Uso de mixers, moedas de privacidade e OTCs na lavagem pela criptodelinquência

25/08/2024

A Lei nº 14.478/22, que além de estabelecer diretrizes a serem observadas na prestação de serviços de ativos virtuais e na regulamentação das prestadoras de serviços de ativos virtuais, e que alterou o Código Penal para criar o tipo previsto na redação do artigo 171-A, promoveu três alterações na Lei nº 9.613/98 (Lei de Lavagem de Dinheiro): uma nova causa especial de aumento de pena quando o crime de lavagem de capitais for cometido "por meio da utilização de ativo virtual" (§4º do artigo 1º); a ampliação do rol fechado das pessoas que devem cumprir obrigações de conformidade para fins de prevenção à lavagem de dinheiro, ao financiamento do terrorismo e à proliferação de armas de destruição em massa (inciso XIX do artigo 9º) ao incluir as "prestadoras de serviços de ativos virtuais"; e a criação de um instrumento de *compliance* para pessoas politicamente expostas (artigo 12-A).

Apesar do avanço legislativo e da discussão sobre o Bitcoin e outras criptomoedas serem ferramentas úteis para a delinquência ainda não ter sido completamente superada — muito embora tenha evoluído[1] —, há de se convir que a utilização de ferramentas de anonimização, como, por exemplo, os *mixers* e as moedas de privacidade representam um desafio significativo para as autoridades na aplicação da lei.

Apesar de o tema não estar em voga no cenário midiático ou acadêmico brasileiro, apesar da notável quantidade de "pirâmides financeiras" que se valem ou fingem se valer do uso de ativos digitais e criptomoedas, os *mixers* atualmente são alvo de forte repressão das autoridades norte-americanas e europeias, tal como podemos denotar do recente desativamento, em março de 2023, por meio uma operação conjunta do Departamento de Justiça dos EUA, do FBI, da Europool e da Polícia Alemã, do ChipMixer [2], um serviço de *mixer* de criptomoedas responsável por processar mais de US$ 3 bilhões em transações ilícitas, oriundas de vários tipos de crime, sobretudo de extorsão criptoviral [3].

É notório que o objetivo da lavagem de dinheiro é ocultar ou dissimular a origem ilícita de bens e valores que sejam frutos de crime para que, posteriormente, possam ser acessados e gastos. No contexto do crime baseado em criptomoedas, isso geralmente significa mover fundos para serviços onde eles possam ser convertidos em moeda fiduciária, frequentemente, e por evidente, tomando medidas extras para ocultar a origem ilícita dos fundos. Nesse sentido, os serviços de *mixer*, também conhecidos como *tumblers*, têm grande relevância e aplicabilidade.

Trata-se de *softwares* especializados utilizados no ecossistema de criptomoedas com o objetivo de aumentar a privacidade e o anonimato das transações mediante a "mistura" de criptomoedas de diferentes usuários, criando, dessa forma, um alto grau de ofuscação com o objetivo de dificultar o rastreamento das transações originais. Os *mixers*, na verdade, não surgiram com a intenção de ser uma ferramenta voltada para atividades criminosas, mas, sim, como uma ferramenta tecnológica para aumentar a privacidade e o anonimato nas transações realizadas com ativos digitais para indivíduos que residem em países cujos regimes são repressivos e cuja vigilância governamental é intensa, como, por exemplo, a Coreia do Norte.

Importante destacar que, como a função primária dos *mixers* é de aumentar a privacidade, deve-se reconhecer que nem todas as transações processadas nesse tipo de serviço são ligadas à atividade ilícitas. Ocorre, contudo, que diante da natureza desse tipo de serviço, que garante ainda mais uma camada de privacidade e de anonimato em comparação com as transações tradicionais, os serviços de *mixer* inevitavelmente atraíram a atenção da criminalidade.

Como funcionam os mixers

Os *tumblers* funcionam na modalidade *peer-to-peer*, permitindo que os usuários "misturem" seus ativos digitais com as de outros participantes sem a necessidade de um intermediário centralizado e de maneira criptograficamente segura, de modo que o detentor da plataforma não pode se apropriar indevidamente das unidades, que são posteriormente redistribuídas entre os usuários do *pool* na proporção individual de cada um, mediante a remuneração de 1% a 3% do valor total das moedas misturadas para o detentor do *software* ou plataforma.

As moedas de privacidade, por sua vez, oferecem recursos de anonimato aprimorados, tornando ainda mais difícil rastrear as transações que ocorrem com essas criptomoedas. Da mesma forma que acontece com os serviços de *mixer*, embora todas as transações realizadas com esse tipo de moeda não sejam destinadas a atividades ilícitas e mesmo considerando-se que esse tipo de ativo digital não foi criado com a intenção de cometer crimes, há de convir que as funções das moedas de privacidade são particularmente atrativas à criminalidade.

Spacca

O Monero (XMR), por exemplo, utiliza técnicas criptográficas avançadas, como assinaturas em anel, endereços furtivos e transações confidenciais para ocultar o remetente, o destinatário e o valor da transação. Em razão dessas características, organizações terroristas como o Estado Islâmico passaram a solicitar doações com essa criptomoeda [4] para posteriormente liquidá-las em moeda fiduciária mediante o uso de corretoras descentralizadas ou plataformas de pontes criptográficas, que permitem a transferência de ativos digitais entre diferentes *blockchains*, e que geralmente não possuem medidas firmes de *compliance*. Em razão disso, algumas autoridades regulatórias como, por exemplo, a japonesa, a emiradense e a coreana [5], baniram as moedas de privacidade, decisão que foi seguida por algumas corretoras de renome que funcionam no Brasil, como a Binance [6].

Enquanto alguns cibercriminosos podem manter seus ganhos ilícitos em carteiras pessoais por anos — presumivelmente na esperança de que as autoridades voltem sua atenção para outro lugar —, a maioria dos atores maliciosos busca converter seus fundos em ativos digitais para moeda fiduciária. Segundo a Chainalysis, após o uso de técnicas de ofuscação, mais de 50% dos fundos ilícitos acabam em corretoras centralizadas, direta ou indiretamente [7], devido à alta liquidez dessas plataformas e diante da facilidade de conversão de criptoativos para dinheiro que eles possuem.

Percebe-se, contudo, que diante dos riscos envolvidos nesse tipo de operação e diante da evolução do cenário regulatório brasileiro, os ambientes OTC [8] (*over-the-counter*) têm sido usados pela criminalidade para fins de lavagem de dinheiro com ativos digitais. Embora a maioria das OTCs sejam serviços legítimos, algumas operam sob a aparência de legitimidade, sem, contudo, exigir procedimentos adequados de KYC e AML (conheça seu cliente e antilavagem de dinheiro) e, muitas vezes, atendem especificamente à conversão de fundos ilícitos sob o recebimento de um percentual da operação.

Embora a legislação brasileira sobre lavagem de dinheiro tenha evoluído significativamente no que concerne aos ativos digitais e criptomoedas, é imperativo que o operador do direito e o legislador se atentem continuamente às novas práticas empregadas pela criptodelinquência. A dinâmica do mercado de ativos digitais é caracterizada por sua rápida evolução e pela constante inovação tecnológica, o que demanda uma vigilância jurídica e regulatória permanente. É necessário que se mantenham atualizados sobre as tendências globais e locais, observando atentamente as novas metodologias de lavagem de dinheiro e outras práticas ilícitas que emergem nesse setor.

[1] A Chainalysis, uma empresa norte-americana líder global em análise de blockchain e que fornece serviços e ferramentas para monitoramento e investigações que envolvem ativos digitais, esclareceu que em 2023 apenas 0,34% das transações *on-chain* (transações validadas e registradas permanentemente por meio do consenso da rede) de Bitcoin estavam associadas a atividades ilícitas. Disponível em: https://go.chainalysis.com/crypto-crime-2024.html

[2] Disponível em: https://www.moneylaunderingnews.com/2023/03/darkweb-cryptocurrency-mixer-chipmixer-shut-down-for-allegedly-laundering-3-billion-worth-of-crypto/

[3] SYDOW, Spencer Toth. Extorsão criptoviral. Boletim IBCCrim, São Paulo, v. 22, n. 258, p. 6-7, maio 2014.

Disponível em: https://www.lexml.gov.br/urn/urn:lex:br:rede.virtual.bibliotecas:artigo.revista:2014;1001079143. Acesso em: 11 jul. 2024.

[4] https://br.cointelegraph.com/news/isis-affiliated-news-website-to-collect-donations-with-monero

[5] https://beincrypto.com/privacy-coins-take-another-beating/

[6] https://www.coindesk.com/markets/2024/02/06/binance-to-delist-monero-privacy-token-xmr-slides/

[7] The Chainalysis 2024 Crypto Crime Report. Disponível em: https://go.chainalysis.com/crypto-crime-2024.html

[8] O significado de OTC é: over-the-counter (sobre o balcão, no sentido literal) e representa os ambientes e operações paralelas para negociar ativos financeiros. Sendo assim, o OTC equivale também ao chamado mercado de balcão no Brasil Sendo assim, pode-se dizer que o OTC é um mercado de títulos não regulamentados ou não cotados pelas regras da bolsa de valores. Disponível em: https://www.suno.com.br/artigos/otc/