Criptomoedas e investigação do branqueamento de capitais

Federico Paesano
Especialista senior de investigação financeira

Tem sido uma viagem incrível até agora. Ouvi falar da Bitcoin pela primeira vez em 2010, numa conferência sobre cibercrime. Ainda não sabíamos muito, exceto que se tratava de uma nova forma de dinheiro - completamente descentralizada, uma vez que não era emitida ou controlada por nenhum governo - e que tinha o potencial de ajudar os criminosos a movimentar e branquear os seus lucros através das fronteiras sem serem detetados.

Como pode o dinheiro ser descentralizado? Podem os criminosos converter os seus fundos ilícitos em bitcoins e depois em moeda fiduciária? Será o fim do jogo para as agências de aplicação da lei se a adoção da Bitcoin crescer exponencialmente? Estas eram as nossas perguntas na altura.

A resposta à última pergunta parecia ser um grande "sim", uma vez que a atividade criminosa tinha começado a ser detetada neste domínio e parecia ainda impossível investigar os fluxos de criptomoeda na cadeia de blocos. A utilização da Bitcoin parecia ser a derradeira ferramenta de anonimato.

Cada vez mais atenção

Quando o Basel Institute on Governance decidiu sentar-se à mesa com a Organização Internacional de Polícia Criminal (INTERPOL) e a Agência da União Europeia para a Cooperação Policial (Europol) em 2014, o tema era um nicho muito pequeno.

Na altura, existia apenas uma criptomoeda, a Bitcoin, um único caso para ser analisado, a Rota da Seda (*Silk Road* em inglês) e apenas 20 pessoas numa pequena sala na Universidade de Basileia. Não obstante, decidimos fundar conjuntamente um grupo de trabalho sobre criptomoedas e branqueamento de capitais. Sentimos que algo importante estava a acontecer e que as autoridades tinham de estar aptas a enfrentar o desafio.

Mas que mudança em apenas alguns anos! Hoje em dia, milhares de pessoas inscrevem-se na nossa Conferência Mundial anual sobre Delitos Financeiros e Criptomoedas. Existem centenas de novas criptomoedas e outras formas inovadoras de activos virtuais - tais como *tokens* não fungíveis (*NFT* na sua sigla inglesa) e moedas digitais de bancos centrais - e cada vez mais casos de branqueamento de capitais estão a obrigar os investigadores a mergulhar na "cripto-esfera".

Os organismos reguladores a nível mundial também estão a levar esta questão mais a sério. O Grupo de Acção Financeira (GAFI), o guardião que fiscaliza o branqueamento de capitais a nível mundial, actualizou as normas e orientações sobre activos virtuais e prestadores de serviços de activos virtuais (VASP na sua sigla inglesa), e tem estado a acompanhar de perto a evolução dos diversos países em matéria de cumprimento normativo.

E em junho de 2023, a União Europeia adotou a estrutura regulatória mais abrangente para ativos digitais até o momento: o Regulamento de Mercados de Ativos Criptográficos (MiCA).

Que tipo de crime utiliza criptomoedas?

As criptomoedas têm inúmeros usos e benefícios legítimos, incluindo a possibilidade de oferecer um sistema de pagamento internacional barato, rápido e acessível a milhões de pessoas que vivem actualmente em zonas não cobertas pelo sistema bancário pelo mundo fora. Mas, como qualquer reserva de valor, podem ser utilizadas indevidamente.

Alguns processos envolvem criminosos que utilizam criptomoedas para branquear os "habituais" proventos do crime ou corrupção. Um simples exemplo é um funcionário corrupto que recebe subornos e tenta ocultar a origem do dinheiro através da transferência de dinheiro de e para várias criptomoedas e moedas fiduciárias, tais como o dólar.

Na sua maioria, porém, trata-se de crimes que geram lucros em criptomoedas. Tal como referido na Avaliação da Ameaça da Criminalidade Organizada dinamizada pela Internet (iOCTA) da Europol, as criptomoedas são utilizadas para facilitar os pagamentos de diversos tipos de actividades ilícitas.

Entre estas incluem-se o tráfico de droga e o comércio de outros bens ilícitos na *dark web* (parte obscura da internet), o *software* de sequestro de dados *(ransomware)* como o Rhysidia o Abyss, o pagamento de raptos e resgates, e a cibercriminalidade.

Seguir o percurso do dinheiro virtual, mais fácil nalguns aspectos, mais difícil noutros

Teoricamente, as tecnologias de cadeia de blocos (blockchains) por detrás das criptomoedas facilitam a tarefa dos investigadores financeiros de "seguir o rasto do dinheiro". Porquê?

Porque cada transacção é registada de forma imutável num livro-razão partilhado - a cadeia de blocos - o qual não pode ser posteriormente alterado ou falsificado. Teoricamente, o rasto do dinheiro fica lá registado para sempre, pronto para servir de prova mesmo anos mais tarde.

A recente acusação de um indivíduo que roubou mais de 50 000 bitcoins da extinta bolsa de criptomoedas MtGox em 2012 ilustra claramente este processo. A imutabilidade da cadeia de blocos permitiu aos investigadores seguir o rasto do dinheiro, identificar o culpado e recuperar ativos no valor recorde de 3,36 mil milhões de dólares quase dez anos após o facto.

O mesmo não se aplica, por exemplo, às transacções em numerário. É impossível voltar atrás no tempo e ver quem deu o quê a quem.

As transacções em bitcoin incluem a data e o montante da transacção, bem como os endereços do remetente e do destinatário (pseudónimos sob a forma de longas cadeias de caracteres alfanuméricos). Em contrapartida, duas criptomoedas de menor dimensão – por exemplo Monero – apostam no anonimato.

A parte mais complexa em todos os processos é a *atribuição,* ou seja, estabelecer uma ligação entre transacções e endereços a pessoas reais no mundo real. Por outras palavras, identificar actividades potencialmente criminosas e transacções conexas e os criminosos que estão por detrás delas.

Quebrar o escudo do anonimato

Felizmente para os investigadores, existem técnicas capazes de penetrar o aparente anonimato das criptomoedas, permitindo estabelecer uma relação entre transacções e endereços a presumíveis criminosos e branqueadores de capitais.

Por exemplo, a heurística pode ser utilizada para criar agrupamentos *(clusters)*, ou seja, grupos de endereços que muito provavelmente são controlados pela mesma entidade. São então aplicadas técnicas especiais para que esses agrupamentos percam o seu anonimato.

É neste âmbito que as empresas de análise de cadeia de blocos podem dar a sua contribuição. Mediante o pagamento de honorários, podem analisar endereços e transacções para obter informações cruciais, tais como dados de geolocalização ou a bolsa de criptomoedas utilizada para comprar as moedas.

Em seguida, os investigadores podem solicitar mais pormenores à bolsa, tal como fariam a um banco ou a outro prestador de serviços de pagamento. Uma vez que as normas acima mencionadas do GAFI sobre os VASP são implementadas através da legislação nacional, esperamos e contamos que dados mais fiáveis sobre os seus clientes possam ser disponibilizados às autoridades competentes.

O custo de recorrer a uma empresa de análise de cadeia de blocos poderá ser um obstáculo em países com recursos limitados no que diz respeito à aplicação da lei.

Contudo, na realidade, a maioria das investigações que envolvem criptomoedas começam com um suspeito, e não com uma transacção misteriosa ou um endereço anónimo. Os investigadores apenas tentam descobrir que endereços de criptomoedas são controlados pelo suspeito. Muitas vezes, esta informação pode ser revelada através da análise forense dos dispositivos do suspeito, sem necessidade de consultar uma empresa de análise de cadeia de blocos.

Processos judiciais - por que razão as testemunhas periciais são úteis

A natureza relativamente nova e de rápida evolução dos activos virtuais significa que as tecnologias de cadeia de blocos, tais como as criptomoedas, são no geral pouco conhecidas.

Isto é válido para os agentes da autoridade e para as autoridades judiciárias, que podem ter de interpretar provas da análise de cadeia de blocos ou carteiras digitais, a fim de condenar um suspeito.

Neste caso, é útil convocar uma testemunha pericial para esclarecer e verificar as referidas provas em tribunal. É evidente que uma explicação clara das diligências de investigação empreendidas também ajudará a demonstrar ao tribunal que a prova daí resultante é igual a qualquer outra prova de crime financeiro.

Recuperação de activos roubados detidos em criptomoeda

Os activos detidos em criptomoeda podem ser tratados exactamente como os activos detidos em contas bancárias ou bens imóveis. Por exemplo, um juiz pode emitir uma ordem de congelamento de activos numa conta em criptomoeda, enquanto se aguarda o resultado do processo.

Dado que as transacções em criptomoeda podem ser feitas em apenas alguns minutos, a cooperação internacional em matéria de congelamento de activos precisa de ser efectivamente mais célere. O tempo que demora para emitir uma ordem de congelamento, mesmo quando se trata de transferências bancárias normais, dá tempo para que o dinheiro circule várias vezes pelo mundo.

Quando se trata de confiscar e recuperar activos detidos em criptomoedas, as autoridades - que ainda utilizam moedas fiduciárias nacionais, apesar de não se saber o que o futuro reserva - têm algumas opções.

- Uma delas é transferir a criptomoeda para a moeda fiduciária em causa, por meio de troca.

- Outra é a realização de um leilão. O Departamento de Justiça dos EUA recuperou quase 50 milhões de dólares americanos através de um leilão de moedas fiduciárias ilícitas, após o encerramento do mercado *online* da Silk Road em 2013.

A volatilidade do valor das criptomoedas é uma dor de cabeça para os responsáveis pela recuperação de activos. As 144.336 bitcoins vendidas em 2013 nos leilões da Rota da Seda, teriam gerado hoje cerca de 4.2 mil milhões de dólares americanos.

O que podem fazer os responsáveis pela aplicação da lei?

Na 6.ª Conferência Global sobre Criptomoedas e Financiamento Criminal de 2022, co-organizada pelo Instituto de Basileia e pela EUROPOL, e que contou com a presença de mais de 2000 participantes presenciais e remotos, emergiram dos debates cinco recomendações fundamentais.

1. **Quebrar os silos entre "tradicional" e "cripto"** – não tratar a criptografia como uma área separada, mas operar nos domínios físico e virtual (como fazem os criminosos).

2. **Regulamentar amplamente e fazer pleno uso das leis existentes** – para garantir que os cripto-ativos sejam tratados como qualquer outro ativo para fins de supervisão AML/CFT, aplicação e recuperação de ativos.

3. **Aproveitar a cadeia de blocos para desmantelar a criminalidade organizada** – uma vez que a cadeia de blocos oferece inúmeras oportunidades para investigar e desmantelar esquemas criminosos e de branqueamento de capitais, recolher informações e congelar e confiscar ativos ilícitos.

4. **Aumentar a literacia em matéria de criptomoeda através do reforço das capacidades e de uma comunicação clara** – eliminando o jargão e os acrónimos e alargando a formação básica em matéria de criptomoeda a grupos mais vastos de funcionários.

5. **Aumentar a cooperação público-privada** – uma vez que as autoridades responsáveis pela aplicação da lei podem beneficiar muito das competências técnicas das empresas de rastreio de activos e de análise de cadeias de blocos, bem como cooperar com os prestadores de serviços de criptoativos para acelerar as ordens de congelamento de contas e a partilha de informações.

Publicado originalmente em inglês a 15 de março de 2019 e actualizado a 11 de agosto de 2023.
Todos os nossos guias rápidos estão disponíveis em learn.baselgovernance.org

ISSN 2673–5229

Basel Institute on Governance
Steinenring 60
4051 Basel, Switzerland

+41 61 205 55 11
info@baselgovernance.org
baselgovernance.org

@BaselInstitute
Basel Institute

The Basel Institute on Governance is an Associated Institute of the University of Basel