New York Law Journal
Corporate Update
WWW.NYLJ.COM
ALM.
VOLUME 268—NO. 63
THURSDAY, SEPTEMBER 29, 2022

FINANCE

Sanctioning Code: What's Next for Crypto Sanctions?

By **Jeffrey Alberts**

Recent government sanctions against blockchain programs have highlighted the power held by the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) and the vulnerability of the blockchain ecosystem to an abuse of that power. OFAC is now facing a lawsuit funded by the largest blockchain exchange in the United States relating to sanctions on a blockchain protocol known as "Tornado Cash." The future of blockchain technology could depend on the outcome of that lawsuit and on how OFAC's decides to exercise its power to impose sanctions on blockchain programs and assets.

OFAC Sanctions Tornado Cash

On Aug. 8, 2022, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) announced that it had sanctioned a virtual currency mixer known as Tornado Cash. OFAC also sanctioned the website tornado.cash, along with dozens of addresses on the Ethereum blockchain that it described as "associated virtual currency addresses."

As a justification for these sanctions, the Treasury Department asserted that Tornado Cash had been used to launder more than $7 billion worth of virtual currency since its creation in 2019. This included over $455 million stolen by the Lazarus Group, a Democratic People's Republic of Korea (DPRK) state-sponsored hacking group; $96 million of malicious cyber actors' funds derived from the June 24, 2022 Harmony Bridge Heist; and at least $7.8 million from the Aug. 2, 2022 Nomad Heist.

The language used in OFAC's press release announcing this sanction was familiar to anyone who has reviewed previous OFAC sanctions of persons and entities that OFAC believes to be engaging in activities that threaten the national security, foreign policy, or economy of the United States. The press release quoted an Under Secretary of the Treasury stating that Tornado Cash "has repeatedly failed to impose effective controls designed to stop it from laundering funds," "[d]espite public assurances otherwise." It warned that "[v]irtual currency mixers that assist criminals are a threat to U.S. national security." Anyone reading the press release would think that Tornado Cash was an entity that had willfully laundered criminal proceeds using a mixer that it controlled.

OFAC Sanctioned Code

For members of the global community of people who actually use Tornado Cash, the Treasury Department's language was misleading, if not false. By referring to Tornado Cash as an "entity," suggesting that mixers "assist" criminals, and

JEFFREY ALBERTS *is a partner at Pryor Cashman, where he works in the white-collar defense and investigations group, the financial institutions group, and the fintech group.*

referencing "public assurances" about how Tornado Cash would "impose" controls, the Treasury Department suggested that Tornado Cash is a traditional entity, like a partnership or a cartel. Many users of Tornado Cash, however, understand Tornado Cash to consist only of open-source software code that had been developed by a large group of independent contributors. These contributors are not understood to be members of an entity known as "Tornado Cash." Rather, they independently contributed code to this open-source project because they were interested in creating an automated protocol that could be used by anyone to protect privacy on the Ethereum blockchain.

The code contributed to this open-source project was used to create several smart contracts when the code was deployed on the Ethereum blockchain. Smart contracts are programs stored on a blockchain that run automatically when specified conditions are met. Anyone can use the Tornado Cash smart contracts to transfer digital assets from one Ethereum blockchain address to a smart contract and then withdraw the digital assets to a new Ethereum blockchain address. The Tornado Cash smart contracts operate automatically on the blockchain, without oversight or control from any person or group. They are immutable. Most of the Ethereum blockchain addresses sanctioned by OFAC are addresses of these smart contracts.

It is important to users of these Tornado Cash smart contracts that there is no entity that has the ability to impose controls over these smart contracts. This protects the security of their assets, because no entity can exercise control over them. It also protects the users' privacy, because no supervising entity knows their identity.

The future of blockchain technology could depend on the outcome of that lawsuit and on how OFAC's decides to exercise its power to impose sanctions on blockchain programs and assets.

Coders Fight Back

On Sept. 8, 2022, six users of Tornado Cash sued the Department of the Treasury, as well as OFAC, the Secretary of the Treasury, and the Director of OFAC. This case, *Van Loon v. Treasury*, was filed in a U.S. District Court in the Western District of Texas. In their complaint, the plaintiffs alleged that the Treasury Department lacked authority to sanction Tornado Cash and that the sanction violated the First Amendment and the Fifth Amendment to the U.S. Constitution.

These coders explained that they were using Tornado Cash for lawful purposes, like many other Tornado Cash users. These lawful purposes included concealing their ownership of valuable digital assets from malicious hackers who otherwise could attempt to steal the digital assets, making anonymous contributions to the Ukrainian government without attracting attacks from Russian state-sponsored hacking groups, and concealing the ownership of valuable digital assets to reduce the risk of attacks on the owner or the owner's family by criminals seeking to extort the owner of the assets.

This lawsuit has received very public support from many participants in the community of blockchain users. Most notably, Coinbase, the largest cryptocurrency exchange in the United States, announced that it was funding *Van Loon v. Treasury*. Coinbase CEO Brian Armstrong explained in a blog post that, "while we share Treasury's commitment to fighting crime, we believe this action harms innocent people and threatens the future of decentralized finance (DeFi) and web3 specifically."

OFAC Answers (Some) Questions

The week after the *Van Loon* action was filed, the Treasury Department published on its website responses to several Frequently Asked Questions about the sanction imposed

on Tornado Cash. These FAQs stated that people whose digital assets were sent to a Tornado Cash smart contract before the imposition of sanctions cannot withdraw their assets from the smart contract unless they obtain a specific license from OFAC to engage in these withdrawal transactions.

With respect to the code itself, OFAC essentially dodged the frequently asked question of whether it was legal to copy the open source code used in the Tornado Cash smart contracts and deploy this same code in identical or slightly altered form in new smart contracts on the Ethereum blockchain. Rather than answer this question, OFAC stated that "interacting with open-source code itself, in a way that does not involve a prohibited transaction with Tornado Cash, is not prohibited." This circular response is unlikely to answer anyone's questions. OFAC did, however, give a couple examples of permitted interactions with the open-source code, such as "making it available online for others to view, as well as discussing, teaching about, or including open-source code in written publications, such as textbooks." OFAC stopped short of explaining whether the code could be used in the most common way code is used—to create programs that are used by others.

Probably most notably, OFAC did not answer the frequently asked question of what exactly it had sanctioned. Did it think it had sanctioned a group of people that it is calling "Tornado Cash" who participated in the creation of the relevant smart contracts? Or perhaps a group of people who deployed the smart contracts? Or was it sanctioning only the protocol that operated by means of the deployed smart contracts? Does OFAC believe that this sanction would apply if the same smart contracts were redeployed to a new blockchain address by a person who was not sanctioned? Nobody knows, and OFAC isn't saying.

OFAC appears to believe that it has legal authority not only to sanction entities, but to sanction technological instrumentalities that are used by these entities, such as smart contracts and computer programs.

The Future of Crypto Sanctions

OFAC appears to believe that it has legal authority not only to sanction entities, but to sanction technological instrumentalities that are used by these entities, such as smart contracts and computer programs. If this is OFAC's position, which we may soon learn in the *Van Loon* case, then it is difficult to identify statutory limits on the scope of this power. If OFAC can sanction smart contracts and protocols making use of smart contracts by asserting that the programs were used by bad actors to threaten national security, could it sanction a blockchain token, or even the native asset of a blockchain, such as Bitcoin, and prohibit all transfers involving these digital assets? Could it sanction an entire blockchain protocol, by asserting that it had been used to threaten national security? For that matter, does OFAC think it could sanction widely used technological instrumentalities such as the internet itself? These all could be described as instrumentalities that have been used by criminals to engage in activity that threatens the national interest. Presumably, OFAC would draw the line somewhere, but we do not yet know if OFAC believes this to be a legal limit on its authority or an exercise of agency discretion in how it uses its legal authority. Hopefully, these questions will be answered soon. For now, the Treasury Department has introduced more unpredictability into the future of blockchain.