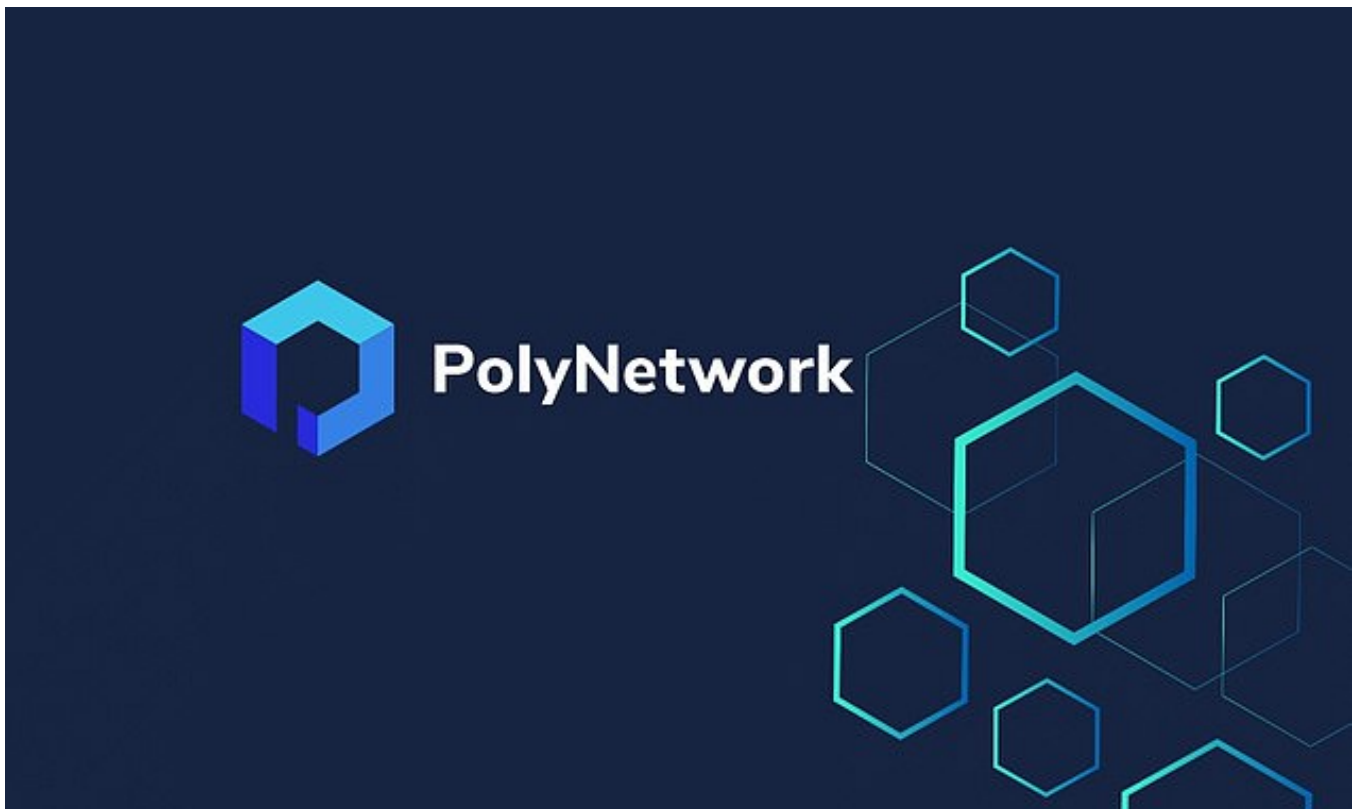


# Cryptographic platform PolyNetwork rewards hackers who stole \$ 610 million with a \$ 500,000 bug bounty

[isabellakhademhosseini](#) 08:49 EDT, August 13, 2021



**Cryptographic platform PolyNetwork thanks "ethical" hackers who steal \$ 610 million and reward him with a \$ 500,000 "bug bounty" after most of the money has been returned.**

- Almost all of the stolen \$ 610 million cryptocurrency has been returned to PolyNetwork
- Hackers argue that the breach is for "fun" and for pointing out vulnerabilities.

- **The company calls hackers "white hats", a jargon for ethical bug researchers.**
- **But a true white hat usually warns the company directly, rather than abusing the bug.**
- **The company thanked the hackers and offered a \$ 500,000 "bug bounty"**
- **Approximately \$ 268 million remains in accounts that require keys from both sides**

By Keith Griffith of Dailymail.com and Reuters

Release: 08:49 EDT, August 13, 2021 |

PolyNetwork, a cryptocurrency platform that lost \$ 610 million in hacking earlier this week, confirmed that it offered hackers a \$ 500,000 "bug bounty" on Friday.

In a statement, hackers (a sectoral terminology commonly referred to as "white hats" for ethical hackers aimed at exposing cyber vulnerabilities) were funded to "help improve the security of polynetworks." Thank you after returning most of the. ..

The network also said it wanted 'Mr. White Hat' will contribute to the continued development of the blockchain sector by accepting the \$ 500,000 reward provided as part of negotiations on the return of digital coins.

The statement did not specify the format in which it would pay \$ 500,000. The hacker said he had accepted the offer, but did not say whether it was accepted.

PolyNetwork, a cryptocurrency platform that lost \$ 610 million in hacking earlier this week, confirmed that it offered hackers a \$ 500,000 "bug bounty" on Friday.

TX

0x98b6316d3004be81c5d1b06c27472bef8097c9c922345876cd36111495ccf32a DECRYPTED: 'We appreciate you sharing your experience and believe your action constitutes white hat behavior. But we can't touch user assets and Poly Network doesn't have its own token. Since , we believe your action is white hat behavior, we plan to offer you a \$500,000 bug bounty after you complete the refund fully. Also we assure you that you will not be accountable for this incident. We hope that you can return all tokens as soon as possible. You can reserve the equivalent value of 500,000 USD in any assets to the current owner address. We will make up this part of the assets to Poly Network users. Your contribution is very helpful to us. Again, we think this behavior is white hat behavior, therefor this 500,000 USD will be seen as completely legal bounty reward. We will also ensure that you will not be held accountable for this incident, and we will publicly express our gratitude to you.'

© Twitter/ Tom Robinson

TX

0x05f90618be1e7f64230618476912dcccb0091f6eb011dd983f4ac7239e846d422 DECRYPTED: 'We've had a fix. It had been cross-checked internally and reviewed by a well known security audit team. The multi-sig address we provided is safe, please send the remainings to that address. We will send you the 500k bounty when the remainings are returned except the frozen USDT.'

© Twitter/ Tom Robinson

Polynetwork communicated with hackers and provided a \$ 500,000 "bug bounty" in messages shared by hackers embedded in digital transactions.

Almost all of the stolen ciphers have been returned, but now about \$ 268 million is in joint custody accounts that can only be accessed with keys from both hackers and polynetworks.

In a message embedded in the digital currency transaction, the hacker said, "When everyone is ready, we will provide the final key."

On Thursday, the hacker appeared to be speaking a digital message embedded in a transaction and was shared on Twitter by Tom Robinson, chief scientist and co-founder of crypto tracking company Elliptic.

They showed that the person who claimed to have carried out the hack stated that Polynetwork had provided him with a bounty to return the stolen property.

Hackers claimed to have committed the breach "for fun" and "to save the world," and were always planning to return the money.

THE POLY DID OFFERED A BOUNTY, BUT I HAVE NEVER RESPONDED TO THEM. INSTEAD, I WILL SEND ALL OF THEIR MONEY BACK.

© Twitter/ Tom Robinson

The hacker suggested he didn't ask for a prize and instead return the stolen money



**Tom Robinson**

@tomrobin



The \$600 million Poly Network hacker has published part one of a "Q&A":

[#polynetworkhack](#)

Q & A, PART ONE:

Q: WHY HACKING?

A: FOR FUN :)

Q: WHY POLY NETWORK?

A: CROSS CHAIN HACKING IS HOT

Q: WHY TRANSFERING TOKENS?

A: TO KEEP IT SAFE.

WHEN SPOTTING THE BUG, I HAD A MIXED FEELING. ASK YOURSELF WHAT TO DO HAD YOU FACING SO MUCH FORTUNE. ASKING THE PROJECT TEAM POLITELY SO THAT THEY CAN FIX IT? ANYONE COULD BE THE TRAITOR GIVEN ONE BILLION! I CAN TRUST NOBODY! THE ONLY SOLUTION I CAN COME UP WITH IS SAVING IT IN A \_TRUSTED\_ ACCOUNT WHILE KEEPING MYSELF \_ANONYMOUS\_ AND \_SAFE\_.

NOW EVERYONE SMELLS A SENSE OF CONSPIRACY. INSIDER? NOT ME, BUT WHO KNOWS? I TAKE THE RESPOSIBILITY TO EXPOSE THE VULNERABILITY BEFORE ANY INSIDERS HIDING AND EXPLOITING IT!

Q: WHY SO SOPHISTICATED?

A: THE POLY NETWORK IS DECENT SYSTEM. IT'S ONE OF THE MOST CHALLENGING ATTACKS THAT A HACKER CAN ENJOY. AND I HAD TO BE QUICK TO BEAT ANY INSIDERS OR HACKERS, I TOOK IT AS A BONUS CHALL :)

Q: ARE YOU EXPOSED?

A: NO. NEVER. I UNDERSTOOD THE RISK OF EXPOSING MYSELF EVEN IF I DON'T DO EVIL. SO I USED TEMPORARY EMAIL, IP OR \_SO CALLED\_ FINGERPRINT, WHICH WERE UNTRACABLE. I PREFER TO STAY IN THE DARK AND SAVE THE WORLD.

12:02 PM · Aug 11, 2021 · Twitter Web App

© Twitter/ Tom Robinson

On Thursday, hackers appeared to be speaking digital messages embedded in transactions, shared by industry expert Tom Robinson on Twitter.

White hat hackers typically notify companies directly when they discover a vulnerability, rather than using it to steal huge sums of money.

However, hackers who appear to be completely fluent in English explain that company insiders are afraid to exploit the vulnerability for themselves, and their funds are stolen and kept "safe." Claimed to be leaning.

A lesser-known name in the crypto world, PolyNetwork is a decentralized finance (DeFi) platform that facilitates peer-to-peer transactions with a focus on allowing users to transfer or exchange tokens between different blockchains. is.

According to blockchain forensics company Chainalysis, an unidentified hacker or hacker has exploited a digital contract vulnerability that PolyNetwork uses to move assets between different blockchains.

According to a statement on Friday, hackers returned \$ 340 million worth of assets and transferred most of the rest to a digital wallet jointly managed by them and PolyNetwork.



Currently, about \$ 268 million worth of stolen cryptography is stored in joint custody accounts that can only be accessed with keys from both hackers and polynetworks.

The rest held in tether was frozen by the cryptocurrency company behind stablecoin.

“After contacting Mr. Whitehat, I was able to better understand how the situation evolved and Mr. Whitehat’s original intentions,” Polynetwork did not elaborate. Said to.

Polynetwork announced the hack on Tuesday, but said the next day the hackers began returning the digital coins they had taken.

Hackers said in a digital message shared by Elliptic that they carried out an attack for fun and plan to always return tokens.

Some blockchain analysts speculate, but you may find it too difficult to launder stolen cryptocurrencies on such a scale.

advertisement

## Share or comment on this article:

Cryptographic platform PolyNetwork rewards hackers who stole \$ 610 million with a \$ 500,000 bug bounty

[Source link](#) Cryptographic platform PolyNetwork rewards hackers who stole \$ 610 million with a \$ 500,000 bug bounty