DAOs e cybersecurity

10.10.2022 3 minutos de leitura

Autores

Felipe Palhares

Áreas relacionadas

Proteção de Dados e Cybersecurity

Assuntos

Proteção de Dados e Cybersecurity | DAOs

Como já foi destacado em outros artigos deste e-book, DAOs são, na sua essência, códigos em linguagem de computação armazenados em uma rede pública descentralizada – leia-se: *smart contracts* em uma determinada *blockchain*.

Por isso mesmo, *cybersecurity* é um tema fundamental quando se trata da construção e funcionamento de uma DAO, na medida em que as ações que serão por ela executadas dependerão da validade e integridade das condições e das automatizações implementadas pelos *smart contracts*.

Uma falha no código pode colocar em risco todos os recursos mantidos na tesouraria da DAO, assim como expor os seus membros a ataques direcionados, planejados especificamente para alcançar determinados indivíduos. No passado, alguns casos notórios envolveram problemas na codificação dos smart contracts de uma DAO.

O mais famoso deles ocorreu com a chamada gênesis DAO, a *TheDAO*, que levantou mais de US$ 150 milhões em 2016. Em razão de vulnerabilidades no código de seus *smart contracts*, um terceiro conseguiu desviar quase um terço dos respectivos valores para uma carteira própria, o que acabou culminando num *hard fork* da *blockchain* da *Ethereum*, gerando duas *blockchains* distintas (a *Ethereum Classic* – versão anterior ao *fork* – e a que atualmente se chama de *Ethereum*).

Exemplos mais recentes também demonstram a relevância de aspectos de *secure coding* e de segurança da informação na estruturação dos *smart contracts* que formarão a base de uma DAO e no seu regular funcionamento. Em novembro de 2021, um dos desenvolvedores da *bZx DAO*, uma plataforma de DeFi, foi alvo de um ataque bem-sucedido de *phishing*, que permitiu que o atacante obtivesse acesso à carteira do desenvolvedor e, posteriormente, desviasse mais de US$ 55 milhões.

Por conta do incidente, pessoas que foram afetadas pelo desvio dos recursos ajuizaram uma ação coletiva contra os fundadores e membros da *bZx DAO* no Estado da Califórnia, alegando que todos são solidariamente responsáveis por negligência na estruturação de um protocolo seguro. Embora referida demanda ainda não tenha sido julgada, as repercussões da futura decisão serão relevantes para a avaliação de quem deve ser considerado responsável por situações como esta, e, especialmente, se DAOs devem ser compreendidas como *'general partnerships'*, ou, no equivalente nacional, como sociedades em comum.

Em qualquer cenário, não há dúvidas que desenvolvedores dos smart contracts e fundadores de uma DAO devem tomar cautelas adicionais para evitar serem posteriormente responsabilizados por falhas nos códigos ou por problemas relacionados à segurança da informação.

Vale lembrar que DAOs naturalmente tratarão dados pessoais dos seus

membros, de modo que, em tese, considerações acerca da conformidade das estruturas criadas com a Lei Geral de Proteção de Dados Pessoais deverão ser avaliadas, muito embora a tecnologia *blockchain* traga desafios inerentes em aspectos de observância às normas de proteção de dados.

No mínimo, será fundamental que desenvolvedores e fundadores adotem boas práticas no quesito de segurança da informação, mitigando riscos de problemas conhecidos e frequentes, como ataques de phishing iguais àquele que resultaram no desvio dos recursos da *bZx DAO*, e que poderiam ter sido evitados com certa facilidade. Em casos como esse, furtar-se de um argumento de negligência pode se tornar complexo, uma vez que poderia ser esperado que o desenvolvedor adotasse precauções maiores para proteger suas contas – e, consequentemente, os recursos de terceiros, que estavam depositados na tesouraria da DAO afetada.

Portanto, na hora de se estruturar uma DAO, além de técnicas de *secure coding* também será essencial avaliar quais medidas de segurança da informação serão implementadas por seus desenvolvedores e fundadores, a exemplo da utilização de duplo fator de autenticação, atualização frequente de softwares e realização de auditorias nos códigos para garantir a ausência de falhas evidentes.

A ausência desses cuidados pode dificultar a defesa de fundadores e desenvolvedores em demandas judiciais que venham a ser ajuizadas por membros da DAO que sejam lesados por alguma falha nos *smart contracts* ou por condutas negligentes praticadas por fundadores e desenvolvedores.

>>> Este conteúdo faz parte do e-book "DAOs: Desafios Jurídicos das Organizações Autônomas Descentralizadas". Clique aqui para ler mais artigos.

› PROFISSIONAIS

Profissionais que aliam visão jurídica e visão de mercado

Felipe Palhares