



Criptomoedas e investigação do branqueamento de capitais



Federico Paesano
Senior Financial Investigation Specialist

Foi em 2014, quando comecei a falar com os meus homólogos da INTERPOL e Europol sobre criptomoedas e branqueamento de capitais, que este tópico começou a ocupar um pequeno nicho.

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.

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 um aumento em flecha do número de casos de branqueamento de capitais que exigem que os investigadores entrem na criptosfera.

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.

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 WannaCry, o pagamento de raptos e resgates, e a cibercriminalidade.

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

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.

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 – Monero e Zcash – 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 Rota da Seda 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 6 mil milhões de dólares americanos.

O que podem fazer os responsáveis pela aplicação da lei?

Durante a 4ª Conferência Mundial anual sobre Delitos Financeiros e Criptomoedas em 2020, que foi organizada pela INTERPOL no ciberespaço devido às restrições da pandemia, emergiram dos debates sete recomendações de importância fundamental.

Em suma, já se vêem progressos, mas os responsáveis pela aplicação da lei ainda têm um longo caminho pela frente.

Uma abordagem multidisciplinar

Por exemplo, a Recomendação 5 incentiva os investigadores a adoptarem uma abordagem multidisciplinar, fomentando a criação de equipas de investigação conjuntas que associam áreas como investigação financeira, cibercriminalidade e conhecimentos técnicos de TI/análise forense.

No entanto, ainda há muitos investigadores que não recorrem a especialistas com este tipo de conhecimentos, e as suas instituições não organizam regularmente uma investigação multidisciplinar, nem reúnem equipas de recuperação de activos. Deveriam fazê-lo.

Novas tecnologias

De igual modo, a Recomendação 6 promove a utilização de novas tecnologias no âmbito da investigação financeira de activos virtuais.

Os governos devem apoiar a investigação e inovação de instrumentos que facilitem a investigação e prevenção do branqueamento de capitais e do financiamento do terrorismo através da utilização de criptomoedas.

Actualmente, este trabalho está a ser feito essencialmente por empresas privadas, que depois cobram honorários pelos serviços prestados às autoridades.

Estratégias de investigação

Por último, é preciso ter presente que as criptomoedas são utilizadas por pessoas reais no mundo real. A Recomendação 7 do ano passado, no sentido de adaptar as estratégias de investigação, inclui, por exemplo, a procura sistemática de dispositivos ou documentos nas instalações dos suspeitos, que possam conter detalhes de contas em criptomoeda.

À medida que a utilização de criptomoedas aumenta em todo o mundo, o rastreio de transacções através da criptosfera tem de se tornar uma prática rotineira por parte dos investigadores. Para isso, os nossos agentes responsáveis pela aplicação da lei precisam de melhorar rapidamente as suas competências.

Publicado originalmente em inglês a 15 de Março de 2019 e actualizado a 6 de Agosto de 2021
Todos os nossos guias rápidos estão disponíveis em learn.baselgovernance.org

ISSN 2673-5229

Esta obra está licenciada sob uma Licença Creative Commons Atribuição-Não-comercial-NoDerivs 4.0 Internacional (CC BY-NC-ND 4.0).

