

Hamis recebeu mais de US\$ 40 milhões em criptomoedas: entenda como o terrorismo se financia com moedas digitais

Ação do grupo terrorista Hamas trouxe à tona discussão sobre uso de criptos em atividades criminosas, o falso anonimato e a rastreabilidade de transações na blockchain e a adoção de políticas e prevenção a ilícitos no ecossistema

Por Laelya Longo, Valor Investe — São Paulo

18/10/2023 09h10 - Atualizado há 2 horas



Palestinos seguram bandeira da Hamas na Faixa de Gaza — Foto: AP Photo/Bilal Hussein

Além da indignação e do horror provocado pelo ataque do grupo terrorista Hamas contra Israel, uma outra discussão veio à tona: o uso das criptomoedas para o financiamento de atividades criminosas. Nos últimos dias, a imprensa internacional publicou declarações do governo israelense de que teria identificado carteiras digitais que seriam ligadas a membros do Hamas e bloqueado seus recursos em criptoativos.

Em torno desses eventos, o paradoxo do ecossistema cripto: o (falso) anonimato por trás de identidades alfanuméricas e a rastreabilidade de todas as transações realizadas em uma blockchain, a rede de dados criptografados, imutáveis e públicos. E, nesse cenário, a crescente institucionalização desse mercado, com o aumento da regulamentação oficial e a consequente adoção de políticas e ferramentas de prevenção à lavagem de dinheiro e financiamento ao terrorismo (PLD/FT).

Em entrevista ao portal especializado CoinDesk, Yaya Fanusie, ex-funcionário da CIA (o serviço de inteligência americano), que acompanha o financiamento do terrorismo por meio de criptos desde 2016, atualmente diretor de política de prevenção à lavagem de dinheiro (PLD) no Crypto Council for Innovation, afirmou que “criptos estão longe de ser um bilhete premiado para quem quer arrecadar recursos secretamente”.

“Na verdade, pode ser exatamente o oposto”, ressaltou Fanusie. “A natureza pública das blockchains e dos endereços de carteiras digitais expõe o financiamento do terrorismo ao escrutínio.” Para ele, o doador a um grupo criminoso “é burro o suficiente” para achar que não pode ser descoberto por um sistema de segurança.

Veículos de imprensa ao redor do mundo especularam quanto o Hamas teria arrecadado em criptos para financiar seus ataques a Israel. O Wall Street Journal publicou que seriam US\$ 40 milhões utilizados na ofensiva que matou milhares de israelenses.

A agência de notícias alemã Deutsche Welle publicou que, entre agosto de 2021 e junho de 2023, o Hamas teria recebido US\$ 41 milhões em criptomoedas, citando dados da empresa de análise de criptofinanças BitOK, sediada em Tel Aviv. Entre as criptos transacionadas estariam bitcoin, a maior em valor de mercado, atualmente em US\$ 28 mil, tether, a maior “cripto de dólar”, e até dogecoin (que é uma memecoin, isto é, foi criada por diversão).

As campanhas de arrecadação do Hamas foram públicas: começaram e terminaram no Telegram. Em 2019, membros do grupo pediram doações em bitcoin e publicaram o endereço da carteira digital. Em abril de 2023, a ação foi inversa: solicitaram a suspensão do envio de recursos, justamente porque as transações estavam sendo rastreadas e os colaboradores, identificados.

Felipe Medeiros, analista de criptomoedas e sócio da Quantzed Criptos, casa de análise e empresa de tecnologia e educação financeira para investidores, explica que as exchanges possuem o cadastro de seus clientes, “então é muito fácil de bloquear” recursos de carteiras digitais.

De acordo com o Financial Times, em reportagem publicada nesta terça-feira (17), mais de 100 contas teriam sido congeladas na Binance, a maior plataforma de negociação de criptomoedas do mundo, a pedido do governo israelense. Informações de outras 200 contas teriam sido solicitadas.

Em posicionamento enviado ao Valor Investe, a exchange afirmou que, “como sempre, a Binance segue as regras de sanções reconhecidas internacionalmente, bloqueando o pequeno número de contas vinculadas a fundos ilícitos”.

Ainda segundo o comunicado oficial, “nos últimos três anos, a Binance atendeu mais de 103 mil solicitações de aplicação da lei com um tempo de resposta médio de três dias, que é mais rápido do que a maioria das instituições financeiras tradicionais”. “Só entre janeiro e setembro de 2023, a equipe de Inteligência e Investigações da Binance respondeu a mais de 40 mil pedidos de informações de autoridades”, conclui a nota.

Na segunda-feira, a Tether, empresa emissora da cripto de mesmo nome, informou que congelou 32 endereços, contendo US\$ 873 mil em criptos, “que foram considerados vinculados a atividades ilícitas em Israel e na Ucrânia”. “Tether tem trabalhado com a NBCTF [órgão do governo em Israel para combater o terrorismo e a guerra financiados por criptomoedas]”, destaca o comunicado.

Ainda na nota, a emissora ressalta que “até o momento, a Tether ajudou 31 agências em todo o mundo com investigações em 19 jurisdições, congelando um total de US\$ 835 milhões em ativos principalmente associados a roubo (hacks de blockchain e exchanges), com uma pequena parcela a outros crimes”.

Por não ser uma exchange, surgiu a dúvida de como uma emissora de criptomoeda teria mecanismos para identificar e congelar carteiras digitais.

Medeiros explica que os emissores de criptos pareadas a ativos reais, as chamadas stablecoins, como tether (pareada ao dólar), “têm acesso ao rastro que esse dinheiro deixa em blockchain, que pode ser acompanhado desde a movimentação da carteira até alguns envios para exchanges, saques e envios para outras carteiras”.

Ele explica ainda que essas carteiras não são bloqueadas especificamente, mas “marcadas”. “Quando a Tether disse que bloqueou uma carteira, na verdade, ela marcou essa carteira, pois não tem o poder de bloquear dentro da blockchain”, ressaltou Medeiros. “Essa carteira entra em uma ‘blacklist’ e todas as plataformas centralizadas e descentralizadas não interagem com ela, passando a ter muita dificuldade ou até impossibilidade completa de se desfazer das stablecoins e converter em moeda fiduciária”, aponta.

“A criptomoeda é uma ferramenta poderosa, mas não é uma ferramenta para o crime”, afirmou Paolo Ardoio, presidente da Tether, no comunicado. “Ao contrário da crença popular, as transações com criptomoedas não são anônimas; eles são os ativos mais rastreáveis existentes. Cada transação é registrada na blockchain, tornando viável para qualquer pessoa rastrear movimentos de fundos. Consequentemente, criminosos tolos o suficiente para empregar criptomoedas para atividades ilegais serão inevitavelmente identificados.”

O amadurecimento do mercado cripto, com uma maior adoção institucional e regulamentações oficiais sendo implementadas, tem aumentando a adoção de políticas e ferramentas de prevenção à lavagem de dinheiro e financiamento ao terrorismo (PLD/FT).

O Grupo de Ação Financeira contra a Lavagem de Dinheiro e o Financiamento do Terrorismo (Gafi/FATF), criado no âmbito da Organização para a Cooperação e o Desenvolvimento Econômico (OCDE), estabeleceu 40 recomendações que seus países-membros devem implementar para desenvolver e

promover políticas de combate a atividades ilícitas por meio de transações financeiras e comerciais locais e transfronteiriças.

Periodicamente, o Gafi realiza avaliação dos países membros acerca da implementação dessas recomendações e atribui uma “nota” para a saúde e a integridade do sistema financeiro relacionado a esses crimes, elaborando uma lista de países menos seguros que são monitorados e outra com as “jurisdições de alto risco”. A avaliação deste ano, manteve Irã, Coreia do Norte e Mianmar nessa última categoria.

No ano passado, o Gafi atualizou suas recomendações, incluindo os prestadores de serviços de ativos virtuais, os chamados VASPs, na sigla em inglês. Entre as ferramentas do mundo tradicional que foram levadas para o mercado cripto está a chamada abordagem baseada no risco (ABR), uma metodologia de análise individual de perfil e comportamento que permite identificar transações suspeitas. Entre os processos dessa metodologia está o KYC, Conheça Seu Cliente, que identifica e traça o potencial de risco de pessoas físicas e jurídicas.

“O pilar fundamental de prevenção à lavagem de dinheiro e ao financiamento do terrorismo é conhecer o cliente e as contrapartes de uma transação financeira, no jargão: know your client ou KYC”, ressalta Mariana Tumbiolo, sócia do Madruga BTW Advogados e especialista em PLD. “Instituições reguladas são obrigadas a checar diariamente listas restritivas, de forma a prevenir que sejam realizadas operações com pessoas suspeitas de terrorismo ou seu financiamento.”

Mariana aponta que “a descentralização e a rapidez das operações com criptoativos, assim como a não identificação dos reais detentores das carteiras virtuais, podem facilitar o mau uso do sistema para financiamento do terrorismo”.

“As corretoras de criptoativos [exchanges] são o principal ponto de contato entre as moedas tradicionais e as moedas virtuais”, afirma a especialista. “Como tal, elas devem desempenhar um papel importantíssimo de verdadeiras ‘guardiãs’ do sistema financeiro, buscando evitar que as transações sejam utilizadas para fins ilícitos.”

No Brasil, pontua Mariana, o marco legal dos criptoativos (Lei 14.478/22) determina que as VASPs sejam incluídas no rol de sujeitos obrigados às regras de prevenção à lavagem de dinheiro. “Nesse contexto, de extrema importância é a publicação de regulação pelo Banco Central, que detalhe essas obrigações, diminuindo uma preocupante lacuna no sistema.”

Para a advogada Fernanda Tórtima, sócia do Tórtima, Galvão & Maranhão Advogados, o fato de o Banco Central “ainda não ter editado as normas específicas, relativas ao funcionamento e aos deveres a serem observados por essas plataformas, dificulta, senão inviabiliza, ao menos no Brasil, a fiscalização eficiente de suas operações e eventuais sancionamentos em caso de infrações”.

Segundo Fernanda, há normas gerais editadas pelo Conselho de Controle de Atividades Financeiras (Coaf), que, “em tese, se aplicariam a qualquer instituição que tenha como atividade a intermediação e aplicação de recursos de terceiros. Mas, por falta de regulamentação específica, as operações com criptomonedas só passam a ter efetivos instrumentos de PLD e KYC quando os valores delas decorrentes entram no sistema financeiro tradicional”.

[< Mais recente](#)

[Próxima >](#)

Agora o Valor Econômico está no WhatsApp!

Siga nosso canal e receba as notícias mais importantes do dia! [CONHECER >](#)

Recomendadas para você

Empresas



Entenda por que Felipe Neto não afetou as ações da Mondelez, dona da Bis

Mundo



Ataque em hospital na Faixa de Gaza pode ter matado mais de 500 pessoas; Israel e Jihad negam autoria

Carreira



Homem mais rico de Israel deixa Harvard após polêmica sobre guerra

Brasil



Receita, PF e PGFN deflagram Operação Sucata contra grupo empresarial com R\$ 5 bi em autuações

Comentários