

Renewed Crypto Winter? Will this Hacking Cold Lead to Flu?

Type: Editorial

Received: February 26, 2025

Published: March 14, 2025

Citation:

Mark Le Page. "Renewed Crypto Winter? Will this Hacking Cold Lead to Flu?". PriMera Scientific Engineering 6.4 (2025): 01-02.

Copyright:

© 2025 Mark Le Page. This is an open-access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Mark Le Page*

ESCP Business School, Paris, France

***Corresponding Author:** Mark Le Page, ESCP Business School, Paris, France.

Decentralized Finance (DeFi) has once again been in the news for the wrong reasons. Is it time for unsophisticated investors to be proscribed from accessing?

Even before President Trump chinked his first alcohol-free glass in celebration, the DeFi industry was looking forward to a welcome reset after Gary Gensler's capricious SEC. Many giants of the new economy attended his inauguration. A new era of optimism was palpable.

Nevertheless clouds of concern were not far away. The double launch of the President's and First Lady's memecoins, hit hard by two whales dumping at large on 25 February 2025, shows the continuing volatility of memecoins, where intrinsic value is difficult, if not impossible, to discover.

Meanwhile cyber threats had never quite left the horizon. How could they since the theft of 850 million bitcoin in the Mt Gox scandal in 2014, and the problematic corporate governance subsequent to the \$80 million "Rari Hack" of 2022? Further, security experts prophesied aggressive state actors launching a cyber-attack, robbing significant wealth from a DeFi platform.

21 February's Bybit hack, at US\$1.3 billion, was the sum of all fears. Elliptic, Arkham Intelligence, Verichains and Sygnia Labs all agree that the hack was the work of Lazarus, a front for North Korea. Intriguingly the weakness was not within Bybit, but the misnomered Safe wallet. Lazarus inserted malware JavaScript, and the rest is history.

These latest examples do nothing other than discredit the DeFi environment and discourage those of us who have championed DeFi through its highs and lows. They will do nothing to discourage regulators from limiting access to unsophisticated investors, who are in no position to understand the risks.

It is not time to draw up the drawbridge just yet. As Commission Peirce wrote, there are high returns to be made which should not be denied to investors [1]. At the same time, unsophisticated investors should be educated to stay away from memecoins. And it is heartening that third parties provided a capital injection to Bybit to restore the financial loss.

This should herald a platform for some form of third party(ies) underwriting of losses arising from hacks. Such underwriters would surely provide that a platform or dApp - including exchanges or wallets - has an annual independent cybersecurity audit. A poor audit could lead to the withdrawal of such insurance. Additionally any adverse findings should be published as a headline warning on the front page of a dApp, exchange or wallet. Investor education should also point towards this.

The DeFi industry certainly has a hacking cough, but medicine is yet available.

Foot Note

1. Peirce H. Out, Damned Spot! Out, I say! Statement on Omnibus Approval Order for List and Trade Bitcoin-Based Commodity - Based Trust Shares and Trust Units (2024).