NORTON ROSE FULBRIGHT

Blockchain Law

Can there be law without people?

Robert A. Schwinger, *New York Law Journal* — January 24, 2023

In his Blockchain Law column, Robert Schwinger takes a deep dive into the issue of legal responsibility when dealing with "smart contracts." He concludes: "Smart contracts are not simply a feature of nature that one might encounter as one might a volcano or a raging river. Humans create them, and humans make choices about interacting with them."

Two seemingly unrelated recent developments in the world of blockchain are now posing the same odd question: Can there be law without people?

Blockchain technology has enabled a world of "smart contracts"—programs stored on the blockchain that automatically run and carry out predetermined tasks when predetermined conditions are met. These smart contracts are often integrated with so-called decentralized autonomous organization (DAOs), loose groups of tokenholders who effectuate decisionmaking through software protocols.

Can DAOs, natural persons or other legal entities be held legally responsible when outcomes that are caused or enabled by those "smart contracts" are ones that society seeks to prevent and hold unlawful? Or is no one legally responsible, so that whatever these "smart contracts" might do is simply beyond the power of the institution of the law to remedy or prevent?

The Tornado Cash Sanctions

Last summer, in an effort to block avenues for circumventing U.S. sanctions against North Korea, the Treasury Department's Office of Foreign Asset Control (OFAC) added to its sanctions list the virtual currency mixer Tornado Cash. Notice of OFAC Sanctions Action, 87 Fed. Reg. 49,652 (Aug. 11, 2022); see also U.S. Dep't Treasury, U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash (Aug. 8, 2022). This marked a continuation of the U.S. government's efforts to combat persons attempting to circumvent North Korean sanctions by using virtual currency. See, e.g., R. Schwinger, Cryptocurrency Offers No Escape from International Sanctions, N.Y.L.J., March 8, 2021.

According to OFAC's Aug. 8 press release, Tornado Cash "is a virtual currency mixer that…indiscriminately facilitates anonymous transactions by obfuscating their origin, destination, and counterparties, with no attempt to determine their origin," which allegedly "receives a variety of transactions

Robert A. Schwinger is a partner in the commercial litigation group at Norton Rose Fulbright US.

and mixes them together before transmitting them to their individual recipients," thus enabling "illicit actors to launder funds."

Asserting that Tornado Cash had been used to launder monies stolen in illicit activities, including by a North Korean state-sponsored hacking group that was itself targeted by U.S. sanctions, OFAC added to the sanctions list the website tornado.cash and 38 Ethereum addresses for various wallets associated with Tornado Cash. Thereafter, OFAC issued a set of FAQs in which it referred to Tornado Cash as an "entity" with which the listed wallet addresses were "associated" and stated that the intent of the designation was to prohibit U.S. persons from "engaging in any transaction with Tornado Cash or its blocked property or interests in property." U.S. Dep't Treasury, FAQ Nos. 1076-1079 (Sept. 13, 2022).

In November 2022, OFAC issued an updated sanctions designation for Tornado Cash. Notice of OFAC Sanctions Action, 87 Fed. Reg. 68,578 (Nov. 15, 2022); see also U.S. Dep't Treasury, Treasury Designates DPRK Weapons Representatives: Tornado Cash Redesignated with Additional DPRK Authorities, New OFAC Guidance (Nov. 8, 2022), along with an additional FAQ. U.S. Dep't Treasury, FAQ No. 1095 (Nov. 8, 2022).

Who or what can be the subject of sanctions?

Various Tornado Cash users filed lawsuits challenging the sanctions designations on several grounds. See *Joseph Van Loon v. Dep't of Treasury*, No. 6:22-cv-920-ADA-JCM (W.D. Tex. Waco Div.); Coin Center v. Yellen, No. 3:22-cv-20375-TKW-ZCB (N.D. Fla. Pensacola Div.). One of the grounds raised was to argue that "Tornado Cash" and its associated wallets were not in fact sanctionable under the statutes and executive orders pursuant to which OFAC had purported to act in issuing the Tornado Cash sanctions, because "Tornado Cash" was merely computer code rather than a person or entity and did not hold any interests in property.

These plaintiffs argued that the sanctions authority under the International Emergency Economic Powers Act (IEEPA) extends only to transactions involving "any property in which any foreign country or a national thereof has any interest…, or with respect to any property, subject to the jurisdiction of the United States." 50 U.S.C. §1702(a)(1)(B).

Similarly, under the United Nations Participation Act of 1945, sanctions authority is granted with respect to "economic relations…between any foreign country or any national thereof or any person therein and the United States or any person subject to the jurisdiction thereof, or involving any property subject to the jurisdiction of the United States." 22 U.S.C. §287c(a). Likewise, under the North Korea Sanctions and Policy Enhancement Act of 2016, the President may only designate "any person" engaged in certain enumerated conduct relating to North Korea. 22 U.S.C. §9214.

The plaintiffs also argued that under Executive Order 13,694, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," the Treasury Department is authorized only to identify certain "person[s]" involved in malicious cyber-enabled activities and to block "property and interests in property" that any of those identified persons "dealt in." 80 Fed. Reg. 18,077 (April 2, 2015).

Likewise Executive Order 13,722, "Blocking Property of the Government of North Korea and the Workers' Party of Korea, and Prohibiting Certain Transactions With Respect to North Korea," only authorizes sanctions against "any person" engaged in certain enumerated conduct relating to North Korea, and the blocking of "[a]ll property and interests in property" of those identified persons. 81 Fed. Reg. 14,943 (March 18, 2016).

The plaintiffs argued that "Tornado Cash" could not be the target of sanctions under these authorizations, such that the plaintiffs could be barred from using it. The *Van Loon* plaintiffs, for example, alleged that they themselves were not terrorists, criminals, money launderers or members or supporters of the North Korean government, but simply American citizens who used Tornado Cash for privacy purposes, to protect against the public availability of the information contained in blockchain transaction records. Tornado Cash, they alleged, was simply:

> a decentralized, open-source privacy protocol—not a person, entity, or organization. No person or group of people controls Tornado Cash. No person or group of people—not even the original developers of Tornado

> Cash—can remove or modify Tornado Cash. Anyone with an internet connection can develop code and add it to the Tornado Cash privacy tool. And anyone with an internet connection can use Tornado Cash.

(*Van Loon* Amd. Complt. ¶ 64.)

The *Van Loon* plaintiffs alleged that "Tornado Cash" was merely "smart contract" open-source software code that "was developed over many years by a large group of individual contributors" and "can be used or distributed by anyone." (Id. ¶ 4.) A "smart contract," they asserted, was merely "a program stored on the blockchain that runs when predetermined conditions are met," which has "a public address with which any user can interact. When an individual user interacts with a smart contract, the code automatically carries out a particular, predetermined task without any human intervention." (Id. ¶ 5.)

The *Van Loon* plaintiffs thus argued that the Tornado Cash sanctions were improper because "[t]he Tornado Cash smart contracts are not a foreign country or a national thereof, a person of any kind, or the property of any person or country. The Tornado Cash smart contracts are also not identifiers for any person, country, or property." (Id. ¶ 65.) They also asserted that Tornado Cash was not "operated under centralized control." (Id. ¶ 57.) In fact, they claimed that "[a]lthough OFAC has procedures by which a designated person can apply for delisting, no such application is possible here because open-source code is not owned by anyone." (Id. ¶ 58.)

Similarly, the *Coin Center* plaintiffs alleged that Tornado Cash was simply a "privacy tool" that was "beyond the control of anyone." (*Coin Center* Complt. ¶ 26.) They asserted that because in many instances this tool is used to protect Americans' "own property" and not that of North Korea or any other foreign country or national, it cannot legitimately be the subject of sanctions under the existing legal authority. (Id. ¶¶ 17-18.)

OFAC in its FAQs, however, took a very different position. U.S. Dep't Treasury, FAQ No. 1095 (Nov. 8, 2022). It asserted that "the entity known as Tornado Cash" was a "partnership, association, joint venture, corporation, group, subgroup, or other organization" subject to sanctions designation. It further asserted that Tornado Cash had an "organizational structure" consisting of: "(1) its founders and other associated developers, who together launched the Tornado Cash mixing service, developed new Tornado Cash mixing service features, created the Tornado Cash Decentralized Autonomous Organization (DAO), and actively promoted the platform's popularity in an attempt to increase its user base; and (2) the Tornado Cash DAO, which is responsible for voting on and implementing new features created by the developers."

OFAC further asserted that Tornado Cash's "smart contracts" were used "to implement its governance structure, provide mixing services, offer financial incentives for users, increase its user base, and facilitate the financial gain of its users and developers." OFAC noted that it had "not designated Tornado Cash's individual founders, developers, members of the DAO, or users, or other persons involved in supporting Tornado Cash" themselves as sanctions targets, at least "at this time."

There has not yet been any judicial determination regarding the legal questions about whether Tornado Cash, its website, its wallet addresses or the "smart contract" programs that its users can invoke fit within the existing statutory and executive order authorization for the imposition of sanctions. There also has not been any factual determination whether Tornado Cash on a functional level should be regarded as an entity as OFAC has asserted it should.

Even if there were determinations on these issues that might impact the government's ability to sanction Tornado Cash under existing authority, that ultimately may just be a temporary issue of drafting. Statutes and executive orders can always be revised and expanded to bar the use of software code, smart contracts and/or websites that could be used by malign actors for illicit purposes.

Indeed, on Dec. 14, 2022, Senator Elizabeth Warren (D.-Mass.) and Representative Roger Marshall (R.-Kan.) introduced their proposed Digital Asset Anti-Money Laundering Act of 2022 which seeks to do just that. Section 3(d) of the proposed bill would direct the Secretary of the Treasury to promulgate a rule prohibiting financial institutions from "handling, using, or transacting business with digital asset mixers, privacy coins, and other anonymity-enhancing technologies" or "with digital assets that have been anonymized by" such means. The proposed bill would go beyond addressing just persons and

entities by expressly defining the term "digital asset mixer" to mean "a website, software, or other service designed to conceal or obfuscate the origin, destination, and counterparties of digital asset transactions." Id. §2(3).

Suing the Ooki DAO

On Sept. 22, 2022, the Commodities Futures Trading Commission (CFTC) filed a complaint for injunctive relief and penalties concerning a blockchain-based software protocol that relied on smart contracts and tokens to effectuate commodities transactions that the CFTC alleged were "unlawful off-exchange leveraged and margined retail commodity transactions" and "activities that can only lawfully be performed by a registered Futures Commission Merchant." *CFTC v. Ooki DAO*, No. 3:22-cv-5416-WHO (N.D. Calif., S.F. Div.). The CFTC's complaint named as the defendant a DAO currently known as the "Ooki DAO." (For more on DAOs, see generally R. Schwinger, DAOs Enter the Spotlight, N.Y.L.J., March 21, 2022.)

The software protocol at issue in this case was known as the "bZx Protocol." It allegedly originally had been designed and deployed by an LLC called bZeroX, LLC, but in August 2021 that LLC allegedly "transferred control" of that protocol to a DAO then called "bZx DAO," which a few months later was renamed and rebranded as "Ooki DAO."

DAOs as defendants

The CFTC alleged that the defendant DAO was "an unincorporated association comprised of holders of [the protocol's tokens] who have voted those tokens to govern (e.g., to modify, operate, market, and take other actions with respect to)" the software protocol during the relevant period. It alleged that the Ooki DAO website described procedures for the DAO's members to propose and vote on Ooki DAO governance proposals so that, "[i]n short, the Ooki DAO is governed by the vote of holders of Ooki Tokens" and had operated similarly when it had used its prior name. It alleged that certain Ooki DAO members resided in the United States and "conducted Ooki DAO business (for example, voting Ooki Tokens to govern the Ooki DAO and operate the Ooki Protocol)" from within the United States.

But the CFTC's complaint also made a more stunning claim: It alleged that a "key…objective" of the LLC "in transferring control of the [protocol] to the [DAO] was to attempt to render the [DAO], by its decentralized nature, enforcement-proof. Put simply, the bZx Founders believed they had identified a way to violate the [Commodity Exchange] Act and Regulations, as well as other laws, without consequence."

In fact, the CFTC alleged that one of the founders had stated on a call that transitioning to a DAO was an effort to "prepar[e] for the new regulatory environment by ensuring bZx is future-proof" against "legal notices" and registration requirements, by "tak[ing] all the steps possible to make sure that when regulators ask us to comply, that we have nothing we can really do because we've given it all to the community."

Matters became further complicated when the CFTC, asserting that it was unable to identify an individual authorized to accept service of process on the Ooki DAO's behalf or a physical location to which a summons and complaint could be mailed, sought and obtained permission to make alternative service upon the Ooki DAO defendant through its online Help Chat Box and Online Forum, which the court agreed to permit.

The Ooki DAO itself filed no appearance or opposition in the CFTC's lawsuit. However, several industry players emerged making amicus filings strongly opposing and seeking reconsideration of the CFTC's attempt to serve a DAO as a defendant through alternative means without giving notice to any individual tokenholder.

One amicus brief argued that Ooki DAO could not be sued as an "unincorporated association" of its voting members because a DAO was not a "group of persons" but merely "a technological tool for social coordination through which people can make decisions."

It further argued that the DAO's members could not be said to be pursuing a "common objective" merely by voting on DAO matters. Another amicus argued in its brief that in order to be treated as an "unincorporated association" under California law, the group's alleged common objective must be a "lawful objective," and thus an entity cannot be served as an unincorporated association "where its only common purpose is the unlawful conduct that is the subject of the suit."

A third amicus argued in its brief against the "unincorporated association" approach by arguing that "DAOs are not ordinary business entities," as they "lack any central organization or management" and their token holders "often lack coordination or common objectives" As a result, this amicus argued, because a DAO does not qualify as an "association" it cannot qualify as a "person" against whom the CFTC can take statutory action.

A fourth amicus argued in its brief that DAOs were a "novel type of loose-knit, technologically mediated social structure." DAOs "associated with DeFi [decentralized finance] systems," it argued, were thus not like corporations "but rather are ad hoc social formations organized around providing infrastructure that help make possible" certain activities.

Several of the amici contended that naming the amorphous DAO as the defendant was an improper back-door attempt to expose individual tokenholders who had cast governance votes on Ooki DAO matters to liability, without ever naming or serving them individually as defendants. They argued that allowing theories like the CFTC's to proceed would have the effect of disincentivizing individuals from DAO participation, and that the CFTC's approach was so novel that it could only be sustained through statutory amendments and/or formal agency rulemaking.

The CFTC in its consolidated response to the amici disputed their characterization of the CFTC's complaint as suing and/or seeking recovery directly against individual Ooki tokenholders, and thus argued there was no need for the CFTC to serve each individual tokenholder. It argued that the Ooki DAO "meets the well-established definition of an unincorporated association" and "there is nothing novel about applying this definition to the Ooki DAO." Suing the DAO, said the CFTC, was "not suing technology" or taking action "against the blockchain-based Ooki Protocol" (i.e., the software); it was simply bringing suit against the Ooki DAO (i.e., the alleged organization that uses the software), as "an association that acts and makes collective decisions regarding the Ooki Protocol through voting by its governance token holders."

The CFTC also pushed back against the amici's concerns over potential liability of individual DAO members. It noted that DAOs can be wrapped in various kinds of "entity structures with a goal of enabling nascent DAOs to address potential individual-member liability issues," but that the DAO "cannot avoid liability" for unlawful activities "simply by placing the organizational and governance functions previously performed by an LLC in a DAO."

It further argued that "[t]o serve an unincorporated association, the CFTC need only serve the association itself; it need not serve all of the association's uncharged individual members," even though individual members could be held jointly and severally liable for the unincorporated association's debts, because the judgment the CFTC is seeking against the DAO would not be a judgment against any individual DAO member.

The CFTC concluded by charging the amici with "ultimately saying…that DAOs are nothing—or at least nothing that can be sued, or served, or held accountable for running a for-profit trading platform" that violates the law, and that "simply switching business forms from an LLC to a DAO makes an entity immune from suit and outside any government's enforcement reach." It urged the court to reject "that radical and dangerous proposition."

'*Someone* must be responsible'

On Dec. 20, 2022, the court did just that, issuing a ruling rejecting the amici's objections. *CFTC v. Ooki DAO*, 2022 WL 17822445 (N.D. Cal. Dec. 20, 2022). Noting that this "appears to be a case of first impression," it concluded that the CFTC had properly served the Ooki DAO as an unincorporated association.

The court first held that contrary to the amici's contention, the CFTC was "suing an entity, not a technology." It noted that control of the "Administrator Keys" for the Ooki Protocol had passed from the LLC that originally owned the protocol to the tokenholders who now governed the Ooki DAO. Accordingly, the CFTC "may now sue Ooki DAO as an entity for its use of Keys to control and govern the Protocol," even if as a "litigation strategy" the CFTC had chosen not to sue individual tokenholder members of the DAO themselves.

For the purposes of deciding whether the CFTC made valid service of process upon the Ooki DAO as an unincorporated association, the court held that it need not address the

substantive question of whether DAOs or unincorporated associations could be subject to liability under the CFTC's authorizing statutes and regulations. "The critical question for this motion is whether and how the DAO can be served, which requires answering if it has the capacity to be sued and if it was properly served in that capacity." Issues beyond that, said the court, were "merits" issues that "cannot and should not be analyzed" on a motion about the validity of service of process.

The court next held that Ooki DAO had the capacity to be sued under FRCP 17(b), because it met the qualifications for being an unincorporated association under California state law. Citing Cal. Corp. Code §18035(a), it held that such status requires only "an unincorporated group of two or more persons joined by mutual consent for common lawful purpose, whether organized for profit or not," where such persons "function under a common name under circumstances where fairness requires the group be recognized as a legal entity. Fairness includes those situations where persons dealing with the association contend their legal rights have been violated."

The court concluded that Ooki DAO was being sued as a group of two or more people, namely tokenholders, and not as a "technological tool." While the tokenholder members may have joined the DAO at different times and had inconsistent views on particular issues upon which they voted, that did not obviate the fact that they still "have a common objective: making choices to govern the DAO." Nor was the DAO's objective unlawful, despite the CFTC's allegations. The court explained:

> "[I]t is not inherently unlawful to operate retail commodity exchanges; doing so merely requires following federal regulations. . . . Providing this technology—and governing its use—is not inherently unlawful, even if the CFTC asserts that Ooki DAO did not comply with all applicable laws when doing so."

Moreover—and perhaps more fundamentally—the court stated that "fairness requires recognizing the DAO as a legal entity because as alleged in the complaint, the Protocol itself is unregistered in violation of federal law, and *someone* must be responsible." (Emphasis in original.)

Having concluded that the Ooki DAO could be legitimately be served, the court concluded that Ooki DAO had been properly served here. Given that it had no authorized agent or even a physical address, alternative service upon the DAO through electronic means, such as its "Chat Box and Online Forum" which "seem to be the DAO's chosen and preferred method of communication," was appropriate and "reasonably calculated to apprise Ooki DAO of this litigation." All indications were that the online postings had garnered sufficient attention among the DAO's tokenholders for the DAO to have gotten actual notice.

The court rejected the amici's contention that the CFTC was required to have served the individual tokenholders, noting that the CFTC "sued Ooki DAO as an entity and did not sue the individual Token Holders." While the court had earlier directed the CFTC to serve at least one of the U.S.-based tokenholders known to it "to achieve the best practicable notice," which the CFTC thereupon did, the court termed this just "a belt-and-suspenders procedure to ensure that the due process requirements are met." Because the CFTC had "utilized all of the information reasonably at its disposal to serve Ooki DAO, and it is clear that Ooki DAO has actual notice[,] [s]ervice was proper and complied with due process requirements."

Conclusion

The CFTC and the court in its *Ooki DAO* case resolved the seeming conundrum of whether there can be law without people by rejecting the very premise underlying that supposed conundrum and taking the view that in fact there are always people involved. People create software, modify it, deploy it, participate in its governance and choose whether, when and how to interact with it. Lawsuits may address the use of a software tool and even essentially preclude such use, but in this view the lawsuit should be conceived not as a suit against code or technology, but rather against the people behind it.

Smart contracts are not simply a feature of nature that one might encounter as one might a volcano or a raging river. Humans create them, and humans make choices about interacting with them. Flexible legal concepts such as "unincorporated associations" may provide a sufficient basis

for lawsuits attacking smart contract applications that do not include individuals as defendants, despite the seeming lack of any formal legal organization among the persons allegedly involved.

It appears that OFAC in its Tornado Cash sanctions has taken a similar approach, describing "Tornado Cash" as being not merely a technology or a tool, but in fact an "entity" of some kind. Whether the courts hearing the lawsuits now challenging those sanctions will accept OFAC's view remains to be seen. But when dealing with human creations such as software, the *Ooki DAO* court's insistence that "*someone* must be responsible" for those creations and their effects, rather than no one, may be more likely to appeal to judges than the suggestion that situations have been created where law is powerless to operate because there are no people involved