CoinDesk

More than Just the Ooki DAO: Lessons for Web3 Companies About Control After bZx

The CFTC's decision to bring an action against a DAO late last month sent shockwaves that continue to reverberate through the Web3 community.

By David Kappos, Evan Norris and Daniel Barabander
October 31, 2022

This article was originally published on CoinDesk.

In September, the Commodity Futures Trading Commission (CFTC) brought two actions against bZeroX, its two co-founders and the Ooki decentralized autonomous organization (DAO) for violations of the Commodity Exchange Act and underlying regulations.

While the commission's move against the Ooki DAO is no doubt a significant milestone, there are other important aspects of these enforcement actions that also merit close attention, including for what they teach us about how regulators view control of Web3 protocols to work around technical hurdles and hold operators accountable.

David J. Kappos is a partner in Cravath, Swaine & Moore's corporate department and co-chair of the firm's intellectual property practice. Evan Mehran Norris is a partner in Cravath, Swaine & Moore's litigation department and a member of the firm's investigations and regulatory enforcement practice. Daniel M. Barabander is an associate in Cravath, Swaine & Moore's corporate department.

Over the past several years, we have repeatedly heard from industry participants that enforcement against Web3 platforms is unlikely, or even impossible, because existing regulations have architectural incompatibilities with Web3 platform functionality, making the concept of compliance inapt. That view should finally be put to rest. As the U.S. Treasury Department (Tornado Cash) and now the CFTC have demonstrated, regulators can and will make aggressive arguments to maneuver around potential barriers to enforcement presented by Web3 technology.

The area where we repeatedly see regulators blur the line between technical reality and their regulatory objectives is around control of a decentralized protocol. The bZx protocol, like all Ethereum-based protocols, is built using smart contracts, the defining feature of which is that they do not require a centralized operator to run their code; they run autonomously. This is a challenge blockchain technology presents to regulators across the board – how to hold persons accountable for code that does not require identifiable persons to run?

The bZx enforcement action demonstrates how at least one key regulator is thinking about control of Web3 protocols in order to hold operators accountable: by examining both technical and business control to draw the line between identifiable persons and autonomously run protocols.

Technical control

Technical control refers to technical mechanisms protocol developers use to control their protocol on the smart contract level, often by defining “admin-only” functions that can be called solely by specific parties. Technical control is at the heart of the CFTC’s analysis. In fact, it is the determiner of the two time periods the CFTC lays out – the “bZx Relevant Period” and the “DAO Relevant Period.”

Within those two time periods, the CFTC focuses on four levers of control – admin-only functionalities retained by bZeroX and the co-founders, and subsequently, the DAO: (1) upgrading protocol smart contracts; (2) pausing or suspending trading; (3) pausing or suspending contributions or withdrawals of assets and redemptions; and (4) directing disposition of the funds held on protocol smart contracts.

The CFTC’s primary vehicle for pointing out instances in which these parties did in fact exert such control relate to two exploits. First, it cites a $55 million hack the protocol suffered in November 2021 after a “spearfishing attack against a bZx DAO developer.”

In response to the breach, the DAO exerted its control over treasury funds, by “vot[ing] to utilize funds from the bZx DAO Treasury to compensate certain bZx DAO members and other users of the bZx Protocol who lost funds in connection with” the incident.

Second, the commission cites a February 2020 margin-lending exploit that targeted bZx and led to a loss of 1,300 wrapped ETH. To stop the hemorrhaging, “bZeroX utilized its Keys to pause trading and withdrawals, and to implement fixes to the smart contract code, to address the existing or potential losses to the bZx Protocol” caused by the incident.

As these two incidents show, technical control is at the heart of Web3 exploits because it (a) presents centralized points of failure and thus an attractive attack vector in decentralized systems and (b) exists to allow a protocol to swiftly respond to emergencies. The responses to these attacks make an easy case for regulators to demonstrate technical control and, thus, identifiable operators of the protocol.

Business control

The CFTC also repeatedly points to softer “business controls” to show that the respondents had control of the bZx protocol and, thus, should be liable.

The commission focuses most clearly on the fact that the respondents “designed, deployed, marketed and made solicitations” concerning the bZx protocol.

First, it is clear that the CFTC views operating a front-end website to interact with the bZx protocol as a form of business control. The CFTC cites the front end as a vehicle "to market, solicit orders for and facilitate access to the bZx Protocol" because it "enabled users, through the click of a few buttons, to transfer assets and open positions on the bZx Protocol."

Second, and as discussed above, the CFTC cites the respondents' public statements and marketing as examples of business control. For example, the commission points out that the co-founders "made public statements, appeared in interviews, wrote articles, led calls with community members that are publicly available on YouTube and otherwise publicly marketed and solicited members of the public to utilize the bZx Protocol" pre- and post-shifting technical control to the DAO, all as a form of business control.

Third, active participation in a DAO is seen as a form of business control. The CFTC finds in the settlement order that the co-founders were active on Ooki DAO governance matters. Further, one founder is cited for his "protocol development and marketing work … on the Ooki DAO's behalf during the DAO Relevant Period," while another is cited for his "business and budget planning and marketing work … on the Ooki DAO's behalf during the DAO Relevant Period" for Ooki DAO after it obtained technical control.

The CFTC describes the co-founders' active participation in the Ooki DAO to show why they are being held personally liable for the DAO's actions. This is particularly interesting because the CFTC's definition of DAO membership only requires casting a vote, so there should be no need to show the co-founders' active involvement in the DAO to establish their membership in the DAO as the basis for holding them personally liable for the actions of the for-profit unincorporated association. The commission's focus on such participation – despite it appearing superfluous in light of the CFTC's definition of DAO membership – indicates that it views such participation as probative from a business control standpoint.

These enforcement actions reinforce the need for operators of Web3 protocols to have a better compliance policy than "technological infeasibility of compliance, so no compliance." The CFTC's in-depth analysis of technical and business control shows this clearly. Even though the bZx protocol runs autonomously, that will not stop regulators from seeking to identify operators in order to hold them accountable. While technology-first analysis is an important tool that can be used to support legal risk assessments, the bZx actions make clear that purely technical distinctions cannot justify a legal compliance strategy detached from practical realities.

As long as enforcement actions by federal regulatory agencies remain the dominant approach to policy development in the Web3 field, we must look to those actions to understand the evolving state of the regulatory landscape and what may come next. The CFTC's moves against the bZx protocol demonstrates that regulators see points of control as strings to follow to the marionettist.