CTPRO.IO

TORNADO CASH

What is Tornado Cash?

Tornado Cash is the largest crypto mixer operating on the Ethereum blockchain. Mixers offer users anonymity when transferring cryptocurrency. They also create an indirect link between the accounts sent and received.

Tornado Cash works by using “pools” where users can deposit their tokens. A pool is like a shared bank account managed by a smart contract, ensuring users can’t withdraw more than they put in. Each pool only accepts specific tokens in set amounts. For example, one pool might only take 1 ETH deposits, while another takes 100 ETH. This makes it hard to trace which user is withdrawing their ETH.

Tornado Cash supports various cryptocurrencies and operates on multiple networks, but most transactions are in ETH on the Ethereum Blockchain.

The system uses immutable smart contracts, meaning the code can’t be changed or taken over, even by the creators. However, some functions, like routing and TORN token management, can be adjusted through governance.

Why do People use Tornado Cash?

Tornado Cash provides anonymity on Ethereum, allowing users to hide their transactions. Developers often use it to deploy new token contracts from clean addresses, but hackers and exploiters also use it to hide their activities.

Four of the top five crypto hacks involved Tornado Cash: the Ronin Network Exploit ($624M), Polynetwork Exploit ($611M), Wormhole Exploit ($326M), and Euler Exploit ($197M). Tornado Cash is also used by project insiders to fund clean wallets anonymously.

In 2021, some protocols planned airdrops or positive announcements, leading individuals to use Tornado Cash to transfer ETH and buy project tokens or sybil-attack airdrops on new wallets. Sharp-eyed traders noticed patterns, such as the Ampleforth FORTH token airdrop, which was heavily sybil attacked by one entity, receiving over $28M in tokens across more than 8,000 addresses.

Hackers and Tornado Cash

Hackers will typically use a mixing service such as Tornado Cash to legitimize their funds and remove any direct connections to any hacked wallets or malicious activity used with cryptocurrency.

Along with breaking the link between deposits and withdrawals, Tornado Cash also pulls all deposited funds into a shared pool. This could mean when a user is withdrawing stolen funds from Tornado Cash that Tornado Cash would inadvertently be helping the hacker remain undetected.

Torn Token

The TORN Token is the governance token for the Tornado Cash Protocol. TORN holders can vote on proposals through the on-chain governance smart contract. There are 10 million TORN tokens on Ethereum, distributed as follows since December 18, 2020.

- Airdrop: 5%
- Anonymity Mining: 10%
- Team: 30%
- DAO Treasury: 55%

Governance is used to control certain functions in Tornado’s contracts that require majority approval of TORN tokens. Users can create proposals by locking at least 1,000 TORN. A proposal needs at least 25,000 TORN to vote before it can pass with a majority.

Through governance, TORN holders can add new Tornado Cash Pools, emergency pause the entire TORN contract, change the TORN reward rate, and change routing addresses for the Tornado Cash Router.

Torn Takeover

On May 20, 2023, a hacker manipulated Tornado Cash's Governance Contract to give themselves 1,200,000 fake votes, gaining full control over the protocol. At that time, there were only about 700,000 legitimate votes, so no one could outvote them. With this control, the hacker could redirect withdrawals and deposits, pause all TORN token transfers, and drain all TORN tokens in the Governance Contract.

The hacker drained around $750,000 worth of TORN and sold it for ETH. Soon after, they proposed to undo their changes, which the community approved. The incident was resolved in under two days, with the hacker's voting balance reset to zero. The hacker kept 472 ETH from the exploit and sent it back into Tornado Cash.

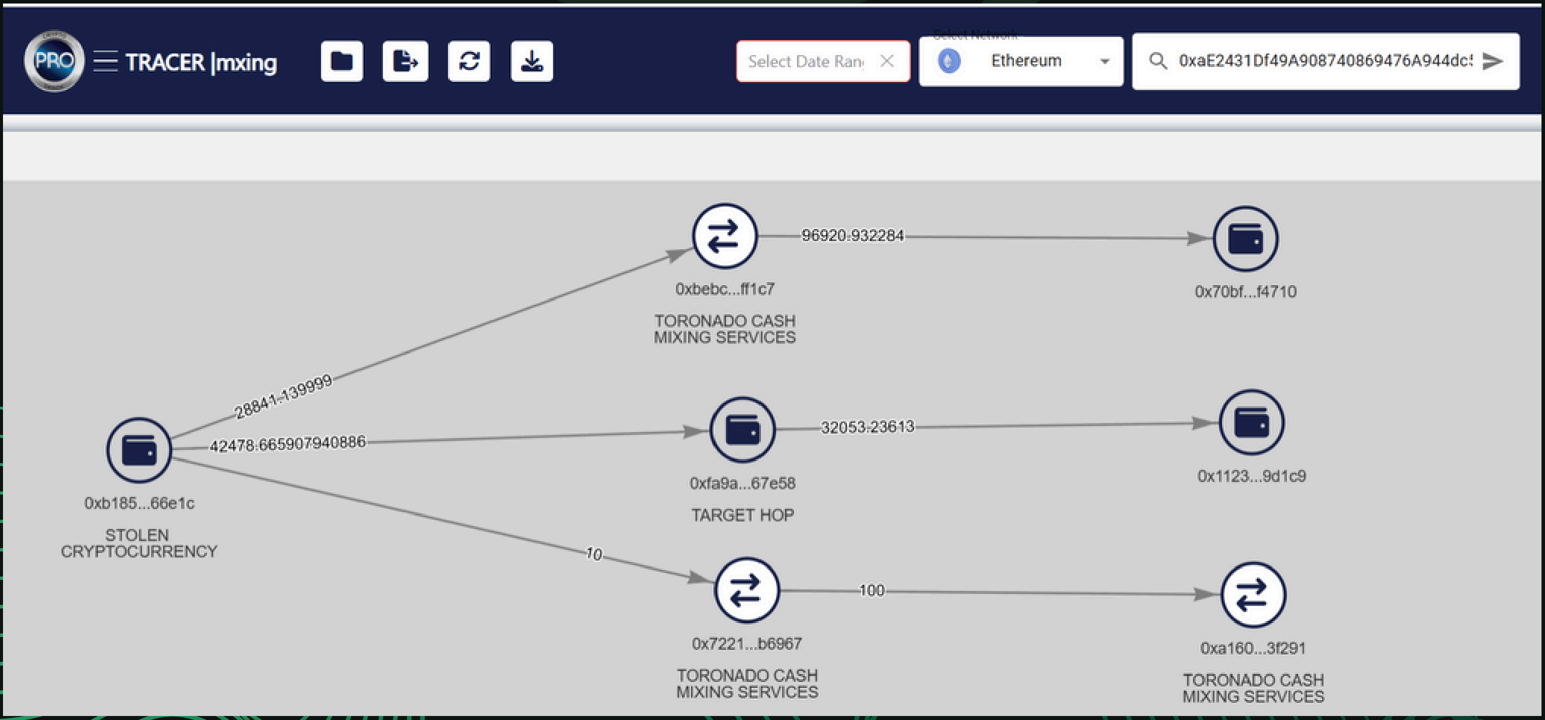
U.S. Treasury Sanctions Tornado Cash

On August 8, 2022, the U.S. Department of Treasury's Office of Foreign Assets Control (OFAC) imposed sanctions on the virtual currency mixer Tornado Cash. Since its inception in 2019, Tornado Cash has been utilized to launder over $7 billion in virtual currency.

However, on November 26, 2024, a U.S. appeals court determined that the U.S. Treasury Department exceeded its authority when it sanctioned the cryptocurrency mixer Tornado Cash in 2022, alleging it had facilitated the laundering of over $7 billion for North Korean hackers and other malicious cyber actors.

U.S. Circuit Judge Don Willett said federal law only gave OFAC the authority to regulate property, which Tornado Cash's immutable crypto-mixing smart contracts did not constitute.

Below is how CT Pro identifies and tracks any stolen cryptocurrency with our Tracer feature. Each node represents an address the funds are hopping to and the nodes with arrows represent Tornado Cash mixing service. Sign up here for a free 14-day trial with CT Pro: **https://analytics.ctpro.io/**



Select Network: Ethereum

0xaE2431Df49A908740869476A944dc!