# I. Problem

Platforms like Tornado Cash on Ethereum have ensured transactional anonymity. However, their lack of sanctions screening mechanisms inadvertently leaves room for financial malpractices such as money laundering.

# II. Solution

Typhoon is a trustless and programmable solution founded on zkSNARK technology, offering:

1. Anonymity

: It preserves the anonymity of transactions by obscuring the link between sender and recipient.

1. Sanctions Screening

: It includes an integral sanctions screening mechanism to deter transactions from flagged or “suspicious” addresses.

## Protocol Description

[

Typhoon Protocol

7470×3588 401 KB

](https://ethresear.ch/uploads/default/original/2X/1/18cd9037d5afd5508d98472719af31a2a73b6cc5.png)

Deposit

: The user construct a commitment from the user’s address and a secret random number and deposit token into the smart contract with the commitment.

Withdraw

: Within the secret random number, user can generate a proof to prove not in the blacklist and withdraw the token.

Any feedback is welcome! Here’s more info and repo