Articles + Publications | September 2, 2022

Plaintiff, Partner, or Neither? The bZx DAO and the Unknown Tale of Token Approvals

WRITTEN BY

Ethan G. Ostroff | Addison J. Morgan

Seven years ago, Ethereum launched and became the predominant blockchain for developers to build decentralized applications powered by smart contracts (dApps). By leveraging Ethereum's smart-contract compatibility, developers realized they could catalyze a new era of finance that affords market participants permissionless access to traditional financial products like insurance, derivatives, and lending and borrowing.

Presumably, a consumer only enters the DeFi realm to obtain a certain level of power that traditional finance does not currently offer: the power to sell, lend, borrow, invest, or otherwise transact on his or her own time without the need of a facilitating intermediary. This point is key. Decentralization — the minimization of the amount of trust a market participant must vest in a single actor within an economic system due to trust being broadly dispersed among a variety of actors within that same system — is the bedrock of DeFi. Nevertheless, this distribution of trust does not automatically render DeFi unsusceptible to error.

This is the unfortunate tale of the 14 named class members of a recent class-action lawsuit filed against bZx DAO. Except for Wyoming and Tennessee, the only states that currently consider decentralized autonomous organizations (DAOs) to be limited liability companies, DAOs are not recognized as legal entities. Consequently, the overarching theory of this putative class-action lawsuit is grounded in common law. If two or more individuals participate in a joint venture and share in profits and losses, the jurisprudence of virtually every jurisdiction in America holds these parties have entered a general partnership. The problem with the general partnership corporate form is that, in the event the partnership incurs any financial liabilities, each partner (even those whose actions did not engender the debts) will be held jointly and severally responsible. Utilizing the general partnership theory as a jurisdictional hook, the class members seek to hold each member of the bZx DAO liable for the alleged negligence of an unnamed developer employed by the bZx DAO.

This brief overview of general partnership law generates an interesting question. Without destroying the applicability of its general partnership theory, can the bZx DAO class members sue the entire bZx DAO membership under the notion that an employee of the bZx DAO negligently carried out his or her responsibilities? Only time will tell, but an overlooked aspect of smart contract functionality may deliver a resounding blow to the plaintiffs' ability to seek the full breadth of potential damages of its negligence claim — token approvals.

Class-Action Lawsuit

On May 6, 14 named individuals brought a putative class-action lawsuit against bZx and its co-founders Kyle Kistner and Tom Bean. bZx is an Ethereum, Polygon (Poly), and Binance Smart Chain (BSC)-compatible DeFi

lending dApp that enables users to borrow, lend, and margin trade. The bZx ecosystem is composed of two interfaces that enable platform participants to interact with bZx smart contracts: (1) Fulcrum, which facilitates tokenized lending and margin trading; and (2) Torque, which facilitates instant issuance of crypto-collateralized loans.

On August 3, 2021, bZx released a blog post, noting that during the week of August 2, 2021, bZx would begin converting to a DAO. An important step in this transitionary phase required the bZx core team to relinquish custody of the private keys of the treasury of the bZx protocol to the new bZx DAO by integrating and deploying a new smart contract address that would enable each holder of the native token of the bZx protocol, BZRX, to steer the platform moving forward. However, on November 5, 2021, an unnamed bZx developer succumbed to a "phishing attack," which granted an unidentified party access to the developer's personal crypto wallet. This event afforded the attacker direct access to the private keys of the Poly and BSC-Fulcrum smart contracts and the public wallet addresses of the Poly and BSC-Fulcrum users. Equipped with this data, the attacker absconded with approximately $55 million in total value from the bZx protocol and $1.6 million in total value from the named plaintiffs.

According to the plaintiffs, bZx consistently touted its commitment to ensuring the safety of user funds. Prior to the attack, the developer had successfully transitioned the private key of the Ethereum-Fulcrum smart contracts to the bZx DAO. Consequently, users who exclusively interacted with the bZx protocol through Ethereum were not affected by the attack. Based on the discrepancy in security measures, the plaintiffs contend the bZx DAO and the co-founders negligently failed to maintain the security of the Poly and BSC deployments of the bZx protocol.

General Partnership or Not?

The class definition proposed by the plaintiffs includes individuals who "delivered cryptocurrency tokens to the bZx protocol and had any amounts of funds stolen in the [phishing attack]," but specifically excludes individuals who solely lost BZRX tokens, which were the native tokens of the bZx protocol and are the governance tokens of the bZx DAO. As we have previously discussed, an individual's DAO membership status is generally derived from his or her possession of the DAO's governance token. Consequently, the plaintiffs' present class certification framing may prove to be problematic in the long run. It facially excludes holders of the BZRX token and impliedly suggests that the 14 named plaintiffs never held BZRX tokens as they "used different tokens on the protocol." Sharing in the profits or losses of a DAO alleged to be a general partnership presupposes that an individual is in possession of the DAO's governance token. However, it appears that the plaintiffs and the putative class are comprised of individuals who had been depositing their personal cryptocurrency holdings on Fulcrum in exchange for yields ranging from 5.3% APR to 7.2% APR. This indirect interaction with the bZx DAO (through Fulcrum) may not be enough to transform the named plaintiffs into members of the bZx DAO.

Negligence 101

To prevail on a negligence claim, a plaintiff must generally establish four elements: (1) the defendant owed the plaintiff a "duty of care"; (2) the defendant breached this duty of care; (3) the defendant's breach of duty caused the plaintiff's injury; and (4) the plaintiff incurred damages because of the injury caused by the defendant's breach of duty.

The duty of care element of plaintiffs' negligence claim will likely develop into a contentious point of dispute.

Duty of Care. Generally, parties do not immutably owe each other a duty of care. However, partners in a business organization owe fiduciary duties to each other. Under California law, partners of a general partnership owe to each other a duty of care to refrain from engaging in intentional misconduct, a knowing violation of law, or grossly negligent or reckless conduct. Therefore, if the court does not concur with the plaintiffs and refuses to characterize the bZx DAO as a general partnership, California's general partnership law will not apply, and no fiduciary duties will arise. Additionally, if the named plaintiffs fail to establish the bZx DAO owed a general duty of care, this event could possibly nullify the lawsuit as a matter of law since negligence claims cannot survive without the existence of a duty of care, irrespective of the conduct of the developer employed by the bZx DAO.

Token Approvals and Contributory Negligence. All dApps leverage "contract operations," which refer to the process by which smart contracts communicate to effectuate transaction finality. Contract operations involve two separate transactions with differing functionality: (1) an "approve" function, which grants to the smart contract access to a user's wallet address and enables the smart contract to validate a user's token balances; and (2) a "transferFrom" function, which enables the smart contract to facilitate the transfer of a specified amount of the user's tokens to another smart contract.

For example, if a user desires to deposit 1,000 Tether (USDT) on a dApp to earn interest, the user must first "approve" the dApp's smart contract to withdraw USDT from the user's wallet. Approval is effectuated through signature of the private key address that corresponds to the public key address of the user's wallet. Once it receives authorization, the dApp's smart contract will commence the "transferFrom" function, which will deposit into the dApp's smart contract the 1,000 USDT approved by the user. This is where things become tricky.

After a user approves a dApp's smart contract for the first time, the dApp's smart contract may no longer request approval from the user for future transactions. This is because, in the interest of swiftness, many dApps set smart contract default approval limits to "unlimited." Practically speaking, this default setting effectively grants smart contracts the ability to transfer a user's tokens at any time, without obtaining the user's consent, which in theory, reduces transaction costs as a user only must provide the smart contract with authorization once. However, the "Catch-22" of this practice is that unlimited approvals, in effect, afford smart contracts unrestricted access to tokens contained in a user's wallet. Therefore, if our hypothetical user's wallet contained 10,000 USDT and the dApp's smart contract he or she interacted with had a default approval limit of unlimited, the user has granted the smart contract continuous access to his or her 10,000 USDT, notwithstanding the fact that only 1,000 USDT was deposited into the smart contract through the "transferFrom" function.

Therefore, if a malicious actor gains control over a DeFi protocol, the actor could upgrade the protocol's smart contracts and drain the funds of user wallets with an approval limit of unlimited because, as discussed above, approvals are authorized by a user's own private key signature. Importantly, "approval" permissions can be modified and revoked, but this is one of the most esoteric, consumer-facing aspects of smart contract functionality.

It is unclear whether the plaintiffs and the putative members of the class fall into this bucket of individuals who granted unlimited approvals to the Poly and BSC-Fulcrum smart contracts, but if so, the failure to institute approval limitations may constitute contributory negligence, which could theoretically lessen the bZx DAO's liability. Notably, according to bZx, only a "limited number of users" had funds directly stolen from their wallets due to

unlimited approvals.

Our Take

For the remainder of 2022, the legal recognition of DAOs as true, corporate entities is likely to remain in flux throughout the country. However, the bZx DAO case implicates an issue that has been overlooked — consumer education. Blockchain technology removes centralized intermediaries from transactions, and as a result, it incidentally places a substantial research obligation in front of those who dare leverage its utility. Malicious actors exist in every facet of the global economy. And, in a decentralized world run on blockchain, the prevalence of these type of actors could exponentially increase due to the complexities underpinning blockchain technology. A potential solution would be to require the leadership of DeFi protocols to uniformly disclose to individual consumers the risks, technical and otherwise, associated with interacting with DeFi products offered by the protocol. In turn, as a consumer navigates through DeFi, these disclosures could continuously increase a consumer's base knowledge of the obscure aspects of blockchain technology — for example, custody, cryptography, smart contracts, and token approvals — which will better enable the consumer to insulate him or herself from monetary loss.

RELATED INDUSTRIES + PRACTICES

- Consumer Financial Services
- Digital Assets + Blockchain
- Payments + Financial Technology