RE: SR-CBOE BZX-2023-072

Jayson Hobby, Compound Companies and Ethereum Enterprise Alliance

Date: 28/11/23

SEC:

It is important that this proposal be rejected on grounds relating to both hacking, and more importantly reverse-hacking.

Spot Bitcoin and Ether publicly listed ETFs have well-known hacking vulnerabilities. Losses can occur on any decentralized or centralized platform whether spot crypto is in transit or dormant. Because of the nature of the assets, their trading and systems (poor or no compliance, poor controls, and little to no regulatory oversight), there's generally little or no remedy for a hack or loss.

Here the sponsor does nothing to address losses in custody or otherwise, merely disclosing that the average ETF investors will wear this risk - there's no way the average retail investor has any ability to evaluate, hedge or prepare for this risk transfer.

If the sponsor guarantees the provenance of all of the coins/tokens with some riskless collateral or escrow arrangement, maybe this works.

An even bigger risk seemingly missed by everyone is crypto provenance. That is, if the Trust owns crypto, how are we sure that those coins or tokens are not the product of an alleged hack from months or years earlier, only for the crypto to be "reverse hacked" out of the Trust's assets on the instructions of a U.S. or foreign court order. This reverse theft has happened a number of times, but is kept silent by crypto operators and their counsel.

One of the largest hacks was conducted by a combination of Oasis and Summerfi and based on a yet to be released UK court order.

Sincerely,

Hobby....

DEEP DIVES

The Oasis "counter-hack" and the centralization of defi

Wormhole, Jump Crypto, and Oasis demonstrate the centralization threat introduced by multisig-controlled upgradeable smart contracts.

MOLLY WHITE
FEB 26, 2023

♡ 68 💬 19 Share

Note: This essay is more technical than most of my writing, and so you may find the W3IGG glossary useful if there is unfamiliar jargon. If anything is too complex, feel free to drop a comment and I will do my best to explain further.

In February 2022, a hacker stole 120,000 wrapped Ethereum from Wormhole, a cross-blockchain bridge. It was (and still is) one of the largest hacks in the crypto world. Based on the Ethereum prices at the time, the hacker made off with around $320 million. Because it's crypto, there was no "undo".

A loss of this magnitude might spell the end for many crypto projects, but Wormhole had deep-pocketed backers. The crypto arm of the Chicago-based proprietary trading firm Jump Trading had acquired Certus One, the developers of Wormhole, some months prior.

Jump Crypto, the crypto subsidiary of Jump Trading, was launched in September 2021 following a $350 million raise, and has been heavily involved in the crypto ecosystem since: both by trading cryptocurrencies and market-making, but also developing software. Fellow Jump Trading subsidiary Jump Capital has also invested heavily in the industry as a venture fund. The Jump conglomerate has been in the news quite recently following the SEC charges against Do Kwon and Terra/Luna. Although the SEC complaint does not directly name Jump Trading, it has been reported that they are the "U.S. Trading Firm" mentioned in the lawsuit that profited enormously from the Terra fraud. The firm reportedly enjoyed an almost $1.3 billion (with a B) windfall after stepping in to rescue the Terra stablecoin's peg on at least one occasion in May 2021. This action was hidden from the public by Terra founder

Do Kwon, and the others who knew about it, and instead Kwon claimed that Terra had naturally regained its peg via a “self-healing” mechanism. He suggested this was a demonstration that it was not at risk of the kind of devastating collapse that ultimately occurred only a year later, and this “U.S. Trading Firm” made no apparent effort to correct the record.

But back to Wormhole: when the February 2022 hack occurred, Jump Crypto stepped up — putting $325 million of their own funds into the project. Wormhole offered a $10 million “bounty” [1] to the hacker if they returned the funds, but the attacker decided they’d rather just keep the $325 million, thankyouverymuch.

In the year since the hack, the hacker has taken a different strategy with their newfound riches than many other thieves. Rather than trying to launder and then cash out their profits into fiat, they have instead moved the funds through various decentralized finance (defi) protocols. In late January 2023, after a period of dormancy, they began to take highly-leveraged positions on the liquid Ethereum staking derivatives stETH (Lido) and rETH (RocketPool). In fact, between the capital they deployed and the leverage, they became the third-largest holder of wrapped stETH in existence. Some in the crypto industry were a little mystified, and wondered if perhaps the attacker was a crypto native taking “degen” positions. [2]

In order to lever up, the hacker opened two vaults on the Oasis protocol. Oasis is a project that was originally created by members of the MakerDAO team, and it serves as a frontend to the MakerDAO project. Oasis has since branched off into its own company, though it still remains the favored platform by MakerDAO — the big green “Use DAI” button on the MakerDAO homepage links to Oasis.