The recent sanctions against Tornado Cash and subsequent debate around censorship, money laundering and slashing have raised several important issues for the Ethereum community to address.

I am proposing a simple, common sense, solution to one small part of the problem: A proactive way for Ethereum users to protect themselves from unwarranted association with stolen funds or terrorism-linked accounts.

Background

On August 8, 2022 the US Treasury announced sanctions against Tornado Cash. The crypto mixer has been used to obfuscate the origins of more than $7 billion worth of crypto, to date. In 2022 alone, 74.6% of stolen funds on the Ethereum network (approx. 300,160 ETH) were laundered through Tornado Cash.

Following the announcement, a firestorm has swept the Ethereum ecosystem concerning how to balance a free, fair and open network with government compliance and good-faith attempts to isolate stolen or terrorist-linked funds.

While the broader debate around validator censorship and social slashing has consumed most of the attention, an obvious but dangerous weakness in blockchain payments has also appeared.

Attack Vector

An interesting consequence of how Ethereum, Bitcoin and other blockchain networks function is that transactions only need to be signed by the sender of funds.

No one anticipated a world where receiving money would lower the value of your wallet.

Since transactions do not require symmetric approval (receiver and sender), a simple attack on a public address is possible. A malicious account can pollute another address simply by sending funds which have been negatively flagged (stolen, mixed, linked to terrorism, etc). Several days after the government crackdown on Tornado Cash, just such an attack occurred.

A hacktivist sent 0.1 ETH to several major crypto exchanges (Binance, Kraken,Gate.io) and celebrity ETH accounts (Justin Sun, Jimmy Fallon, Dave Chappelle) in a “dusting attack”

Economic Terrorism

It’s not hard to imagine, as crypto becomes a central part of global finance and infrastructure, that more serious versions of this attack could be carried out by nation states or terrorist organizations.

It’s concerning to think that ISIS, Al Qaeda or a foreign adversary could freeze the assets of a target by unilaterally associating themselves with the target wallet. A widespread dusting attack would set off banking AML triggers, shutting down whole industries for weeks.

Even more concerning is that any good-faith attempt

to identify, regulate or isolate malicious accounts could itself be turned into a weapon of economic terrorism or a extortion.

Imagine an extortion scheme where hackers purchase a small amount (100 ETH) of North Korean or Hezbollah assets and hold it like a container of plutonium, threatening European businesses with a banking and asset freeze unless they are quietly paid a ransom.

We need a simple, proactive way for Ethereum users to protect themselves from malicious attacks and rehabilitate their address instantaneously.

Solution

Instead of the altering Ethereum’s single signature transaction system to a more complex and slower, receiver/sender agreement system, I propose that we adopt a convention to rehabilitate accounts that have received tainted funds.

When a user/business receives undesired funds or discovers, after the fact, that they took payment from a stolen account, they can clean their account in two steps:

1. Burn the tainted ETH by sending to a thenull address (0x00…000)
2. Attaching a memo with the TX hash/id of the assets being burned

The second step (memo) is important because the issue may not be discovered by the user/business until many transactions later. Also the source of funds (burn target) could be ambiguous if the wallet has high transaction volume.

Adoption

For this method of protecting user accounts to really work, it needs to be adopted by the Ethereum community, chain analysis providers and (eventually) by government criminal enforcement.

I am going to work over the coming weeks, with my partner Vivek Raman, to socialize this idea with the core members of the Ethereum community and several chain analysis companies (Elliptic, Chainalysis, SlowMist, etc). Eventually, if the concept is adopted, we will speak with OFAC, FinCEN, FBI as well.

To help address this attack vector, please share the proposal within the Ethereum community.

If you have suggestions, thoughts, criticisms, please contact me at@NickYoder86

Suggested enhancements:

1. Someone could create a user-friendly front end that links to EtherScan/memo
2. Create a dedicated burn address for this fix, instead of the null address. Any clever ENS suggestions?