# DAOs and cybersecurity

10.10.2022 3 min read

**Authors**

**Felipe Palhares**

**Related areas**

Data Privacy and Cybersecurity

**Topics**

Data Privacy and Cybersecurity
DAOs

As previously mentioned in other articles of this e-book, DAOs are, in essence, computer language code stored on a decentralized and public network – which means: smart contracts on a certain blockchain.

For this very reason, cybersecurity is a fundamental issue when dealing with the development and functioning of a DAO, given that the actions to be executed by it will depend on the validity and integrity of the conditions and automations employed by the smart contracts.

A flaw in the code may put at risk all the resources kept in the DAO's treasury, as well as expose its members to directed attacks, specifically planned to reach certain individuals. In the past, some notorious cases involved problems in the encoding of DAOs' smart contracts.

The most famous of them occurred with the so-called genesis DAO, "TheDAO", which had raised more than US$150 million in 2016. Due to vulnerabilities in the smart contracts' code, a third party was able to divert almost a third of such amount to its own wallet, resulting in a hard fork of the Ethereum blockchain, which generated two distinct blockchains (the Ethereum Classic – the version prior to the fork – and the one currently called as Ethereum).

More recent examples also demonstrate the relevance of secure coding aspects, as well as information security during the structuring of smart contracts that will form the basis of a DAO and its regular functioning. In November 2021, one of the developers of bZx DAO, a DeFi platform, was the target of a well-succeeded phishing attack, which allowed the attacker to access the developer's wallet and, afterward, divert more than US$ 55 million.

Because of the incident, people that were affected by the deviation of funds filed a class action against the founders of bZx DAO in the State of California, claiming that all of them were jointly liable for the negligence in structuring a secure protocol. Even though this claim has not yet been reviewed by the court, the repercussions of the future decision will be relevant to assess who shall be considered responsible for similar situations, and, especially, whether DAOs are to be considered as general partnerships, which is the equivalent to the "*sociedades em comum*" in Brazil.

In any event, it is undeniable that smart contract developers and DAO founders must take additional precautions to avoid being, in the future, liable for failures in the code or problems connected with information security.

It is worth remembering that DAOs will naturally process the personal data of their members, so that, in theory, issues related to the compliance of the structures created with the "*Lei Geral de Proteção de Dados Pessoais*" (The Brazilian General Data Protection Law or LGPD) must be evaluated, even though blockchain technology entails inherent challenges in aspects of compliance with data protection laws.

At the very least, it will be fundamental for developers and founders to adopt good practices in information security issues, mitigating risks of known and frequent problems, such as phishing attacks like the one resulting in the deviation of the resources from bZx DAO, which could have been avoided with a certain ease. In such cases, evading a negligence claim can become complex, as it could be expected from a developer to adopt greater precautions to protect their accounts – and, consequently, the assets from third parties that were stored in the DAO's treasury.

Therefore, when structuring a DAO, beyond the secure coding techniques, it is also crucial to assess which information security measures will be employed by developers and founders, such as using a double factor authentication, frequently updating software, and auditing the code to ensure the absence of obvious flaws.

The lack of these cautions may hamper the defense of founders and developers facing lawsuits that may be filed by DAO members when injured by some flaw in the smart contracts or by negligent conduct carried out by founders and developers.

***>>> This content belongs to our e-book "DAOs: Legal Challenges for Decentralized Autonomous Organizations". Click here to read more articles.***

› PROFESSIONALS

## Professionals who combine legal insight and market perspective

**Felipe Palhares**