

Américo Moraes: Apreensão e recuperação de criptoativos

Tem-se tornado popular a prática de delitos envolvendo criptoativos, sobretudo casos cujos autores oferecem auxílio para investimento nesse mercado, mas utilizam a promessa como um pretexto para subtrair os valores cantados de seus clientes. Tais esquemas vêm acompanhados de nomes populares, como "esquemas ponzi".



Quando ocorrem tais delitos, é possível a realização dos

meios tradicionais para a recuperação do prejuízo sofrido pelas vítimas. Juridicamente, é possível a realização do sequestro — caso em que são apreendidos e bloqueados bens adquiridos diretamente com os valores subtraídos das vítimas — e o arresto — quando mesmo o patrimônio adquirido previamente ao crime é bloqueado e destinado ao ressarcimento. Nesses casos, realiza-se a apreensão e bloqueio de todos os bens pertencentes aos autores do delito — tais como imóveis, veículos, embarcações, etc.

Mesmo assim, o surgimento do mercado de criptoativos tornou possível aos indivíduos o armazenamento de valores sem a existência de ponto referencial físico, sem a necessidade de custódia por uma instituição financeira e sem a imediata vinculação a seu detentor (visto que seu registro na *blockchain* é realizado mediante o respectivo "endereço"). Isto é, desde a invenção do bitcoin — seguido pelo surgimento de milhares de outros criptoativos —, é possível que a custódia de valores milionários seja realizada mediante o acesso a uma chave criptográfica, que pode inclusive ser decorada pelo indivíduo [\[1\]](#).

Nesse caso, é correto dizer que há maior dificuldade na identificação e apreensão de valores custodiados em criptoativos. Devido à descentralização — isto é, que as transações não necessitam de intermediários financeiros para serem realizadas —, é possível que não haja um destinatário para as autoridades endereçarem uma ordem para bloqueio dos valores, assim como ocorre no sistema financeiro tradicional.

Todavia, o modo de custódia da imensa maioria dos ativos digitais não ocorre da maneira descentralizada. Devido à complexidade do sistema, há nesse ambiente inúmeros prestadores de serviços, os quais se apresentam como intermediadores. Eles permitem maior facilidade aos usuários e, conseqüentemente, garantem maior volume de transações. É o caso das *exchanges* centralizadas (também chamadas de "casas de câmbio de criptoativos"), que causaram um movimento de "recentralização" no mercado de criptoativos.

O surgimento desses *players* no mercado fez surgir a possibilidade de o Estado realizar o mesmo método de controle praticado no sistema financeiro tradicional: exigir desses intermediadores a identificação dos seus usuários. Com isso, passou a ser possível duas medidas importantíssimas para a realização de bloqueios e apreensões de criptoativos: 1) a capacidade de descobrir o usuário responsável por transações com criptoativos, assim como 2) o cumprimento de ordens judiciais de bloqueio de ativos digitais que estejam custodiados nessas *exchanges*. Em termos simples, criptoativos custodiados em *exchanges* centralizadas operam de maneira idêntica aos valores armazenados em instituições financeiras tradicionais.

Mesmo assim, há nesse ambiente uma possibilidade não existente no sistema bancário: a capacidade de o usuário custodiar seus criptoativos de maneira autônoma, nas chamadas "carteiras privadas". Esse é o cenário mais comum para o caso daqueles que tem a pretensão de impedir o Estado cumprir ordens de bloqueios de seus ativos digitais, cenário que demanda a realização de métodos mais complexos de investigação — os quais estão em constante aperfeiçoamento pelas autoridades policiais.

A primeira hipótese em que é possível a apreensão de criptoativos é quando estão custodiados em "carteiras físicas" — também chamadas de *cold wallet* ou *hardware wallet*. Já houve caso em que a autoridade policial brasileira cumpriu mandado de busca e apreensão na residência de pessoa investigada por esquema de "pirâmide financeira" com criptoativos [2] e apreendeu um dispositivo chamado "OpenDime" [3], uma *hardware wallet* de bitcoin cuja função é ter um dispositivo físico o qual garante que somente seu detentor terá acesso aos bitcoins nele custodiados.

Esse é um caso que, diferentemente das *hardware wallets* convencionais — que permitem a realização de um *backup* da chave mnemônica —, é impossível que terceiros conheçam a respectiva chave criptográfica. Assim, uma vez apreendido, é possível à autoridade policial a transferência dos valores à uma "carteira" controlada pelo Estado.

Outra possibilidade interessante para a apreensão de criptoativos será recorrer a grandes empresas que realizam a análises em *blockchain*. Elas visam o fornecimento de dois tipos de serviços: 1) *softwares* destinados a empresas que operam no mercado de criptoativos para que possam cumprir suas obrigações de prevenção à lavagem de dinheiro e financiamento do terrorismo; assim como 2) disponibilizar sua equipe para realizar o rastreamento dos mais diferentes criptoativos – inclusive aqueles tidos como anônimos, tais como a *monero*, *zcash*, *secret*, *oásis*, dentre outras. Essas empresas são as mesmas que fornecem serviços ao FBI e DOJ, mas que podem ser contratadas por vítimas de crimes patrimoniais envolvendo criptoativos.

Nesses casos, ainda que os valores estejam custodiados em "carteiras privadas", é possível que os "endereços sejam identificados e registrados em uma lista negra, compartilhado com as diversas empresas atuantes no mercado. Com esse método, assim que o autor do delito tente realizar a conversão desses valores para moeda estatal, os intermediadores interromperão imediatamente a transação e comunicarão às autoridades competentes.



Caso como esse já ocorreu na recuperação dos valores da empresa Bitfinex, uma *exchange* centralizada que foi hackeada em 2016 e teve 119.754 bitcoins desviados — os quais passaram posteriormente por processos de lavagem de dinheiro ainda dentro do mercado de criptoativos. Ainda que esses valores possam ser gastos sem retornar ao sistema financeiro tradicional, é comum a necessidade de os criminosos os transformarem em ativos do mundo físico. Foi o que ocorreu nesse caso, quando se acreditou que, devido às técnicas de lavagem, os valores estariam suficientemente mascarados. Para a surpresa deles, o valor equivalente a 3,6 bilhões de dólares foi bloqueado por investigação conduzida pelo *DOJ* [4].

Para nós, entendemos que as investigações em matéria de fraudes com criptoativos devem ser conduzidas com uma parceria entre o público e o privado. Empresas que realizam a monitoração e investigação em *blockchain* possuem, atualmente, tecnologia de ponta para deanonimizar transações com criptoativos e, com isso, permitir às vítimas a recuperação de valores. Somado a isso, as autoridades públicas possuem os métodos coercitivos capazes de realizar o bloqueio e apreensão dos valores. Entende-se que somente com uma estratégia alinhada entre ambos os setores é possível conduzir uma investigação eficiente, que visa garantir aos responsáveis a punição adequada pela prática do crime, assim como ressarcir o prejuízo sofrido pelas vítimas.

[1] MORAES, Felipe Américo. *Bitcoin e Lavagem de Dinheiro*. Belo Horizonte: editora Tirant Lo Blanch, 2022. P. 192-193.

[2] Disponível em: <https://livecoins.com.br/policia-federal-faz-operacao-contr-grupo-bitcoin-banco/>. Acesso em 15 mar. 2022.

[3] Disponível em: <https://opendime.com/>. Acesso em 15 mar. 2022.

[4] Disponível em: <https://www.bloomberg.com/news/articles/2022-02-08/doj-seizes-3-6-billion-in-bitcoin-stolen-in-2016-bitfinex-hack>. Acesso em 15 mar. 2022.