**Basic Intro about tornado-cash**

1. Uses smart contracts that accept token deposits from one address and enable their withdrawal from a different address

2. When a user puts funds into a pool (a.k.a. the deposit), a private note is generated. This private note works as a private key for the user to access those funds later

**Backbone of tornado-cash:**

**Zero-Knowledge Proof:**

<https://research.aimultiple.com/zero-knowledge-proofs/>

<https://www.geeksforgeeks.org/zero-knowledge-proof/>

<https://hackernoon.com/eli5-zero-knowledge-proof-78a276db9eff>

**Video Tutorial on Zero-Knowledge Proof:**

<https://www.youtube.com/watch?v=OcmvMs4AMbM>

# **Some useful articles about tornado-cash:**

# Tornado Cash Is Crypto Hackers’ Favorite Way to Cash Out, But Experts Say It Can Be Traced

**Link:** <https://www.vice.com/amp/en/article/k7bqb9/tornado-cash-is-crypto-hackers-favorite-way-to-cash-out-but-experts-say-it-can-be-traced>

# Tornado Cash says it's using Chainalysis oracles to block access from OFAC sanctioned addresses(This was the step taken by tornado-cash after north korean cyber crime took place)

**Link:**

<https://cointelegraph.com/news/tornado-cash-says-it-s-using-chainalysis-oracles-to-block-access-from-opac-sanctioned-addresses>

<https://decrypt.co/97984/ethereum-privacy-tool-tornado-cash-uses-chainalysis-block-sanctioned-wallets>

Analyzing Tornado Cash Transactions

<https://medium.com/coinmonks/analyzing-tornado-cash-transactions-3d8d6b9731fb>

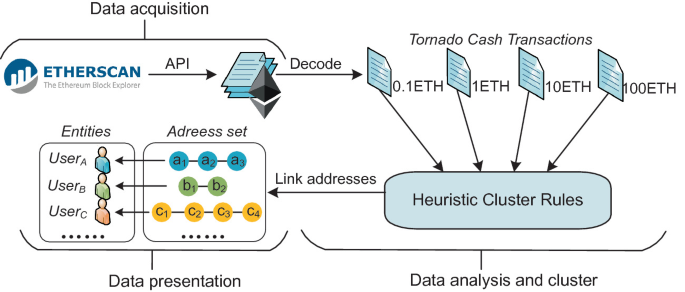
“Crypto Mixer Tornado Cash Says Sanctions Can't Apply To Smart Contracts”

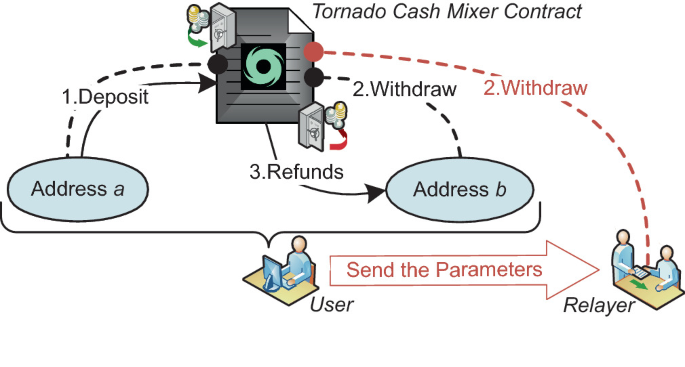
**Link:** <https://www.bloomberg.com/news/articles/2022-03-10/crypto-obfuscator-tornado-says-sanctions-cant-affect-smart-contracts>

Tornado Cash Spins Up Sanctions-compliant Web Interface

**Link:** <https://blockworks.co/tornado-cash-spins-up-sanctions-compliant-web-interface/>

Analysis of Address Linkability in Tornado Cash on Ethereum

**Fig: Analysis of Tornado-Cash(address linkability)**



**Fig: Mixer Contract of tornado-cash**

**Link:** <https://link.springer.com/chapter/10.1007/978-981-16-9229-1_3>