Deep Dive Into Tornado Cash

Date: 01/30/25

The recent decision by the U.S. Court of Appeals for the Fifth Circuit in *Van Loon, et al.* v. *Dep't of the Treasury*, 122 F.4th 549 (2024) held that the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) exceeded its statutory authority by sanctioning the suite of smart contracts (*i.e.*, computer code) comprising Tornado Cash—a decentralized, open-source privacy protocol that facilitates anonymous cryptocurrency transactions—because such smart contracts are not "property" subject to the sanctions jurisdiction asserted by OFAC within the meaning of the International Emergency Economic Powers Act (IEEPA). A central argument in the decision was the perceived "immutability" of the Tornado Cash smart contracts, with the court emphasizing that "once a smart contract becomes immutable, no one can reclaim control over it." However, a closer technical examination reveals that the notion of immutability is much more nuanced.

This article aims to provide a detailed technical overview of Tornado Cash and dissect the nuances of its smart contract architecture to demonstrate the importance of a technical understanding to avoid future pitfalls.

Crypto Under the Hood, a new regular newsletter series, covers hot topics in web3 with clear insights and sufficient technical details to keep you ahead of the curve in the complex world brought by blockchain technology.