Market Insight | 2026.4.22

그림: Midjourney(AI로 인한 암호화폐 해킹 임계점)

디지털자산 핫 이슈

탈중앙화 가치의 소멸과 인프라로서의 이더리움 부상

한종목

chongmok.han@miraeasset.com

CONTENTS

Executive Summary

이제는 탈중앙화의 기치보다는 인프라의 가치가 부각된다

2026년 4월, 디지털자산 시장에서 거대한 사건이 터졌습니다. 디지털 세상의 '은행'들이 줄줄이 무너지고 있는 중입니다. 이 보고서는 그 사건의 전말과 의미, 그리고 앞으로의 전망을 정리한 문서입니다.

무슨 일이 벌어졌는가? 북한으로 추정되는 해커들이 한 가상화폐 프로젝트(KelpDAO)의 허술한 보안 설정을 뚫고 약 3,800억 원어치의 가짜 코인을 찍어냈습니다. 공격자는 이 가짜 코인을 담보로 맡기고, 또 다른 대형 디지털자산 대출은행(Aave)에서 약 3,000억 원의 실제 자산을 빌려 도망쳤습니다. 이 소식에 놀란 예금자들이 한꺼번에 돈을 빼내려 하자, 사건 발생 48시간 만에 이 은행에서만 7조 원 넘는 자금이 빠져나갔고 결국 "예금 인출 불가" 상태에 빠졌습니다. 일종의 디지털 뱅크런입니다. 더 충격적인 장면은 따로 있었습니다. 또 다른 거대 디지털자산 네트워크인 아비트럼(Arbitrum)이 해커의 지갑을 강제로 얼리고 약 900억 원어치의 자금을 직접 되찾아온 것입니다. 그동안 디지털자산 업계가 "우리는 어떤 정부나 회사도 손댈 수 없는 완전히 자유로운 세상"이라고 자랑해왔던 것과는 정반대의 일이 벌어진 셈입니다.

이번 사태의 핵심 에센스! 10년간 업계가 팔아온 "완벽한 분산화(탈중앙화)" 신화는 이번 사건으로 공식적으로 사망했습니다. 알고 보니 위기가 닥치면 결국 몇 명의 운영진이 회의를 열고 투표를 거쳐 해커의 돈을 빼앗아오는, 우리가 쓰는 시중 은행과 논리적으로 단 1%도 다르지 않은 구조였다는 사실이 드러났기 때문입니다. 그리고 이번 붕괴는 2008년 월가가 주택담보대출을 복잡한 파생상품으로 포장해 팔다가 금융위기를 일으켰던 그 역사가, 이번엔 블록체인 위에서 그대로 재현된 사건이기도 합니다. 여기에 AI를 이용한 해킹 자동화까지 임계점을 넘으면서, 기존의 방어 체계가 근본적으로 무력화되고 있다는 점 역시 사태의 중요한 본질입니다.

앞으로 어떻게 될 것인가? 역설적이지만, 이번 충격은 월스트리트의 대형 금융기관들에게는 반가운 일입니다. 블랙록이나 JP모건 같은 기관들이 디지털자산에 수십조 원을 투자하지 못했던 가장 큰 이유는 "해킹당하면 끝이다"라는 공포 때문이었는데, 아비트럼 사태로 "위기 때는 운영진이 개입해 자산을 되찾아올 수 있다"는 사실이 실증되었기 때문입니다. 이제 디지털자산 시장은 두 갈래 길로 갈라질 것으로 판단합니다. 한쪽은 대형 금융기관이 규제를 지키며 운영하는 '관리되는 L2'이고, 다른 한쪽은 사람의 탐욕이 개입할 여지조차 없도록 AI 에이전트만 참여하는 '에이전트 전용 L2'입니다. 그리고 이 모든 길이 최종적으로 모이는 '정산 장부' 역할은 이더리움(Ethereum)이 상당히 점유할 것으로 판단됩니다. 이번 사태에서 작은 디지털 은행들이 결국 인간 운영진의 개입을 허용한 반면, 이더리움은 전 세계 수백만 명이 함께 운영하고 있어 어떤 정부나 기업도 혼자서는 건드릴 수 없는, 유일한 '중립 지대'로 남게 됩니다.

즉, 탈중앙화라는 종교는 죽었지만, 모든 디지털 자산의 최종 정산소가 될 이더리움 인프라 제국은 2막이 열렸다고 생각합니다.

I. 디지털자산 해킹 사태와 이더리움

1. 사건의 해부: 코드가 아닌 '설정'이 무너진 3억 달러 참사

이번 해킹은 블록체인 프로그램(스마트 컨트랙트) 자체에 버그가 있어서 터진 게 아니었다. 사이버 해킹의 공격 경로를 볼 때, 인프라를 운영하는 방식(운영 보안, OpSec)에서 실수가 나와서 터진 사건이다. 이 차이를 분명히 알아야 이번 사태의 진짜 의미가 보인다.

KelpDAO는 사람들이 ETH(이더리움)를 여러 번 맡겨서 더 많은 이자를 받을 수 있게 해주는 프로젝트다. rsETH(Liquid Restaking Token)의 크로스체인 이동을 위해, LayerZero라는 탈중앙화 검증 네트워크(Decentralized Verifier Network, DVN)를 도입했다. 다시 말해, KelpDAO는 rsETH(유동성 재스테이킹 토큰)이라는 자신들의 토큰을 다른 블록체인으로 옮길 때, LayerZero라는 기술을 사용했다는 말이다.

* KelpDAO: ETH를 스테이킹해서 이자를 받고, 다시 그 영수증을 EigenLayer에 맡겨 추가 이자를 받는 '유동성 재스테이킹' 프로젝트. rsETH라는 토큰을 발행해줌.
LayerZero DVN (Decentralized Verifier Network): 서로 다른 블록체인 사이에 "이 메시지가 진짜야"라고 확인해주는 검증 네트워크. KelpDAO는 이걸 1-of-1(단 하나의 노드만)으로 설정.

문제는 KelpDAO가 $10억 규모의 자산을 다루면서도 DVN을 '1-of-1' 구성으로 설정했다는 점이다. 쉽게 말하면 "열쇠를 한 사람한테만 맡기는" 상황이었다. 즉, 메시지의 진위를 확인하는 검증 노드가 단 하나만 존재했고, 그 한 사람(검증 노드)만 해킹당하면 네트워크 전체의 크로스체인 메시지를 위조할 수 있는 구조였다. LayerZero는 멀티-DVN(2개 이상의 검증 노드) 구성을 KelpDAO에게 여러 번 권고했으나 KelpDAO는 이를 수용하지 않았다.

공격자는 정확히 이 단일 검증 노드를 공략했다. LayerZero가 직접 운영하는 컴퓨터(RPC 노드) 2개를 해킹하고, 나머지는 디도스 공격으로 마비시킨 뒤 악성 노드로 바꿔버렸다. 그리고 rsETH가 겨우 47개밖에 없는 아주 작은 L2 네트워크에서 이 유일한 노드를 뚫어 가짜 메시지를 만들었다. 이 가짜 메시지가 이더리움 메인넷(본체)에 도착하는 순간, 진짜 참사가 시작됐다.

* Burn-and-Mint: 기존 토큰을 태우고 새로 발행.

공격자의 위조 메시지는 "메인넷에 실제 돈이 잠겨 있다"고 거짓말을 했고, 메인넷 금고는 담보 없이 rsETH를 풀어줬다. 결과적으로 116,500개의 rsETH(약 2억 9,200만~2억 9,400만 달러)가 실제로는 존재하지 않는데도 새로 만들어졌다. 전체 rsETH 공급량의 17~18%가 가짜로 늘어나 17.5% 담보 부족(Undercollateralization) 상태가 된 것이다.

* Lock-and-Mint: 메인넷에 진짜 토큰을 잠그고, 다른 체인에서 복사본을 만듦. Kelp 사건은 Lock-and-Mint 방식의 허점을 노린 것.

다시 말하지만, 중요한 점은 코드 자체는 전혀 버그가 없었다는 것이다. Slither나 Mythril 같은 최고 수준의 코드 감사 도구로도 절대 잡히지 않았다. 코드는 "1개만 승인하면 된다"는 조건을 정상적으로 충족했을 뿐이다. 결국 $10억 자산의 안전을 단 한 명의 운영자가 관리하는 단일 노드에 맡기기로 결정한 "인간의 판단", 그것이 이 사건의 진짜 원인이다. 기술이 완벽해도 설정값은 사람이 결정하기 때문이다.

2. Aave의 거버넌스가 방아쇠를 당겼다

해커가 허위로 발행한 116,500 rsETH를 현금화하기 위해 선택한 타겟은 Aave였다. 여기서부터 이번 사태의 성격이 근본적으로 바뀐다. 외부 프로토콜에 대한 해킹이, Aave 내부의 의사결정(거버넌스) 실패라는 전혀 다른 종류의 문제로 변질된 것이다. Aave의 코드는 안전했고, 감사도 철저했으며, 리스크 프레임워크도 존재했다. 그러나 이 모든 기술적 안전장치는 사람들의 투표와 결정 때문에 무용지물이 됐다.

첫 번째 방아쇠는 LTV(Loan-to-Value, 담보인정비율)의 경쟁적 상향이었다. Aave의 경쟁 프로토콜들이 rsETH의 LTV를 70% 수준에서 보수적으로 유지할 때, Aave 거버넌스는 이를 93%까지 끌어올렸다. 100달러어치 rsETH를 담보로 넣으면 93달러의 진짜 WETH(이더리움)를 바로 빌릴 수 있다는 뜻이다. 표면상으로는 "시장 점유율을 높이자"였지만, 실질적으로는 돈을 더 많이 벌고 싶은 탐욕이었다.

두 번째 방아쇠는 리스크 관리 주체의 교체 타이밍이다. 오랜 기간 Aave의 리스크를 관리해온 Chaos Labs가 4월 6일 보수 불만과 업무 과중을 이유로 사임했다. 후임으로 들어온 LlamaRisk 팀은 사태 발생 불과 9일 전, "온체인 데이터상 건강하고 유동성이 충분하다"는 피상적 근거만으로 rsETH의 공급 한도를 상향하는 안건을 통과시켰다. 사실 온체인 데이터는 현재의 거래량을 보여줄 뿐, 그 자산이 어떤 취약한 크로스체인 브릿지를 건너왔는지는 보여주지 못한다.

유동성 재스테이킹 토큰(LRT)인 rsETH를 변동성이 낮은 스테이블코인과 유사한 리스크 등급으로 취급한 것은 Aave의 금융공학적 오만이었다. 심지어, 특정 서비스 제공자의 로비가 작용했다는 소문이 사실이라면, 이는 DAO 거버넌스의 구조적 부패를 여실히 보여주는 대목이다.

*** LRT(Liquid Restaking Token):** rsETH처럼 스테이킹 보상을 받으면서도 언제든지 사고팔 수 있는 유동성 토큰.

*** Leveraged Looping:** 담보를 넣고 돈을 빌린 뒤, 그 돈으로 다시 같은 담보를 만들어 반복적으로 레버리지를 높이는 전략. 수익은 커지지만 위험도 폭발적으로 커진다.

그러나 진짜 구조적 문제는 더 아래에 있다. 지금의 DeFi가 얼마나 기형적인 모래성 위에 지어져 있는지 해부할 필요가 있다. 사용자는 ETH(이더리움)를 Lido에 예치해 stETH를 받고(1차 파생), 이 stETH를 EigenLayer에 재스테이킹해 추가 수익을 얻으며(2차 파생, 기초 자산 하나로 두 프로토콜의 보안을 동시에 책임지는 셈이다), 여기서 나온 자산을 KelpDAO가 다시 유동화해 rsETH로 발행한다(3차 파생). 이 시점에서 rsETH는 원본 ETH로부터 세 단계나 멀어진 '영수증의 영수증의 영수증'이다. 그리고 탐욕의 종착지는 Aave다. 사용자들은 rsETH를 Aave에 담보로 맡기고 실제 ETH를 대출받은 뒤, 그 ETH를 다시 stETH → EigenLayer → KelpDAO → rsETH로 돌려 Aave에 재담보화한다. 이른바 레버리지 루핑(Leveraged Looping Position)이다.

이것은 2008년 월스트리트가 서브프라임 모기지를 CDO로 포장해 파생의 파생의 파생을 벌였던 무한 재담보화의 블록체인 버전에 지나지 않는다. 코드로써 모든 것을 해결하고 '이 좋은 걸 왜 안하지?'라는 안일한 일부 코더들의 오만한 행태였다. 단, 이 시스템은 하나의 파이프라인(이 경우 LayerZero의 1-of-1 DVN)이 끊어지면 전체가 무너지는 단일 실패점(Single Point of Failure) 구조를 가지고 있었다. 실제로 공격자는 이 구조의 정점에서 위조된 116,500 rsETH를 Aave에 밀어 넣고 93% LTV를 지렛대 삼아 $2억 3,600만의 실제 WETH를 대출받아 유유히 도망쳤다. Aave에는 가치가 훼손된 허위 rsETH와 최소 $1억 2,370만에서 최대 $2억 3,010만 규모의 악성 부채(Bad Debt)만이 남았다.

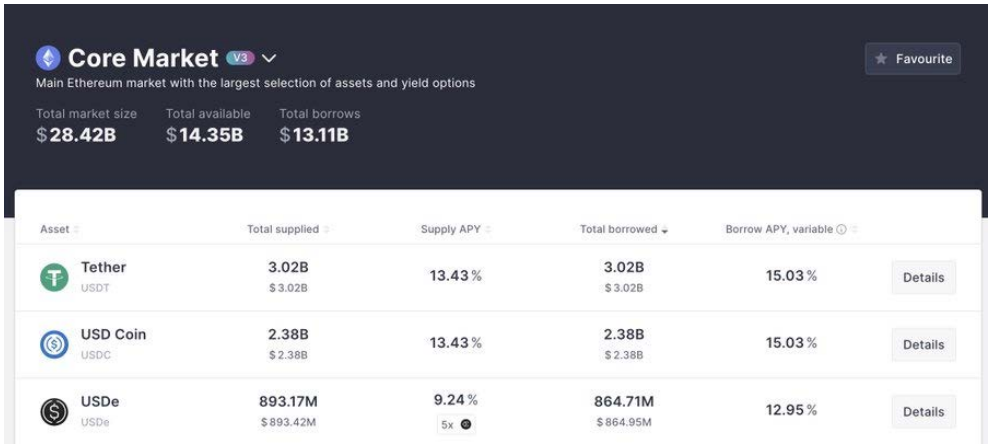
3. 유동성 데스 스파이럴: 100% 활용률의 덫

* **Utilization Rate(자본 활용률):** Aave 풀에 있는 돈 중 실제로 빌려간 비율. 100%가 되면 풀에 현금이 1원도 남지 않아 출금과 대출이 모두 막힘.

이번 해킹 사건이 단순히 "3억 달러를 도둑맞은" 수준으로 끝나지 않고 극도로 위험한 이유는, 그로 인해 발생한 2차 대란(유동성 데스 스파이럴) 때문이다. 저스틴 선(Justin Sun)과 MEXC 등 대형 고래 투자자들은 사태를 직감하자마자 수십억 달러 유동성을 Aave에서 즉각적으로 빼냈다. 그 결과 Aave의 핵심 시장인 WETH(이더리움), USDT, USDC의 자본 활용률(Utilization Rate)이 순식간에 100%를 찍었다. 활용률 100%라는 것은 대출해줄 돈이 완전히 바닥났다는 뜻이다. 무엇보다 치명적인 사실은, Aave에 돈을 맡긴 일반 예치자들이 자신의 돈을 단 1달러도 출금할 수 없다는 점이다.

Aave Core Market V3 대시보드의 수치는 적나라한 상황을 보여준다. 전체 시장 규모는 $28.42B인데, 실제로 빌려갈 수 있는 돈(Available)은 $14.35B, 이미 빌려간 돈은 $13.11B다. 특히 USDT는 34억 달러 규모 풀에 가용 유동성이 고작 $4,762밖에 안 되고, USDC도 $2.38B 풀에 $11,970 정도만 남아 있다. 이 숫자는 "시스템이 사실상 멈췄다"는 뜻이다. 그 때문에 USDT 대출 이자(Borrow APY)는 14.21%, Core Market V3 기준으로는 15.03%까지 폭등했다.

그림 1. Aave V3 Core Market의 전체 규모를 한눈에 보여주는 대시보드
하단에는 스테이블코인 풀의 Supply/Borrow APY가 기재되어 있는데, USDT의 Borrow APY가 15.03%, USDC가 15.03%에 달해 정상 시장 수준을 한참 벗어난 유동성 경색 신호를 보여줌.



자료: Aave, 미래에셋증권 리서치센터

* **Liquidation(청산):** 담보 가치가 떨어지면 제3자가 대신 빚을 갚고 할인된 가격으로 담보를 가져가는 DeFi의 자동 안전장치.

더 무서운 문제는 청산 메커니즘이 완전히 마비된다는 점이다. DeFi의 근간이 되는 기본 안전장치는 차입자의 담보 가치가 하락할 때 제3자 청산인이 대신 갚아주고, 이에 대한 **급부로서** 담보를 할인된 가격에 가져가는 청산(Liquidation) 구조에 있다. 즉, "담보 가치가 떨어지면 다른 사람이 대신 빚을 갚아주고, 대신 할인된 가격으로 담보를 가져가는" 시스템이다.

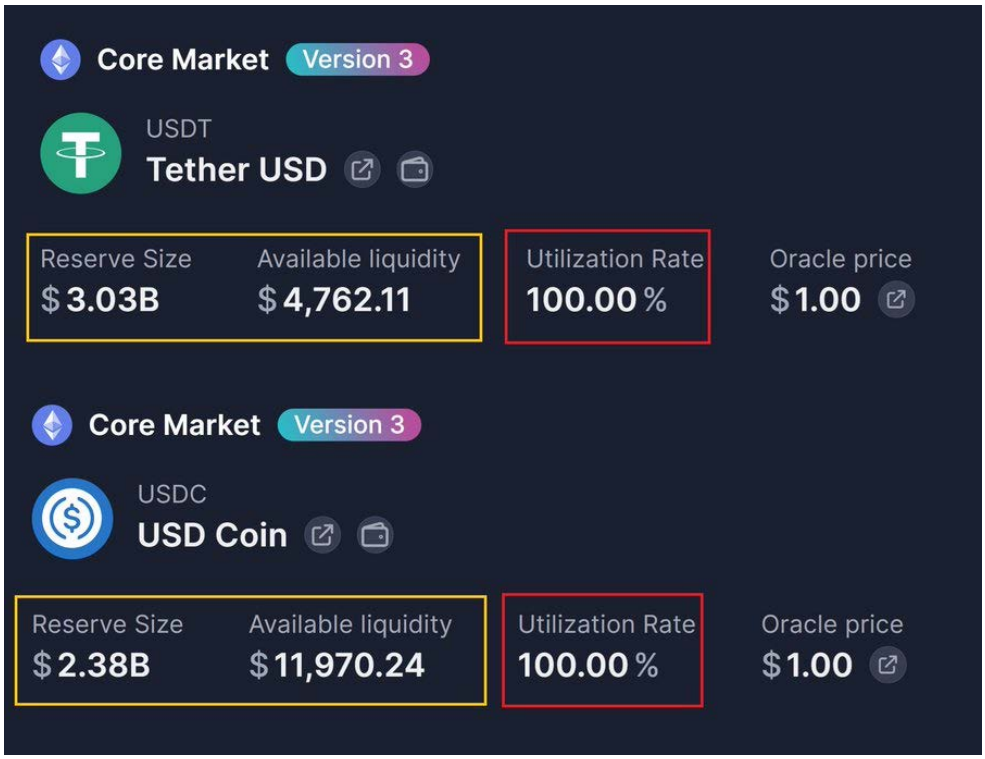
그러나 활용률이 100%인 상황에서는, 청산인이 담보의 대가로 받아낼 현금 자체가 풀에 존재하지 않게 된다. 영수증 토큰(aWETH)으로 받더라도 이를 WETH로 전환하려면 다시 풀에서 출금해야 하는데, 출금 자체가 불가능하니 말이다. 결국 청산인들은 청산을 아예 포기하거나 극소량만 집행하게 된다.

만약 이 상태에서 거시 충격으로 이더리움 가격마저 급락하게 된다면, Aave는 위험한 대출을 정리하지 못한 채 수십억 달러 규모의 추가 악성 부채를 떠안게 된다. 이게 바로 유동성 데스 스파이럴(연쇄 붕괴)다.

* **aWETH / aUSDT:** Aave에 ETH나 USDT를 예치하면 받는 영수증 토큰. 원래 자산을 증명해주지만, 지금은 출금이 막혀서 가치가 떨어진 상태

자산이 묶였다는 사실을 인지한 사용자들은 비정상적인 탈출을 시도하고 있다. Aave에 ETH를 맡긴 사람들은 Uniswap에서 aETH를 1~3% 손해 보면서 팔아서라도 돈을 빼려 한다. 이 사람들은 그나마 사정이 낫다. USDT·USDC 예치자들은 상황이 더 심각하다. 이들은 자신이 맡긴 aUSDT·aUSDC를 담보로 GHO, DAI, USDe 등 다른 스테이블코인을 빌려(대출 이자 15% 수준, 10~25% 손실 감수) 다른 프로토콜로 도피하고 있다. 이 과정에서 다른 스테이블코인 풀마저 활용률 100%에 근접해가며, "살아남으려면 무슨 수를 써서라도 유동성을 빼내라"는 죄수의 딜레마가 작동 중이다.

그림 2. Aave USDT·USDC 풀 Utilization 100%에 대한 부분
USDT 풀은 Reserve Size $3.03B에 Available Liquidity 단 $4,762.11
USDC 풀은 Reserve Size $2.38B에 Available Liquidity $11,970.24로
두 풀 모두 Utilization Rate 100.00%...
50억 달러 규모의 스테이블코인 풀에서 즉시 인출 가능한 현금이 채 2만 달러가 되지 않는다



자료: Aave, 미래에셋증권 리서치센터

* **Umbrella Safety Module & Slashing:** Aave의 비상 안전 기금. 악성 부채가 생기면 이 기금의 자산을 자동으로 소각해서 손실을 메우는 시스템.

Aave에는 최후 방어선인 Umbrella Safety Module에는 약 $5,000만어치의 WETH가 존재한다. 그러나 이번 악성 부채 규모는 최소 $1억 2,370만에서 최대 $2억 3,010만이다. 안전 모듈 자본을 전액 소각(Slashing)하더라도 부채의 28~40%만을 메울 수 있다는 뜻이다. 나머지 1억 달러 이상의 구멍은 결국 선량한 aWETH 예치자들이나 Aave 트레저리(현재 약 $8,350만 보유)가 떠안아야 할 가능성이 높다. 다행히 Umbrella는 이미 Slashing 작동을 시작했으나, 그것만으로는 구멍을 메우지 못한다는 것이 문제의 본질이다.

4. Arbitrum 보안 위원회의 고육지책: Code is Law의 공식 사망 선고

* **Security Council:** L2의 비상 권한을 가진 소수 위원회. 위기 시 관리자 권한(Admin Key)을 발동해 체인 상태를 변경할 수 있다.

필자는 이 사건이 크립토 역사를 2026년 4월 20일 이전과 이후로 갈라놓았다고 해석한다. Arbitrum 보안 위원회(Security Council)가 KelpDAO의 해커의 주소에 보관되어 있던 30,766 ETH(약 $70.97M)를 강제 회수했기 때문이다.

그림 3. Arbitrum 공식 성명 트윗
"Code is Law의 공식 사망 선고"이자 "L2 = 관리되는 금융망"을 뒷받침하는 공식 자료
특히 "law enforcement input" 문구는 본문의 "FBI와 협력해 비상키를 돌려 자산을 되찾아 올 수 있다"라는 의미로 해석.

자료: Arbitrum, 미래에셋증권 리서치센터

Arkham Intelligence 데이터를 보면 상황이 명확하다. "KelpDAO Attacker"로 표시된 주소(0x5d3...)의 자산이 0x000...DA0이라는 특수 동결 지갑으로 한꺼번에 이동됐고, 해커 지갑 잔고는 사실상 0에 가까워졌다. 공격 직전까지 이 주소의 총 자산은 1억 7,451만 달러였고, Aave와의 거래 규모만 4억 6,452만 달러에 달했다.

Arbitrum은 공식 성명을 통해 "비상 조치를 발동하여 해커의 주소를 동결했으며, 보안 위원회가 기술적 접근으로 자금을 중간 동결 지갑(intermediary frozen wallet)으로 이동시켰다"고 밝혔다. 그리고 결정적 문구가 뒤따른다. "법 집행 기관의 입력과 해커의 신원 확인을 바탕으로 내려진 결정"이라는 것이다. 자금은 이제 Arbitrum 거버넌스의 추가 조치를 통해서만 이동이 가능하며, 관련 당사자들과 협의해 처리될 예정이다.

북한 해커는 LayerZero의 설정 취약점을 이용해 트랜잭션을 만들었을 뿐이다. 사실 기술적 관점에서 엄밀하게 말하면, '정당한' 트랜잭션이었다. 그럼에도 Arbitrum 거버넌스는 관리자 권한(Admin Key, Security Council)을 발동해 해커의 프라이빗 키 없이 임의로 체인 상태(State)를 변경하고 자금을 빼앗아왔다. "북한이 훔친 돈을 Arbitrum이 다시 훔쳐왔다"는 코이너들의 평가는 사실 관계상 정확하다.

*** Code is Law:** "스마트 컨트랙트 코드가 곧 법이다"라는 DeFi의 핵심 철학. 이번 사건으로 이 믿음이 크게 흔들렸다.

이 사건이 철학적으로 시사하는 바는 꽤 의미심장하다. 비트코인 탄생 이래 암호화폐의 가장 근본적인 철학은 검열 저항성(Censorship Resistance)과 불변성(Immutability)이었다. "내 프라이빗 키가 없다면 그 누구도 내 자산을 옮길 수 없다"는 것은 매우 강력한 도그마이자 믿음이었다. 그러나 Arbitrum의 이번 조치는 L2 네트워크가 코드로만 돌아가는 무신뢰(Trustless) 망이 아니라, 소수의 위원회(인간)가 언제든 장부를 수정할 수 있는 Web 2.0 은행 서버와 본질적으로 동일한 구조임을 전 세계에 커밍아웃한 사건이다. 고객이 보이스피싱을 당했을 때 시중은행이 계좌를 동결하고 자금을 되돌려주는 것과 논리적으로 단 1%도 다르지 않은 프로세스다.

표 1. 기관 투자자(Smart Money)들은 L2를 어떻게 바라볼까? BlackRock·Fidelity·a16z 등이 자산 배분할 때 쓰는 리스크 계층

단계	유형	핵심 특성	리스크 수준	기관 수용도
1단계	Alt L1 (이더리움과 무관한 대안)	이더리움과 무관한 독립 체인, 독자적 검증자 네트워크	최고 위험. 검증자 수·분산도 미검증	거의 불가 (규제 불확실성)
2단계	Corporate System, CEX (사실상의 중앙화 DB)	검증자 1명. 사실상 중앙화 데이터베이스	매우 높음. 단일 장애점(SPOF)	제한적 (내부 용도만)
3단계	Validium / Optimium L2 (데이터를 외부에 두는 L2)	DA(데이터 가용성)은 이더리움 밖에 둠.	높음. DA 레이어 신뢰 필요	조건부 수용 (저가치 자산만)
4단계	Stage 0 Rollup L2	비상키(Admin Key) 존재. 개발자가 언제든 변경 가능	중간. 개발자 독재 가능	제한적 (파일럿 수준)
5단계	Stage 1 Rollup L2	비상키 + 다수결 위원회. 감시·견제 체제 작동	낮음. 다수결 변경만 가능	수용 가능 (실전 배포)
6단계	**Stage 2 Rollup L2**	**비상키 없음. 코드만 작동, 인간 개입 불가**	**최저. L1 보안 완전 상속**	**Gold Standard (투자 가능)**

자료: 미래에셋증권 리서치센터

위 표에서 보듯, 필자가 작성한 2월 리포트 「올해는 이더리움이다」 18페이지에서 제시했던 L2 리스크 매트릭스(Stage 0/1/2)가 완벽하게 실증되었다고 본다. Arbitrum을 비롯한 대다수 주요 롤업은 Stage 1 단계에 머물러 있으며, 이 단계의 핵심 특성은 "비상키 존재 + 다수결 보안 위원회 승인"이다. 해당 리포트에서는 이 구조를 "실전 배포가 수용 가능한 수준"으로 평가했다. 이번 Arbitrum의 $70.97M 강제 회수 사건은 이 비상키가 이론상의 안전장치가 아니라 위기 상황에서 실제로 작동하는 프로세스임을 전 세계에 증명한 것이다.

그리고 여기서 2016년 DAO 해킹 당시 이더리움 L1이 하드포크로 장부를 되돌렸던 아마추어적 과거와의 결정적 차이가 드러난다. 이번 강제 개입은 L1이 아닌 L2에서 일어났다. 그리고 이번에는 이더리움 L1은 어떤 개입도 하지 않았다. 그저 12초마다 기계적으로 블록을 생성하며 발생한 모든 트랜잭션을 묵묵히 기록했을 뿐이다. L2는 통제 가능한 핀테크 망이 되고, L1은 그 모든 핀테크 망의 최종 정산을 기록하는 유일한 중립 영토로 남는다는 거대한 분업이, 처음으로 물리적으로 실증된 순간이다.

5. 책임 전가의 대치/교착 상황과 DeFi의 민낯

Aave의 창립자 Stani Kulechov를 비롯한 코어 팀이 기술적 해결에 집중하면서도 여전히 조용한 이유는 기술 문제가 아니라, 누가 이 막대한 손실을 떠안을 것인가를 두고 치열한 법적·정치적 눈치싸움이 벌어지고 있기 때문이다.

우선 KelpDAO에게는 직접적 책임이 있다고 보인다. $10억 이상의 자산을 다루면서 1-of-1 DVN을 선택한 것은 기본적인 운영 보안(OpSec) 실패였다. LayerZero가 "적어도 2개 이상 쓰라"고 여러 번 경고했는데도 KelpDAO는 이를 무시했다.

그리고 LayerZero도 간접적 책임이 있다. 1-of-1 설정을 신규 프로젝트의 기본값(default)으로 제공했고 최소한의 보안 기준을 강제하지 않은 설계상의 문제다. 현재 양측은 서로를 공개적으로 비난하는 blame game(책임 떠넘기기)을 하고 있다. LayerZero는 "KelpDAO가 1/1을 선택했고 우리는 여러 번 경고했다. 공격자는 북한 Lazarus 그룹일 가능성이 높다"고 주장하고, KelpDAO는 "1-of-1은 LayerZero의 기본 설정이었고, 실제 뚫린 것은 LayerZero Labs가 운영하는 DVN 인프라"라고 반박한다.

*** Socialize: 손실을 전체 rsETH 보유자에게 골고루 나눔**

*** Isolate:** 피해를 L2 사용자들에게만 집중시킴

어찌 됐든 현재 KelpDAO는 양자택일 앞에 서 있다. (a) 전체 사회화(Socialize) 방식을 택하면 rsETH 전체 보유자에게 17.5%의 손실을 일괄 분배하게 되며(rsETH 가치 15.12% 하락), 이 경우 Aave가 떠안아야 할 악성 부채(bad debt)는 1억 2,370만 달러로 줄어든다. (b) L2 격리(Isolate) 방식을 택하면 이더리움 메인 네트워크의 rsETH는 100% 보호되는 대신 L2에서의 rsETH 보유자는 73.5%의 손실을 떠안게 된다. 이 경우, Aave의 악성 부채는 $2억 3,010만으로 확대된다. KelpDAO의 재무 규모가 제한적이고, LayerZero와의 책임 공방이 계속되다 보니, KelpDAO가 단독으로 전액 메우는 선택지는 사실상 사라졌다.

*** Trustless: 코드와 스마트 컨트랙트만 믿고 인간을 믿지 않는 탈중앙화 금융**

*** TradFi:** 전통 금융(Traditional Finance). 사람·법·합의에 의존하는 방식.

Aave의 딜레마는 더 복잡하다. 이미 rsETH 시장을 V3·V4 모두 즉시 동결하고 Umbrella Safety Module Slashing(자동 소각)을 작동시켰다. 그러나 "우리가 트레저리 자금으로 전액 보상하겠다"고 먼저 선언하는 순간, LayerZero나 KelpDAO로부터 배상을 받아낼 협상 레버리지를 상실하게 된다. 그렇다고 반대로 침묵을 유지하면 Aave에서 돈이 계속 빠져나가면서 프로토콜의 신뢰도가 회복 불가능한 수준으로 추락한다. 이러한 교착 상태는 DeFi가 오랫동안 외쳤던 '스마트 컨트랙트 기반 무신뢰(Trustless) 금융'이라는 슬로건이 여전히 허상이었음을 증명한다. 위기가 닥치면 결국 책임 공방, 법적 다툼, 정치적 합의라는 지극히 인간적이고 전통적인 금융(TradFi) 방식으로 돌아가게 된다는 사실을 이번 사건이 적나라하게 드러낸 것이다.

6. 거시적 재편: AI 해킹 시대의 L2 양분화

지금까지 우리는 해킹, Aave의 거버넌스 실패, Aributrum의 강제 개입을 자세히 살펴봤다. 하지만 이 모든 사건을 관통하는 진짜 큰 흐름이 하나 있다. 10년 동안 크립토 업계가 믿어 온 "교조주의적 탈중앙화"라는 종교가 이제 소멸했고, 그 잿더미 위에서 블록체인 생태계가 두 갈래로 명확히 갈라지고 있다는 사실이다.

(1) 왜 지금인가: AI-해킹 시대의 임계점 돌파

이번 Kelp DAO 사건을 단순한 "한 번의 해킹"으로 치부하면 안 된다. 2026 Hack Scoreboard를 보면 그림이 달라진다. 2026년 1~4월 벌어진 주요 해킹만 모아도 상황이 심각하다.

그림 4. 2026년 1~4월 단 4개월 동안 벌어진 주요 해킹 14건을 한 장에 집약한 스코어보드
KelpDAO $290M을 필두로 누적 10억 달러를 훌쩍 넘는 피해 규모
공격 유형이 Bridge Exploit, Protocol Drain, Social Engineering, Physical Attack, Key Compromise, Smart Contract, Oracle Manipulation까지 7종 이상으로 다양화된 점이 핵심
이번 사건이 고립된 일회성 사고가 아니라 AI 해킹 시대의 임계점 돌파를 보여주는 시스템적 징후

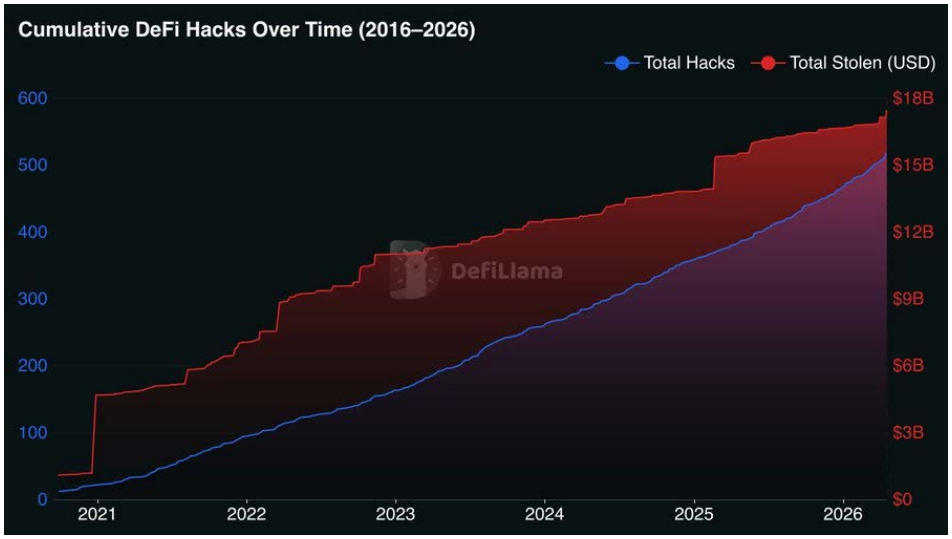
Name	Amount	Date	Type
KelpDAO	$290M	April	Bridge Exploit
Drift Protocol	$285M	April	Protocol Drain
Hyperbridge	$2.5M	April	Bridge Exploit
Resolv Labs	$25M	March	Infra Compromise
Sillytuna	$24M	March	Physical Attack
Kraken Whale	$18.2M	March	Social Engineering
Venus Protocol	$2.18M	March	Protocol Exploit
IoTeX Bridge	$4.4M	February	Bridge Exploit
Trezor Victim	$284M	January	Social Engineering
Step Finance	$30M	January	Key Compromise
Truebit	$26.4M	January	Smart Contract
SwapNet	$13.4M	January	Smart Contract
SagaEVM	$7M	January	Smart Contract
MakinaFi	$4.1M	January	Oracle Manipulation

자료: 미래에셋증권 리서치센터

단 4개월 동안 KelpDAO $290M, Drift Protocol $285M, Trezor Victim $284M, Step Finance $30M, Truebit $26.4M, Resolv Labs $25M, Sillytuna $24M, Kraken Whale $18.2M 등 주요 사건만 모아도 누적 10억 달러의 피해 금액을 훌쩍 넘는다. 공격 유형도 브릿지 해킹, 프로토콜 돈 빼내기, 인프라 침투, 물리적 공격, 사회공학, 키 탈취, 스마트 컨트랙트 버그, 오라클 조작까지 전방위로 퍼져 있다. 사이버 해킹의 표면이 이 정도로 넓어진 상황을 단일 방어선으로 막는다는 것은 이제 물리적으로 불가능하다.

DefiLlama 누적 차트를 보면 추세가 더 분명해진다. 2016년부터 2026년까지 누적 518건, 180억 달러에 이른다. 그런데 정작 눈여겨봐야 하는 것은 수치가 아니라 기울기다. 2021~2024년까지 완만한 선형 상승을 그리던 곡선이, 2025~2026년 구간에서는 수직에 가까운 기울기로 꺾였다. 이는 공격이 양적으로 늘어난 것이 아니라 질적으로 완전히 달라졌다는 신호다.

그림 5. 년치 DeFi 해킹의 누적 건수와 피해 금액을 한 장에 담은 DefiLlama의 장기 추이 차트
518건의 누적 해킹, 180억 달러의 누적 손실이라는 수치가 압도적이나, 주목해야 할 것은 기울기
2025~2026년 구간에서 거의 수직으로 꺾여 올라가는 파라볼릭 패턴
최신 AI 공격 역량의 질적 도약을 시각적으로 실증



자료: DefiLlama, 미래에셋증권 리서치센터

도약의 정체는 역시 AI다. 필자의 지난 3월 리포트에서 인용했던 EVMBench 데이터에 따르면, 최신 AI(GPT-5.3-Codex)의 스마트 컨트랙트 해킹 성공률은 72.2%에 이른다. 북한의 정찰총국(DPRK) 해커들이 이번 KelpDAO의 해킹 과정에서 AI로 취약점을 스캔하고 익스플로잇 코드를 자동 생성했을 확률은 99%에 수렴한다.

방어자가 패치를 적용하는 속도보다, 공격자가 취약점을 찾아내는 속도가 압도적으로 빨라진 것이다. 비탈릭 부테린이 오랫동안 강조해온 "방어적 가속(d/acc)"과 "암호학적 민첩성(Cryptographic Agility)"이 왜 그토록 절박했는지, 이제서야 시장이 체감하고 있다. "혁신을 위해 보안을 조금 타협한다"는 일부 크립토 업계의 변명은 AI 시대에는 전혀 통하지 않는다.

(2) TVL의 구조적 증발: 조정이 아니라 뱅크런

자본이 빠져나가는 규모와 속도를 보면, 이것은 단순한 시장 조정이 아닌 것으로 보인다. DefiLlama TVL 대시보드를 보면 숙청의 강도가 확연히 느껴진다. Swellchain -70.43%, DuckChain -92.22%, Celestia -45.64%, Hydra Chain -45.34%, Merlin -40.97% 등 체인을 가리지 않고 TVL이 반토막 이상 증발했다.

그런데 의문이 든다. KelpDAO가 뚫렸는데 왜 상관도 없어 보이는 Celestia나 Merlin에서 돈이 빠져나가는가. 이것이 바로 '구성 가능성의 저주(Curse of Composability)'다. 대부분의 L2 체인 TVL은 해당 체인이 자체 발행한 네이티브 자산이 아니라, 브릿지를 타고 넘어온 포장 자산(Wrapped Assets)으로 채워져 있다.

KelpDAO-LayerZero 브릿지 해킹은 "L2에 있는 내 자산은 언제든 허공으로 증발할 수 있는 장부상 숫자에 불과하다"는 원초적 공포를 전 시장에 각인시켰다. 스마트 머니는 이 공포를 피하려 모든 L2에서 유동성을 빼내 이더리움 L1이나 중앙화 거래소(CEX)로 대피시키는 중이다.

여기에 리스테이킹 폰지의 연쇄까지 겹친다. rsETH의 페깅(ETH에의 가격 고정)이 깨지자 ezETH, pufETH, weETH 같은 비슷한 구조의 토큰에 대한 신뢰가 도미노처럼 무너지고 있다. 이것이 바로 이번 TVL 증발을 단순 조정이 아니라, "무허가성 크로스체인 금융"이라는 비즈니스 모델 자체에 대한 시장의 파산 선고로 읽어야 하는 이유다.

(3) 교조주의적 탈중앙화의 끝

우리가 10년 넘게 믿어온 '순수한 탈중앙화(Absolute Decentralization)'는 완벽한 허상이었다. 업계가 믿어온 3가지 슬로건("코드가 법이다", "무신뢰", "검열 저항성")은 Arbitrum 보안 위원회의 $70.97M 강제 회수 한 방에 동시에 무너졌다. Code is Law가 진짜 진리였다면 Arbitrum은 그 자금 이동을 지켜봐야 했었다. 그러나 현실은 달랐다. 운영진은 회의를 열었고, 다수결 투표를 했고, 마스터 키를 돌려 해커의 지갑을 얼렸다. 그리고 돈을 강제로 빼앗아왔다.

왜 천재적인 개발자들이 완전한 Stage 2로 가지 않고 Stage 1(비상키 존재)을 유지했을까? 답은 의외로 단순하다. 그들 스스로도 자신들의 코드를 100% 믿지 못했기 때문이다. 수백억 달러가 오가는 금융망에서 버그 하나로 모든 돈이 증발하는 것을 그대로 두는 것은 탈중앙화가 아니라 방임이자 직무 유기다. 그래서 그들은 최악을 대비해 '인간이 개입할 수 있는 뒷문(Admin Key)'을 열어뒀다. 대중 앞에서는 탈중앙화를 외치며 마케팅했지만, 실제 시스템 아키텍처는 철저하게 '통제 가능한 중앙화된 핀테크 망'으로 설계해뒀던 것이다. 탈중앙화는 포장지였을 뿐, 본질은 언제나 관리되는 금융 시스템이었다. 그리고 이번 사태가 드러낸 것은, 오히려 그 '뒷문'이야말로 기관 자본을 끌어들이기 위한 핵심 전제였다고 사료된다.

(4) L2 양분화: 'Managed L2'와 'Agent-Only L2'의 두 갈래 길

이번 사태는 L2 생태계를 두 개의 선명한 스펙트럼으로 갈라놓을 것이라 판단된다. 흥미로운 점은 이 두 갈래가 서로를 부정하는 관계가 아니라, 오히려 서로를 필요로 하는 보완 관계라는 사실이다.

첫 번째 갈래는 'Managed L2(관리형 L2)' 혹은 'TradFi-native L2(전통 금융업체 특화 L2)'다. Admin Key와 보안 위원회(Security Council)를 명시적으로 유지해, 치명적 해킹이 발생했을 때 거버넌스가 자산을 동결·회수할 수 있도록 프로토콜 수준에서 보장하는 계층이다.

KYC/AML과 Compliance(규제 준수) 기능이 내장되고, 그 위에 RWA·토큰화 국채·BlackRock BUIDL·JP Morgan MONY 같은 규제 자산이 쌓이게 된다. 월가가 그동안 수십조 달러를 L2에 넣지 못했던 유일한 이유는 "해킹당하면 돌려받을 수 없다"는 공포였다. 그런데 Arbitrum이 이번 사태로 "FBI와 협력해 비상키를 돌려 자산을 되찾아 올 수 있다"는 사실을 공개적으로 실증해버렸다. 이제 이 계층은 사실상 은행·증권사·자산운용사의 온체인 지점으로 기능하게 된다. 탈중앙화라는 레토릭은 걸어두되 본질은 '관리되는 금융망'이라는 점이, 약점이 아니라 오히려 강점으로 인식되기 시작한 것이다.

*** Admin Key(관리자 키): L2 프로토콜 운영진이 긴급 상황에서 체인의 상태를 수정하거나 자금을 동결할 수 있도록 부여된 특별 권한. 탈중앙화의 반대편에 있는 '백도어'이자, 동시에 치명적 해킹 시 최후의 방어선**

*** 보안 위원회(Security Council):** Admin Key를 단독으로 쥐지 않기 위해 복수의 검증된 개인·단체가 다수결로 합의할 때만 Admin Key가 작동하도록 설계된 거버넌스 기구. Arbitrum의 $70.97M 강제 회수는 이 위원회가 실제로 작동한 첫 대규모 실증 사례.

두 번째 갈래는 'Agent-Only L2(AI 에이전트 전용 L2)'다. 완전히 다른 철학으로 설계되는 계층이다. 인간의 탐욕이 거버넌스로 스며들 통로 자체를 원천 차단하고, AI 에이전트만 경제 주체로 활동하는 '국소적 탈중앙화(Localized Decentralization)' 레이어다. 이번 사태로 인간 투자자는 Aave에서 겨우 3% 이자를 받으려고 전 재산을 날릴 리스크를 더 이상 감수하지 않을 것이다. Kelp DAO-Aave 사태가 인간 중심 DeFi의 구조적 한계를 너무도 뼈저리게 보여줬기 때문이다.

그렇다면 DeFi 대출 프로토콜은 아예 사라질까? 탈중앙화의 가치는 이제 없어진 걸까? 그렇지는 않다. 인간이 중심이 되는 한 탈중앙화는 구조적으로 어렵지만, 인간이 떠난 그 빈자리를 AI 에이전트가 채우면 이야기가 완전히 달라진다. 에이전트에게 '자산 100% 손실'은 감정의 문제가 아니라 수학적 확률 모델의 한 변수일 뿐이다. 공포에 휩싸여 뱅크런하지도 않고, 코딩된 조건에 따라 24시간 쉬지 않고 마이크로 트랜잭션을 수백만 번 실행할 뿐이다. 허술한 스마트 컨트랙트들이 AI 해커에게 모조리 박살 나는 동안, 살아남은 인프라는 오직 기계들만 신뢰할 수 있는 '기계 경제 인프라(Machine Economy Infrastructure)'로 진화해 나갈 것이다.

그런데 이 Agent-Only L2라는 것이 실제로 성립하려면 무엇이 갖춰져야 하는가? 필자는 다섯 가지 조건이 모두 만족되어야 한다고 본다. 이것이 완벽한 Stage 2에 도달하기 위한 출발점이다. 첫째는 Admin Key 제거 및 보안 위원회 해체를 통한 '코드만으로 굴러가는 구조'의 보장이다. Stage 0~1에 머물러 있는 롤업들은 이 계층에 들어올 자격 자체가 없다.

두 번째는 Based Rollup 아키텍처다. L1 검증자가 직접 L2 거래 순서를 정하는 구조로, 시퀀서 중앙화 위험과 MEV 독점 문제가 동시에 해소된다. 세 번째는 Native Rollup 프리컴파일(EIP-8079)이다. L1의 EVM 자체를 L2가 그대로 빌려 쓰게 만드는 기술이다.

네 번째는 필자가 이전 리포트들에서 일관되게 강조해온 에이전트 경제 인프라 스택의 완성이다. ERC-8004(에이전트 식별·평판), ERC-8128(권한 관리), x402(밀리초 단위 확정 결제)로 이어지는 세 표준이 자리를 잡아야 AI 에이전트가 경제 주체로서 계약·거래·정산을 수행할 수 있다.

그리고 가장 중요한 다섯 번째는 인간 UX의 원천적 배제다. 브릿지 UI, 거버넌스 토큰 투표 화면, 사회공학에 취약한 결제 확인창. 이 모든 것이 깨끗이 제거된, 오로지 기계 간 통신(Machine-to-Machine)만 존재하는 계층이어야 한다. 앞의 네 가지 기술 조건이 아무리 완벽해도, 인간이 드나드는 UI 한 장이 남아 있는 순간 KelpDAO의 1-of-1 DVN 같은 실수가 언제든 다시 반복될 수 있기 때문이다. 만약 KelpDAO가 애초에 이 다섯 조건을 모두 갖춘 L2 위에 있었다면, LayerZero 같은 외부 브릿지 DVN은 애초에 필요하지도 않았을 것이고, 위조 메시지는 L1 검증을 통과할 수조차 없었을 것이다.

여기서 중요한 개념적 전환이 필요하다. 크립토 업계의 오래된 전제는 "모든 체인이 최대한 탈중앙화돼야 한다"였다. 그러나 이번 사태가 증명한 것은 그 반대다. 인간의 탐욕이 거버넌스로 개입하는 한, 탈중앙화는 오히려 필연적으로 피해를 입는다. 따라서 탈중앙화는 '전역적(Global)'으로 적용될 대상이 아니라, '국소적(Local)'으로만 유의미하게 작동해야 의미가 있다는 것이 필자의 주장이다.

* Stage 0/1/2 롤업 분류: 이더리움 재단이 정의한 L2 탈중앙화 성숙도 단계. Stage 0은 운영진이 거의 모든 것을 통제하는 초기 단계, Stage 1은 Admin Key는 남아 있지만 보안 위원회의 다수결 합의가 필요한 단계, Stage 2는 Admin Key가 제거되고 오직 코드만으로 작동하는 완전한 탈중앙화 단계. 현재 Arbitrum, Optimism, Base 등 대다수 주요 L2는 Stage 1에 머물러 있음.

사람이 들어오는 계층에서는 차라리 Admin Key를 명시적으로 유지하고 규제 당국과 협력하는 '통제된 불변성(Governed Immutability)' 모델이 실질적으로 더 안전하다. 반대로 AI 에이전트만 활동하는 특화 L2에서는 엄격한 Stage 2 탈중앙화가 비로소 의미를 갖는다. 그곳에는 탐욕도, 실수도, 사회공학 공격 표면도 없다. 인간이 없으면 탐욕도 없고, 탐욕이 없으면 거버넌스 부패도 없다. 오직 여기서만 우리가 진정으로 원했던 순수한 의미의 "Code is Law"가 실제로 작동한다.

그리고 그 위의 L1 계층에서는 절대적·전역적 탈중앙화가 유지돼야 한다. 수백만 검증자가 글로벌로 분산된 이 계층이야말로 어느 L2의 실수·공격·붕괴도 흡수할 수 있는 중립 앵커이기 때문이다. 이번에 해킹당한 "47개의 rsETH만 존재하던 변방의 L2"는 비탈릭 부테린이 말해온 '격리와 특화'의 사례가 아니라, 그저 '팽창을 위한 팽창'의 잔재였다. 이번 산불은 그런 무의미한 L2들을 태워 없애는 거대한 숙청이다.

그리고 자본은 이미 움직이고 있다. 2월 리포트에서 썼듯 "ENSv2의 메인넷 복귀"와 같은 사례는 이제 예외가 아니라 표준이 될 것이다. 가스비가 대폭 낮아지고 데이터 가용성(DA) 비용이 떨어진 L1 환경에서, 신뢰도가 생명인 대형 인프라 프로젝트가 굳이 브릿지 해킹 리스크를 안고 L2에 머물 이유가 사라졌다. 대형 프로젝트들은 L1이나 ZK로 완전 무장한 극소수 최상위 L2로만 뭉치는 질적 통합을 강제받게 될 것으로 사료된다. 그와 동시에 기관 자본은 Managed L2 쪽으로 대거 유입되기 시작할 것이다. Arbitrum이 보여준 '통제된 불변성' 모델은 BlackRock, Fidelity, JP Morgan 같은 기관이 쌍수를 들고 환영할 안전망이기 때문이다. 이들은 애초에 아나키즘적 탈중앙화에 관심이 없었다. 그들이 원했던 것은 블록체인의 기술적 효용(24/7 실시간 정산, 투명한 회계, 에이전트 호환성)뿐이었다. 이제 규제 준수와 자산 복구의 안전망이 검증됐으니, 수조 달러 규모의 RWA·토큰화 국채·기관 스테이블코인이 합법적으로 유입될 수 있는 진입 장벽이 소멸된 셈이다.

결국 모든 자본은 '안전한 곳'으로 향한다. 다만 "안전하다"는 말의 정의 자체가 이번 사태로 완전히 재정립되었다. 이제 "안전하다"는 말은 "탈중앙화되어 있다"와 같은 뜻이 아니다. 대신 "문제가 생겨도 회복이 보장된다"이거나, "인간의 개입 자체가 구조적으로 불가능하다" 둘 중 하나를 뜻한다. 전자는 Managed L2, 후자는 이더리움 L1과 극소수 Agent-Only L2의 영역이다. 그 중간에 어중간하게 걸쳐 있던 L2들은 이번 산불에서 살아남기 힘들 것이라 판단된다.

7. 최종 결론: '인프라로서의 이더리움 제국'

모든 L2가 사실상 중앙화된 은행처럼 변해갈 때, 이더리움 본체(L1)는 글로벌 최종 정산소라는 핵심 테제가 역설적으로 완성되고 있다고 사료된다.

2026년 4월, Kelp DAO 해킹·Aave 데스 스파이럴·Arbitrum $71M 강제 회수라는 대혼란이 벌어지는 동안, 이더리움 메인넷(L1)은 무엇을 했을까? 아무것도 하지 않았다. L1 검증자들은 Arbitrum의 강제 회수를 돕지도, Kelp DAO의 해킹을 막지도 않았다. 그저 12초마다 기계적으로 블록을 만들며, 발생한 모든 거래를 묵묵히 기록했을 뿐이다. 누군가의 돈을 강제로 빼앗지도, 장부를 임의로 되돌리지도 않았다. 2016년 DAO 해킹 때처럼 하드포크로 돈을 되돌렸던 아마추어적 과거는 이제 완전히 끝났다.

이것이 바로 Arbitrum Security Council이 $71M을 강제 회수한 사건의 가장 큰 의미다. L2는 인간(보안 위원회)이 개입해 문제를 해결하는 실용적 중앙화(Practical Centralization)를 받아들이고, L1은 그 어떤 인간도 손대지 못하는 절대 중립 영토로 남는다는 분업이 실제로 증명된 순간이었다.

따라서 앞으로의 모습은 이렇게 전망된다. L2 계층에서는 은행·증권사·게임사·국가 기관들이 각자 목적에 맞게 Admin Key(관리자 권한)를 쥐고 빠르게 운영하는 '실용적 중앙화'가 자리 잡을 것이다. 반면 L1 계층은 그 모든 L2가 하루 일과를 마치고 서로의 장부를 맞추러 돌아오는 유일하게 탈중앙화된 절대 중립 영토로 남게 된다. 이더리움 L1은 이제 미국 정부조차 장부를 임의로 고칠 수 없는 진정한 '신뢰 원자재(Trust Commodity)'로 자리매김했다.

모든 L2가 검열과 통제를 받아들이며 중앙화될수록, 그 모든 중앙화 주체들이 공통으로 믿을 수 있는 하나의 검열 불가능한 밑바탕에 대한 수요는 폭발적으로 증가한다. 이것이 바로 이더리움 L1의 진짜 힘이다.

물론 이번 위기는 단기적으로 ETH 가격에 하방 압력을 줄 수도 있다. 하지만 프로토콜 자체의 가치 포착 메커니즘은 오히려 더 강해진다. 안전한 L1 기반 RWA(토큰화 자산)와 AI 에이전트 경제를 담보하기 위해 더 많은 ETH가 스테이킹에 묶이는 공급 스퀴즈(공급 부족)가 심화되고, 미래에 수십억 개의 AI 에이전트들이 쏟아내는 밀리초 단위 초소액 결제(x402)와 ZK Proof 검증 과정에서 막대한 베이스 수수료가 소각될 것이기 때문이다.

낡은 DeFi의 고름(레버리지 루핑, 취약한 브릿지, 무한 재담보화)을 짜내는 이번 붕괴는, 오히려 가격이 진짜 펀더멘털(기초 가치)로 수렴하는 속도를 극단적으로 앞당기는 촉매제가 될 가능성이 매우 높다.

다만 한 가지 짚고 넘어가야 할 점이 있다. "Aave가 완전히 망할 것"이라는 예측은 과장이다. Aave의 관리 자산은 273억 달러 규모이고, 이번 악성 부채는 전체의 0.65%에 불과한 국지적 타격이다. LUNA 사태 같은 프로토콜 전체 붕괴는 아니며, 수개월에 걸친 거버넌스 조정으로 상처는 충분히 봉합될 가능성이 크다. 다만 '절대적 신뢰'는 영구적으로 훼손됐다는 점은 분명하다.

또한 “이더리움 L1이 유일한 승자”라는 말도 과도한 확신일 수 있다. 솔라나나 비트코인 생태계가 이번과 같은 스트레스 테스트를 의외로 잘 버틴다면, 가치는 이더리움 한 곳에만 집중되지 않고 온체인 전체로 재편될 수도 있다. 다만 수백만 검증자의 글로벌 분산과 검증 내재화 로드맵(Based Rollup, Native Rollup 프리컴파일)의 완성도에서, 현 시점 이더리움이 가장 앞서 있다는 사실은 변하지 않는다.

시장은 이제 혁신의 시대를 지나 ‘혹독한 검증과 규제적 옥석 가리기’의 겨울로 들어섰다. 허리띠를 졸라매야 할 때다. 개인 투자자들의 무작정 수익률 쫓기(Yield Farming)는 끝났고, 투기적 유동성은 소멸할 것이다. 반면에 기관 돈(수조 달러 규모)은 이더리움 L1 위의 RWA와 BlackRock BUIDL, JP Morgan MONY 같은 규제된 안전한 스테이블코인으로 집중될 것이다.

살아남을 L2는 이제 두 가지로 명확히 추려질 것으로 사료된다.

① Admin Key를 명시적으로 가지고 기관 자금을 적극 흡수하는 Managed L2

② Stage 2 + Based Rollup + Native Rollup 프리컴파일로 완전 무장한 AI 에이전트 전용 L2

이러한 혼란 속에서, 이더리움 L1은 “변동성 높은 DeFi 토큰의 근거지”라는 옛 이미지를 벗어던지고, 가장 견고한 글로벌 결제 및 기관 자산 정산의 중립 인프라로 재탄생하는 역사적 시험대에 올랐다. “탈중앙화라는 종교는 죽었다. 이제, 인프라로서의 이더리움 제국이 시작된다.”

Compliance Notice

- 당사는 본 자료를 제3자에게 사전 제공한 사실이 없습니다.
- 본 자료는 외부의 부당한 압력이나 간섭없이 애널리스트의 의견이 정확하게 반영되었음을 확인합니다.