상태로 보였습니다. 이 구성에서는 DVN 1개가 단일 신뢰점(single point of failure)으로 작동합니다.*

왜 사전 탐지가 어려웠는가. 세 가지 요소가 결합되어 탐지 난이도가 높았습니다.

① 오염된 노드가 외부 관측자에게는 정상 응답을 반환했으므로, 제3자가 노드 상태만을 관측해서는 오염을 판별할 수 없었습니다.

② LayerZero Labs DVN이 1-of-1 정족수의 유일한 검증자였으므로, 동일 메시지에 대해 교차 검증할 다른 DVN이 존재하지 않았습니다.

③ EndpointV2 관점에서 DVN 서명은 암호학적으로 유효했으므로, 온체인 로직 레벨에서는 정상 메시지와 구별할 방법이 없었습니다.

이 세 요소가 동시에 작동하면서, 코드 · 스마트 컨트랙트 중심의 기존 감사 프레임만으로는 사전 방어선이 확보되지 않는 구조였습니다.

3.3 OApp Configuration — 1-of-1 DVN 설정

위 공격 경로가 실제로 성공하려면 **공격자가 단 하나의 DVN만 속이면 된다**는 전제가 필요합니다. 여러 공개 분석에 따르면, KelpDAO rsETH OApp의 양측(sender/receiver) DVN 설정은 아래와 같이 구성되어 있었다고 보고되고 있습니다. 이 구성에서는 단일 DVN의 서명 하나만으로 cross-chain 메시지가 유효하다고 간주되며, 서로 독립된 DVN이 다수 구성되어 있었다면 공격자가 **동시에 여러 DVN · RPC 스택**을 오염시켜야 했을 것입니다.

OAPP DVN 설정 (공개 분석 기준, 요약)

```
# KelpDAO rsETH OFT · sender & receiver DVN config
requiredDVNs      : [ 0x282b3386571f7f794450d5789911a9804fa346b4 ]  # LayerZero Labs DVN
requiredDVNCount  : 1
optionalDVNs      : [ ]
optionalDVNCount  : 0
threshold         : 1-of-1

# 참고 권고 구성 (업계에서 논의되는 수준)
requiredDVNs      : [ DVN_A, DVN_B, DVN_C ]          # 3개 독립 운영자
threshold         : 2-of-3                             # 최소 정족수
```

SECTION 04

영향 평가

4.1 직접 피해 — unbacked rsETH

직접 유출 규모

116,500 rsETH

≈ USD 290–294M · 2026년 최대 DeFi exploit

> Unichain 측에서 실제 소각 절차가 수행되지 않았음에도, Ethereum escrow에서 동일 수량의 rsETH가 전송되어 **담보 없이 발행된 상태**로 유통되었습니다. 이는 rsETH의 **총 공급량이 실제 담보를 초과**하는 상태를 의미합니다.

위와 같이 총 공급이 담보를 초과하는 상태는 rsETH의 상환가능성·담보가치·시장가격에 즉각적인 연동 가치에 대한 충격을 주었고, rsETH를 담보로 활용하던 프로토콜들에서 담보 가치 불확실성이 급증했습니다.

4.2 2차 피해 — Lending 프로토콜의 부실채권

금융시장 전파 관점에서 특징적인 점은, **공격자가 탈취 자산을 즉시 매도하지 않고 담보로 예치**했다는 점입니다. 대규모 매도는 슬리피지로 회수액이 제한되지만, 담보 예치는 oracle 업데이트 지연과 청산 프로세스의 시간차를 이용해 단기간에 유동성 자산 (WETH 등)을 차입할 수 있게 합니다. 이로 인해 부실채권이 대출 프로토콜 시장으로 전이되었습니다.

프로토콜	2차 피해 예상 규모	출처 요약
Aave V3 (Ethereum · Arbitrum 등)	USD 124M ~ 230–236M	Aave Governance, Galaxy Research, CredShields, KuCoin Research 등
SparkLend · Fluid · Upshift 등	수천만 USD 수준	각 프로젝트 공지 및 언론 요약

4.3 시장 · 시스템 영향

DEFI TVL

48시간 내 대폭 감소

사건 직후 DeFi 전체 TVL이 약 USD 10–13B 수준 감소한 것으로 추정됩니다. 2026년 최대 DeFi 보안사고로 기록되었습니다.

토큰 가격

LayerZero 토큰 · 파생 조정

ZRO 등 관련 토큰은 단기 20% 이상 하락하였고, EigenLayer 파생 자산들도 동반 조정 움직임이 관찰되었습니다.

CROSS-CHAIN 신뢰

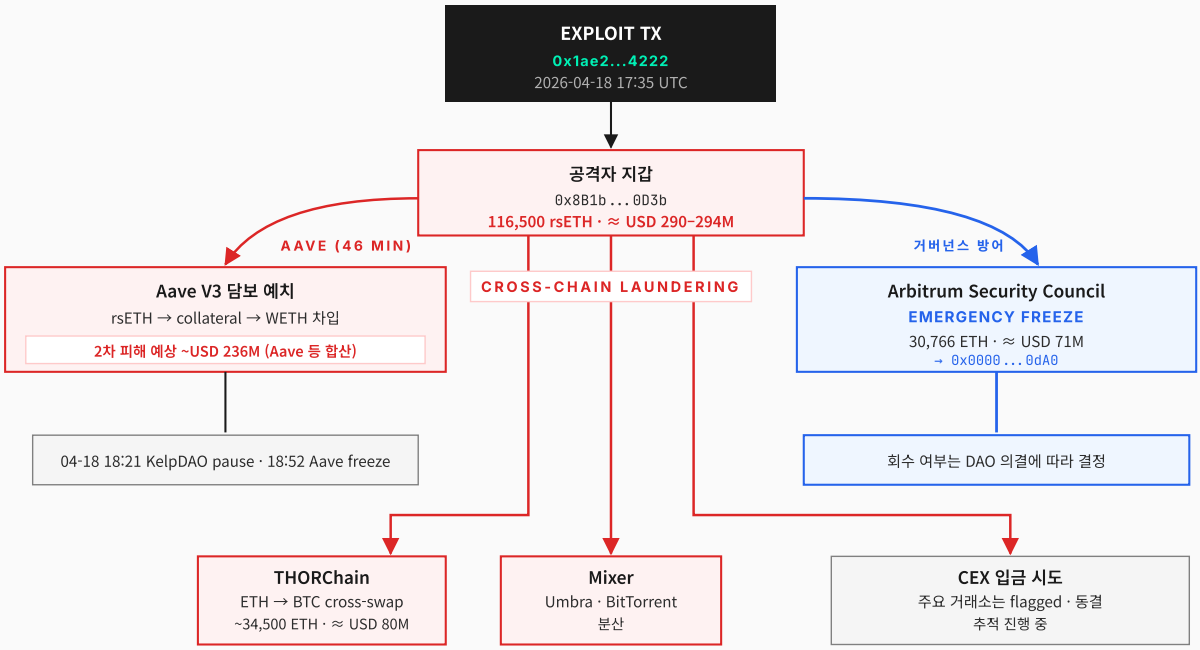
업계 전반 DVN 구성 재점검

다수 프로토콜이 multi-DVN migration 완료 전까지 신규 예치를 일시 제한하는 등 보수적 대응이 이어지고 있습니다.

SECTION 05

자금 흐름 · 유출 경로

Chainalysis · Arkham · ZachXBT 등 온체인 추적 결과를 종합할 때, 유출된 자산은 크게 세 갈래로 분산되었습니다. 이 중 일부는 Arbitrum Security Council의 emergency 트랜잭션으로 거버넌스 통제 주소에 동결된 상태이며, 나머지 상당량은 여러 믹싱·크로스체인 교환 경로를 거쳐 추적이 진행 중입니다.



도식 4 · 유출 자산의 분기 · 자금세탁 경로. *자산은 크게 세 갈래(Aave 담보 차입 · Arbitrum 거버넌스 방어 확보 · Cross-chain 자금 세탁)로 분산되었습니다. 이 중 Arbitrum 동결분은 거버넌스 개입으로 공격자 통제에서 이탈한* **방어 확보** *경로이고, 나머지 자금 세탁 경로는 회수 난이도가 매우 높은 영역으로 구분됩니다.*

참고 · 국가급 행위자 가능성

LayerZero와 일부 리서치는 본 사고 배후로 **DPRK 연계 Lazarus Group / TraderTraitor**의 가능성을 지목하고 있습니다. 다만 이는 현재 공개된 분석 기반의 추정으로, 법집행기관의 공식 귀속과는 구분해 이해해야 합니다. 해당 판단이 확정될 경우, 연관 주소 · 자금 경로는 OFAC SDN, FATF 권고 맥락에서 제재 · AML 리스크가 부각될 수 있습니다.

SECTION 06

책임 귀속 관련 양측 입장

본 사고의 책임 분담에 대해서는 현재까지 LayerZero와 KelpDAO가 서로 다른 강조점을 제시하고 있습니다. 공개된 계약 조건이 없고 법적 절차가 진행 중이지 않은 시점에서, 본 문서는 **어느 한쪽의 책임으로 단정하지 않고** 양측 입장과 업계에서 관찰되는 합의 영역을 병기합니다.

6.1 공개 자료에서 합의되는 영역

- 스마트 컨트랙트(EndpointV2, OFTAdapter, rsETH core)의 코드 취약점은 확인되지 않았습니다.
- 사고의 구조적 기반은 **취약한 DVN 구성**과 **DVN이 의존한 RPC 인프라 탈취**의 결합입니다.
- 다중 DVN (2-of-3 이상) 구성이었다면 동일 공격의 난이도가 크게 상승했을 것으로 평가됩니다.
- 사고 영향은 브릿지 레이어에 국한되었고, KelpDAO 핵심 리스테이킹 컨트랙트는 직접 손상되지 않았습니다.
- 해당 구성 리스크는 사고 15개월 전 외부 보안 감사자 · 연구자 그룹에 의해 공개 포럼에서 지적된 상태로 존재했으며, 양측 모두 이를 접할 수 있는 위치에 있었습니다.

6.2 양측 입장 요약

LAYERZERO 측

"1-of-1 DVN은 KelpDAO의 선택"

- 파트너들에게 다중 DVN 구성을 권고해 왔음
- 1-of-1 DVN은 고가치 자산에 적절한 구성이 아님
- 본 사건은 프로토콜에 내재된 보안 위협이 아니라 DVN이 참조한 RPC 인프라가 국가급 공격을 받은 케이스
- 후속 조치로 1-of-1 앱 대상 추가 서명 중단 · 다중 DVN migration 강제

KELPDAO 측

"LayerZero에서 제공한 기본 설정을 그대로 사용"

- LayerZero 공식 문서·빠른 시작 예제의 기본 구성(1-of-1)을 사용
- 이를 "권고를 무시한 설정 오류"으로 보기 어려움
- 사용된 DVN은 LayerZero Labs가 직접 운영한 검증자 체계 — 공격자는 사실상 LayerZero 인프라를 탈취
- 공개된 기본 설정이 단일-검증자 구성이라는 점 자체가 LayerZero가 고가치 멀티체인 프로토콜로써 부적절했다는 지적

> 관찰
>
> 기술적으로는 ① 단일 정적수 허용 (구성), ② RPC 인프라 보안 (오프체인), ③ 사후 시장 통제의 지연 (대출 프로토콜 정지 타이밍)이 동시에 작용한 사례로 해석되는 경우가 많으며, 어느 한 주체만의 실패로 환원하기 어렵다는 견해가 업계에서 다수 관찰됩니다.

SECTION 07

업계에서 논의되는 대응 방향

본 절은 특정 기관에 대한 권고가 아닌, 사고 이후 LayerZero · Aave 거버넌스 · 주요 리서치 기관 등에서 공개적으로 논의되고 있는 대응 방향을 정리한 것입니다.

7.1 기술 · 구성 관점

- Cross-chain messaging infra 사용 시 **다중 검증자 (2-of-3 이상)** 구성이 산업 표준으로 확산되는 흐름
- 검증자 운영 주체의 다각화 (독립 법인 · 독립 키 관리 · 독립 RPC provider) 요구 강화
- OApp configuration을 체인 상에서 직접 decode · 검증하는 **설정 감사**의 필요성

7.2 자산 · 담보 관점

- LRT · LST · OFT 기반 자산에 대한 **2차 전이** 리스크의 별도 평가
- Bridge layer에서 비담보 자산 발생 시나리오의 스트레스 테스트 편입
- 오라클 정보 시차 · 청산 지연 · 연계 프로토콜 정지로 인한 지연을 합산한 복합 노출 시뮬레이션

7.3 법률 · AML · 거버넌스 관점

- 국가급 공격 가능성이 제기된 사고의 경우, 일반 해킹과 분리해 제재 · AML 리스크를 별도 카테고리로 관리하는 논의
- L2 Security Council의 긴급 정지 메커니즘이 주는 **거버넌스 개입 가능성**의 양면성(방어 확보 ↔ 검열저항성)
- Cross-chain 인프라 계약에서 DVN · RPC provider 책임 범위 · SLA · 사고 disclosure timeline의 명시화 논의

SECTION 08

참고 자료

접근 일자는 모두 2026-04-24 기준이며, 원문 URL의 변경 가능성이 있어 가급적 원 출처에서 재확인을 권합니다.

공식 성명 · 거버넌스 포럼

[1] LayerZero. (2026, April 19). *KelpDAO incident statement*. LayerZero Blog. https://layerzero.network/blog/kelpdao-incident-statement

[2] Aave Governance Forum. (2026, April 18). *rsETH incident — 2026-04-18*. https://governance.aave.com/t/rseth-incident-2026-04-18/24481

[3] Aave Governance Forum. (2026, April 20). *rsETH incident report — April 20, 2026*. https://governance.aave.com/t/rseth-incident-report-april-20-2026/24580

[4] KelpDAO. (n.d.). *Audits*. KelpDAO GitBook. https://kelp.gitbook.io/kelp/audits

[5] Code4rena. (2023, November). *Kelp DAO: rsETH audit contest*. https://code4rena.com/audits/2023-11-kelp-dao-rseth

온체인 정보

공개 분석에서 반복적으로 인용되는 사고 관련 온체인 식별자와, 호출된 함수 인터페이스를 함께 정리합니다. 각 주소 · 해시는 Etherscan에서 직접 조회 가능합니다.

대상	식별자
Exploit TX	`0x1ae232da212c45f35c1525f851e4c41d529bf18af862d9ce9fd40bf709db4222`
호출 함수	`lzReceive(Origin, address, bytes, bytes)`
Forged packet	`srcEid = 30320 (Unichain)`, `nonce = 308`
LayerZero EndpointV2 (Ethereum)	`0x1a44076050125825900e736c501f859c50fE728c`
Kelp rsETH OFTAdapter / Escrow	`0x85d456B2DfF1fd8245387C0BfB64Dfb700e98Ef3`
공격자 지갑	`0x8B1b6c9A6DB1304000412dd21Ae6A70a82d60D3b`
Arbitrum 거버넌스 동결 주소	`0x0000000000000000000000000000000000000dA0`

LAYERZERO ENDPOINTV2 · LZRECEIVE 인터페이스 (단순화)

```
// EndpointV2.sol — LayerZero 공식 인터페이스
function lzReceive(
    Origin  calldata _origin,    // srcEid, sender, nonce
    address _receiver,            // 수신 OApp (= rsETH OFTAdapter)
    bytes   calldata _payload,    // Unichain 소각 증명 (위조됨)
    bytes   calldata _extraData
) external payable;

// forged packet 파라미터 (공개 분석 기준)
_origin = {
    srcEid:   30320,        // Unichain
    sender:   0x...,
    nonce:    308
}
```

Etherscan 링크

[1] Etherscan. (2026, April 18). *Transaction 0x1ae232da212c45f35c1525f851e4c41d529bf18af862d9ce9fd40bf709db4222*. https://etherscan.io/tx/0x1ae232da212c45f35c1525f851e4c41d529bf18af862d9ce9fd40bf709db4222

[2] Etherscan. (n.d.). *LayerZero EndpointV2 contract 0x1a44076050125825900e736c501f859c50fE728c*. https://etherscan.io/address/0x1a44076050125825900e736c501f859c50fE728c

[3] Etherscan. (n.d.). *Kelp rsETH OFTAdapter 0x85d456B2DfF1fd8245387C0BfB64Dfb700e98Ef3*. https://etherscan.io/address/0x85d456B2DfF1fd8245387C0BfB64Dfb700e98Ef3

[4] Etherscan. (n.d.). *Attacker wallet 0x8B1b6c9A6DB1304000412dd21Ae6A70a82d60D3b*. https://etherscan.io/address/0x8B1b6c9A6DB1304000412dd21Ae6A70a82d60D3b

[5] Etherscan. (n.d.). *Arbitrum governance-frozen address 0x0000000000000000000000000000000000000dA0*. https://etherscan.io/address/0x0000000000000000000000000000000000000da0

전문 리서치 · 분석

[1] Chainalysis. (2026, April). *KelpDAO bridge exploit — April 2026 on-chain analysis*. https://www.chainalysis.com/blog/kelpdao-bridge-exploit-april-2026/

[2] Galaxy Research. (2026, April). *KelpDAO × LayerZero exploit: DeFi implications*. Galaxy Digital. https://www.galaxy.com/insights/research/kelpdao-layerzero-exploit-defi

[3] CredShields. (2026, April 20). *Incident report: Kelp DAO rsETH bridge exploit*. https://discover.credshields.com/incident-report-kelp-dao-rseth-bridge-exploit/

[4] LlamaRisk. (2024, July). *Collateral risk assessment: rsETH*. https://www.llamarisk.com/research/collateral-risk-rseth

[5] DefiPrime. (2026, April). *The KelpDAO rsETH exploit: $292M minted from a 1-of-1 bridge*. https://defiprime.com/kelpdao-rseth-exploit

언론 보도

[1] CoinDesk. (2026, April 19). *2026's biggest crypto exploit: $292 million drained from Kelp DAO*. https://www.coindesk.com/tech/2026/04/19/2026-s-biggest-crypto-exploit-kelp-dao-hit-for-usd292-million

[2] Crypto Briefing. (2026, April). *LayerZero says North Korean Lazarus Group behind $292M Kelp DAO attack*. https://cryptobriefing.com/kelpdao-exploit-layers-of-compromise/

[3] Crypto Briefing. (2026, April). *KelpDAO exploit creates $236M bad debt risk for Aave*. https://cryptobriefing.com/kelpdao-exploit-creates-236m-bad-debt-risk-for-aave-ethereum-drops-3/

[4] Cybernews. (2026, April). *$300M stolen in cross-chain bridge hack, largest DeFi exploit of 2026*. https://cybernews.com/crypto/300m-stolen-in-cross-chain-bridge-hack-largest-defi-exploit-of-2026/

[5] Infosecurity Magazine. (2026, April). *North Korean actors blamed for $290M KelpDAO exploit*. https://www.infosecurity-magazine.com/news/north-korean-blamed-290m-kelpdao/

[6] Cryptopotato. (2026, April). *The biggest hack of 2026: What we know about the $294M KelpDAO exploit*. https://cryptopotato.com/the-biggest-hack-of-2026-what-we-know-about-the-294m-kelpdao-exploit/

[7] StreetBrief. (2026, April 26). *Arbitrum Security Council freezes $71 million linked to Kelp DAO exploit*. https://www.streetbrief.co/article/arbitrum-security-council-freezes-71-million-linked-kelp-dao-exploit-2604/

[8] AInvest. (2026, April 26). *KelpDAO exploit: $80M laundered via THORChain as volume surges to $394M*. https://www.ainvest.com/news/kelp-dao-exploit-80m-laundered-thorchain-394m-volume-surge-2604/

한국어 설명 자료

[1] Xangle. (2026, April). *KelpDAO rsETH LayerZero 브릿지 사고 정리*. https://xangle.io/en/insight/events/69e6ba27afe6454f3d390987

[2] BloomingBit. (2026, April). *KelpDAO 해킹 이후 자금 추적 · THORChain 이상 거래*. https://en.bloomingbit.io/feed/news/110477

[3] PANews. (2026, April). *KelpDAO 보안 구성 분석*. https://www.panewslab.com/en/articles/019da9ba-cfc3-75a8-b5a1-f8475f5a37f3

> **면책**
>
> 본 문서는 공개 자료를 종합한 정보 제공용 알림이며, 투자 · 법률 · 세무 자문을 대신하지 않습니다. 수치 · 귀속 · 책임 분담은 추가 공식 조사 결과에 따라 변경될 수 있으며, 내부 의사결정 시에는 자체 실사 및 법률 검토를 병행하시기 바랍니다.

SOOHO.IO

SECURITY RESEARCH · INCIDENT BULLETIN

Security Research — Incident Bulletin

SOOHO.IO 보안연구팀은 블록체인 · DeFi 인프라에서 발생하는 주요 보안 사건에 대해 정기적으로 공개 자료 기반 알림을 제공합니다. 본 문서는 그 정례 시리즈의 일부입니다.
