Tornado Cash, OFAC and a Whirlwind of Confusion

Tl;dr:

The series of updates and clarifications from the Office of Foreign Assets Control (OFAC) on *Tornado Cash* illustrate the challenges of shoehorning new and novel technologies into existing regulatory frameworks in ways that were not envisioned by Congress. On November 8, 2022, OFAC delisted and simultaneously redesignated decentralized virtual currency privacy protocol Tornado Cash to its sanctions list – this time sanctioning Tornado Cash under its authority to designate malicious cyber activities and for supporting the Government of North Korea. The announcement also is the second time OFAC has publicly clarified the scope of its sanctions against Tornado Cash. It previously issued one set of frequently asked questions (FAQs) in response to concerns regarding the unprecedented sanctions. It has now issued a second set, which includes corrections to its initial FAQs. The announcement also comes after several lawsuits were filed challenging OFAC's authority to sanction the decentralized privacy protocol (including one supported and funded by Coinbase).

Part 1

Why are privacy tools needed for crypto?

Crypto transactions are made between *wallet addresses*, which are unique strings of numbers and letters. This makes the parties to transactions pseudonymous – identifiable, but not in a way that necessarily reveals their true identity. If you know that a particular address belongs to a specific individual, however, you can see their balance and transaction history due to the public nature of a blockchain. While this level of transparency is important for the general auditability of blockchains, it can pose privacy challenges. Crypto privacy protocols and tools have thus become an essential part of the ecosystem. In fact, some believe wider adoption of web3 technologies hinges on the ability of blockchains to support private transactions. If individuals using web3 technologies, or exchanging cryptocurrency, are forced to expose their sensitive financial information, including their salaries or sensitive purchases, people will be reluctant to use these technologies.

To make crypto transactions private, one generally needs to use mixers, privacy protocols or privacy coins. These tools and technologies seek to break the on-chain link between crypto transactions so it is harder to attribute those payments to a particular individual. Some are custodial platforms that commingle funds off-chain to mask ownership of assets. Others offer non-custodial, software-based solutions that leverage cryptographic tools like *smart contracts* and *zero-knowledge proofs*. There are also entirely distinct blockchains that are designed to support private transactions by default.

Some custodial platforms mix assets as a *service*. These platforms, also referred to as centralized mixers, take control of customer funds, mix them with other deposits, and then allow users to withdraw in exchange for a fee. The commingling process obfuscates transaction history to other users, but the operators of a centralized mixer are still able to see the transaction amount, sending address and receiving address. *Blender.io*, which was sanctioned by OFAC this past May, is an example of a custodial mixer.

Rather than using a mixing service that requires surrendering and commingling funds, smart contract-based privacy tools include using zero-knowledge proofs (ZKPs) to preserve privacy. ZKPs enable large amounts of data to be verified quickly using little information.

Smart contracts are software stored on a blockchain that executes automatically upon certain conditions. When combined with ZKPs, smart contract-based privacy protocols do not require users to relinquish control of their assets to a third party.

Tornado Cash is an example of a decentralized, noncustodial privacy protocol. Tornado Cash users deposit their assets into an on-chain smart contract pool, and receive a unique "hash" or key. The user is then able to withdraw those same assets at any time provided they have knowledge of the corresponding key, which is verified using a ZKP. This lets users deposit with one wallet address and then withdraw to another, without an on-chain link between transactions. Since Tornado Cash uses smart contracts and ZKPs to obfuscate ownership (instead of a third party that mixes funds together), at no point does the user have to relinquish custody of their asset, which also provides additional security to users.

Some have compared Tornado Cash pools to a safety deposit box room, where the deposited assets are the individual lockboxes.
The depositor can only access the lockbox belonging to them with the provided key.

By using Tornado Cash pools – smart contracts that individuals can simultaneously use to deposit assets and withdraw them to another address – outsiders are unable to simply "follow the money" to connect the depositing and withdrawing addresses. Because multiple users can interact with these pools at the same time, the blockchain will show multiple input addresses and multiple output addresses, which will be more difficult to identify the owner of particular assets withdrawn from these smart contracts. Provided the transaction pools have sufficient liquidity of incoming and outgoing transactions, the use of a decentralized privacy protocol like Tornado Cash can preserve privacy. But if there isn't a sufficient volume of incoming and outgoing transactions, then it may be possible to match the deposit and withdrawal transactions and identify the link between wallet addresses.

Part 2 Comparing Crypto Privacy Tools

Mixers	Privacy Protocols	Privacy Coins
Centralized	Decentralized	Decentralized
Platform or service	Smart contract	Cryptocurrency
Custodial Third-party intermediary accepts deposits, commingles with other funds to obfuscate ownership and allows users to withdraw assets from another address less a fee. Transaction information is not public but is available to the operator of the platform or service.	Non-custodial Smart contract uses zero-knowledge proof to enable a depositor to withdraw their deposited assets from a different address. Deposit and withdrawal transactions are pooled in smart contracts but depositors are only able to withdraw their specific assets (i.e. no "mixing" of funds)	Non-custodial Cryptocurrency that masks sending/receiving address and transaction amount. Pools addresses and/or uses zero-knowledge proofs to verify transactions.
Blender.io, Helix	Tornado Cash	Zcash

Many of these privacy tools have come under increasing scrutiny by regulators concerned they may be used to launder illicit or stolen funds. However, there are many legitimate uses for privacy protocols in crypto transactions. For example, these tools are valuable for:

- A user with a large crypto balance who wants to maintain privacy in order to avoid becoming a target for kidnapping or physical harm;
- High net worth or noteworthy individuals who wish to maintain privacy or avoid causing market movements;
- Those who donate to a sensitive cause and wish to keep the donation private from others;
- Employees who are paid in crypto who don't want their employer to know their other transaction history;
- Developers who want to deploy software on a blockchain without revealing information about their personal finances.

Part 3 Tornado Cash Sanctions Timeline

Aug 8, 2022	OFAC sanctions Tornado Cash, stating that it "has been used to launder more than $7 billion worth of virtual currency since its creation in 2019." Shortly after the announcement from OFAC, *GitHub*, a software code hosting platform, removed the Tornado Cash source code from its site and suspended the accounts of its developers.
Sept 8, 2022	First lawsuit challenging the sanctions was brought on behalf of six harmed individuals, funded by Coinbase.
Sept 13, 2022	OFAC posted an FAQ stating that: a. Individuals who had deposited funds prior to the sanctions announcement can only withdraw those funds by applying for and receiving a special license to withdraw funds; b. While "dusting" is a violation of the sanctions, OFAC will not "prioritize enforcement" against individuals who were delayed in reporting these involuntary received funds to OFAC; and c. US persons are prohibited from transacting with Tornado Cash but clarifying that merely publishing or making available the open-source code for others to view was not prohibited.
Sept 22, 2022	GitHub reportedly reinstates the previously suspended accounts as "read-only."
Oct 12, 2022	CoinCenter, a DC-based think tank, announces lawsuit challenging the sanctions.
Nov 8, 2022	OFAC delists Tornado Cash from the SDN list and simultaneously redesignates it under the sanctions programs related to cyber activities and those targeting the Government of North Korea. In doing so, OFAC provides additional compliance guidance regarding the nature of the Tornado Cash entity, and corrects three existing FAQs.

Part 4 Why are the Tornado Cash sanctions controversial?

Reducing the risk of illicit finance and maintaining national security are critical public policy goals that few would object to. What sparked outcry with Tornado Cash is the fact that OFAC did not include wallet addresses belonging to individuals and entities, but listed smart contracts that are not under the control of any person, group or entity. This is the first instance of OFAC using its *Specially Designated Nationals and Blocked Persons (SDN) List* to sanction software rather than a person or group.

The core smart contracts that comprise Tornado Cash are *non-upgradeable* – they are not capable of being changed or modified by anyone, even the initial developers who deployed it to the Ethereum blockchain. This effectively means that Tornado Cash can keep running in perpetuity (and still continues to be used today) so long as Ethereum is running. OFAC's sanction of these addresses thus results in the sanctioning of software itself.

Financial privacy is a core pillar of economic freedom. While digital forms of payment offer consumers incredible convenience, they are also susceptible to surveillance, censorship and hacking of personal information. Many believe cryptocurrency, when paired with the right privacy protocols, will allow us to build a more free and open financial system that doesn't sacrifice privacy.

As interest in web3 continues to grow, it is imperative that regulators, policymakers and law enforcement take a measured approach that protects the public without inadvertently criminalizing or chilling the development of privacy-enhancing tools. Lawmakers could more effectively prevent illegal activity by targeting the bad actors who commit those crimes or seizing the funds controlled by those actors. They should not take the unprecedented step of sanctioning open-source technology or privacy protocols like Tornado Cash.