Opinião: Ataques em blockchain e responsabilidade civil

Casos de fraudes envolvendo desvio e subtração de criptoativos acumulam-se no mercado impulsionado pelo uso da *blockchain*. Os criminosos aproveitam-se de vulnerabilidades por vezes existentes em *exchanges* e em *smart contracts*, para drenar criptoativos para *digital wallets* que, embora monitoradas, não possuem nenhum dado pessoal vinculado, o que torna difícil a identificação da autoria do ilícito e

Um dos primeiros casos de furto de criptoativos, e talvez um dos mais emblemáticos, aconteceu com a *exchange* japonesa Mt. Gox. Até hoje não se sabe direito o que gerou o sumiço dos criptoativos. No entanto, especula-se que a *exchange* tenha sido alvo de um ataque *hacker* que lhe tomou mais de 322 milhões de dólares em criptomoedas, sobretudo em bitcoin.

Independentemente do que tenha acontecido, casos como este abrem espaço para a discussão sobre a existência da responsabilidade civil da *Exchange* por defeitos no serviço que causem danos aos clientes, incluindo os advindos de perda, furto ou extravio de criptoativos.

Nesse sentido, a jurisprudência brasileira tem se posicionado quanto à aplicabilidade das normas de direito do consumidor sobre as atividades desempenhadas por *exchanges*. O Tribunal de Justiça de São Paulo (TJ-SP), por exemplo, tem entendido que, como agente prestadora do serviço de intermediação e custódia de criptoativos, a *exchange* encaixa-se satisfatoriamente na definição de fornecedor do artigo 3º do Código de Defesa do Consumidor (CDC). Ainda segundo o TJ-SP, a *exchange* deve responder, conforme o artigo 14 do mesmo diploma, de forma objetiva pelos danos gerados por defeitos relativos à prestação dos serviços.

Mas, se por um lado, a imputação da responsabilidade civil por danos tem sido atribuída às *exchanges* — quando é possível identificar um defeito no serviço que resulte em prejuízo —, como definir a responsabilidade por dano decorrente de falha ou *hack* na própria *blockchain*?

Um dos maiores *hacks* da história do mundo cripto aconteceu semanas atrás na rede Ronin. Ela consiste em uma *sidechain* que funciona como uma espécie de ponte entre diferentes *blockchains*, sendo uma delas a que roda o jogo *Axie Infinity*. Nesse caso especificamente, o hacker aproveitou-se de uma vulnerabilidade do sistema de criptografia e raqueou chaves privadas de ao menos quatro dos nove nós validadores da rede. Com isso, o hacker conseguiu drenar cerca de US$ 625 milhões em criptomoedas, incluindo Ether e USDC.

Ataques desse tipo chamam atenção não apenas pelo volume em dinheiro subtraído, mas sobretudo porque colocam em xeque a própria integridade de uma *blockchain*. Problemas desse tipo são raros no mundo cripto. Uma perda generosa de criptoativos quase nunca acontece por falhas na própria blockchain. Apesar da baixa frequência com que ocorrem, problemas dessa natureza começam a levantar desde já possíveis indagações a respeito do que seria uma *blockchain* segura, e mais, de quem seria a efetiva responsabilidade pelos danos sofridos.

Para responder a essas perguntas, há que se fazer pelos menos duas distinções: primeira, considerar que os criptoativos estão custodiados em uma *exchange*; segunda, considerar que os criptoativos estão sendo negociados em protocolos de finanças descentralizadas (Defi), sem que seja possível identificar uma organização custodiante.

No primeiro caso, em que os ativos estão custodiados em *exchanges*, eventual perda decorrente de ataque na *blockchain* dificilmente poderá gerar alguma responsabilidade para *exchange*. Há quem possa argumentar que, estando a *exchange* inserida na cadeia de consumo, deveria ser ela solidariamente responsável por perdas desse tipo. No entanto, argumentos desse tipo são frágeis, porque não há como identificar diante do caso apresentado nexo de causalidade claro entre o serviço prestado pela *exchange* e o prejuízo. A falta de nexo de causalidade pode ainda levantar a hipótese de excludente de responsabilidade por inexistência de defeito no serviço (artigo 14, parágrafo 3º, I do CDC) ou, ainda, por caso fortuito (artigo 393 do Código Civil).

A situação é um pouco diferente caso os criptoativos cuja *blockchain* foi raqueada estejam sendo negociados em protocolos de Defi sem que seja possível identificar uma organização custodiante. incerteza jurídica, mas da própria dificuldade de identificar uma organização responsável pelo oferecimento da estrutura de negociação e custódia dos criptoativos.

É ilusório pensar que pelo fato de o registro em *blockchain* ser descentralizado não haja uma instituição identificável ou alguém por trás da criação do protocolo e da sua manutenção. Normalmente, fundações ou, no mínimo, um grupo de pessoas sem personalidade jurídica constituída, desempenham esse papel. No entanto, permanece ainda uma dificuldade identificar qual o exato papel a fundação ou o grupo de pessoas desempenhou na criação ou na manutenção.

Nesse caso especificamente, a dificuldade na atribuição de responsabilidade não decorre tanto da protocolo e, ainda, se as atividades desempenhadas poderiam classificar a organização ou o grupo de pessoas como "fornecedores" e atrair, com isso, alguma responsabilidade decorrente de lesão ao consumidor.

Enquanto se discute de quem é a responsabilidade em casos como esses, ou até mesmo se há algum tipo de responsabilidade (solidária), prejuízos decorrentes de ataques como o da rede Ronin e outros acabam tendo que ser resolvidos, se é que são resolvidos, com base apenas em negociações com o hacker.

Date Created
02/06/2022