Poly Network hack: the silver lining

Published 14 September 2021

WisdomTree
Contributor

On August 10, the relatively young Poly Network found a lot of ‘locked-up’ funds had gone missing. Exploiting a vulnerability in the smart contracts used to manage Poly Network, the culprit managed to divert the equivalent of USD 600 million in cryptocurrencies. Then he or she returned the funds…

This turn of events was characteristically in line with the often surreal happenings that one comes to expect when working in the digital assets space for long enough. Somewhat counter-intuitively, the events also have a silver lining: they point to growing levels of security in the wider digital asset ecosystem, which have implications for asset managers already operating in or seeking to enter this space.

The Poly Network is one of the newer ‘de-fi’ (decentralized finance) platforms to emerge this year. Posting their first code to Github in late 2020, the young platform managed to attract over to USD 1 billion in ‘locked’ funds to power its cross-chain platform.

Upon discovering the theft of such a large amount of funds in August, the operators of Poly Network spilt onto social media to ask for the digital assets to be returned – hinting at the law enforcement repercussions of the theft. Shortly later, returning with a changed tone, the operators again publicly asked ‘Mr White Hat’ to return the assets and to be their ‘Chief Security Advisor’ as well as a USD 50,000 ‘bug bounty’. A day or so later – and most of the funds were returned.

Why would someone return so much?

In a Q&A posted shortly after returning the assets, the culprit explained that he/she hacked Poly Network ‘for fun’ and had no intention of keeping the stolen assets. Could this possibly be true?

Historically the preferred path of digital assets thieves was to launder stolen assets through intermediaries like exchanges. This is no longer the case. For many years most large exchanges have implemented KYC/AML1 ID requirements on users that exchange large amounts of assets. Very recently this position has changed – an example being Binance2, which now requires all users to go through these ID checks. It is no longer so easy to obscure the path of digital assets via exchanges, which makes their theft less likely in the first place.

The sheer amount of assets stolen was far too conspicuous to hide or evade attention. Moreover, tracing the path of digital assets has become its own cottage industry. The recipient addresses were hardcoded into the Poly hack, which means that the funds could be followed until they eventually hit a fiat-off ramp or exchange. With no way to convert the assets why hold onto them?

One final takeaway - the digital asset space is amongst the most adversarial of all software environments. Any mistake written into mission-critical software, which implies 100% uptime, will eventually be discovered when the pay-off for said discovery is so high. It is not unusual for a critical bug to be found in a relatively young platform – one that has not had the years of battle testing that other platforms have benefitted from. It is to be expected that attackers would strike at a younger platform, rather than the larger and older de-fi platforms, because of this lack of battle hardening. This has implications on how one might allocate a portfolio of digital assets in a risk-adjusted way – opting to allocated toward the older and more secure platforms that are less likely to incur such attacks.

Promising signs of a maturing, more secure eco-system

Hacks of digital asset exchanges, protocols and 'smart contracts' are not new. What is new are the counter-measures that have emerged to deal with and limit the losses potentially incurred from the cybersecurity incidents. This space is maturing, and becoming more secure, as time goes on particularly as greater regulatory scrutiny is applied to certain actors. This is all good news – a silver lining - as the space becomes less 'Wild West' and the nature and level of risks associated with investing in this asset class diminish.

1 Anti money laundering (AML); Know your client (KYC)

2 Binance is a cryptocurrency exchange which is currently the largest exchange in the world in terms of daily trading volume of cryptocurrencies

Important Risks Related to this Article

Important Information

Marketing communications issued in the European Economic Area ("EEA"): This document has been issued and approved by WisdomTree Ireland Limited, which is authorised and regulated by the Central Bank of Ireland.

Marketing communications issued in jurisdictions outside of the EEA: This document has been issued and approved by WisdomTree UK Limited, which is authorised and regulated by the United Kingdom Financial Conduct Authority.

WisdomTree Ireland Limited and WisdomTree UK Limited are each referred to as "WisdomTree" (as applicable). Our Conflicts of Interest Policy and Inventory are available on request.

For professional clients only. The information contained in this document is for your general information only and is neither an oer for sale nor a solicitation of an oer to buy securities or shares. This document should not be used as the basis for any investment decision. Investments may go up or down in value and you may lose some or all of the amount invested. Past performance is not necessarily a guide to future performance. Any decision to invest should be based on the information contained in the appropriate prospectus and aer seeking independent investment, tax and legal advice.

The application of regulations and tax laws can oen lead to a number of dierent interpretations. Any views or opinions expressed in this communication represent the views of WisdomTree and should not be construed as regulatory, tax or legal advice. WisdomTree makes no warranty or representation as to the accuracy of any of the views or opinions expressed in this communication. Any decision to invest should be based on the information contained in the appropriate prospectus and aer seeking independent investment, tax and legal advice.

This document is not, and under no circumstances is to be construed as, an advertisement or any other step in furtherance of a public oering of shares or securities in the United States or any province or territory thereof. Neither this document nor any copy hereof should be taken, transmitted or distributed (directly or indirectly) into the United States.

Although WisdomTree endeavours to ensure the accuracy of the content in this document, WisdomTree does not warrant or guarantee its accuracy or correctness. Where WisdomTree has expressed its own opinions related to product or market activity, these views may change. Neither WisdomTree, nor any ailiate, nor any of their respective oicers, directors, partners, or employees accepts any liability whatsoever for any direct or consequential loss arising from any use of this document or its contents.