Bitcoin e lavagem de dinheiro: como as criptomoedas podem revolucionar o crime de lavagem de dinheiro

Lucas Miranda

Mestrando e Graduado em Direito pela Universidade Federal de Minas Gerais. Advogado. ORCID: 0000-0002-9682-1115
lucasmiranda@tuliovianna.adv.br

Túlio Vianna

Pós-Doutor em Direito pela Università Di Bologna. Doutor em Direito Pela UFPR. Professor de Direito Penal da Faculdade de Direito da UFMG. Advogado.
ORCID: 0000-0002-8002-3960
tuliovianna@tuliovianna.adv.br

Recebido em: 18.07.2019
Aprovado em: 06.10.2019
Última versão dos autores: 11.10.2019

Áreas do Direito: Penal; Digital

Resumo: O presente trabalho tem como objetivo analisar os novos métodos de lavagem de dinheiro no paradigma das criptomoedas, especialmente através do *Bitcoin*. Para essa finalidade, realizou-se uma pesquisa acerca do funcionamento desta criptomoeda, expondo, de forma simplificada, sua tecnologia. Seguidamente, analisa-se alguns aspectos do tipo penal de lavagem de dinheiro relevantes no ambiente virtual. O ponto central do trabalho é a investigação das novas tipologias de lavagem de capitais resultantes do advento das criptomoedas. Por fim, procura-se refletir sobre possíveis modificações legislativas para fomentar o sistema brasileiro de prevenção à lavagem de dinheiro. Ressalta-se que as

Abstract: This article aims to analyze the new methods of money laundering in the cryptocurrency paradigm, especially through Bitcoin. For this purpose, an investigation will be carried out on the Bitcoin operation, exposing its technology in a simplified manner. Next, we discuss some relevant aspects of money laundering in the virtual environment. The central point of the work is the investigation of the new typologies of money laundering resulting from the advent of cryptocurrencies. Lastly it is sought to evaluate proposals for legislative changes to promote the Brazilian system of prevention of money laundering. We concluded that cryptocurrencies characterize a relevant social change of the 21st

Miranda, Lucas; Vianna, Túlio. *Bitcoin* e lavagem de dinheiro: como as criptomoedas podem revolucionar o crime de lavagem de dinheiro. *Revista Brasileira de Ciências Criminais*. vol. 163. ano 28. p. 265-309. São Paulo: Ed. RT, janeiro 2020.

criptomoedas caracterizam uma modificação social relevante do século XXI e que, a despeito dos benefícios da sua utilização, a facilidade de sua aplicação no crime de lavagem de dinheiro manifesta a necessidade de modernização da legislação brasileira.

PALAVRAS-CHAVE: Criptomoedas – *Bitcoin* – *Blockchain* – Lavagem de Dinheiro – Prevenção.

century and that, despite the benefits of its use, the ease of its application in the crime of money laundering manifests the need for modernization of Brazilian legislation.

KEYWORDS: Cryptocurrencies – Bitcoin – Blockchain – Money laundering – Prevention.

1. INTRODUÇÃO: CONTEXTO E APRESENTAÇÃO DO TEMA-PROBLEMA

No dia 15 de setembro de 2008, o Lehman Brothers, quarto maior banco de investimento dos Estados Unidos, registrou pedido de falência após 158 anos de atuação no setor financeiro norte-americano. Esse evento, conhecido como o ápice da crise econômica internacional de 2008, poderia ter se espalhado por diversas companhias multinacionais se os países atingidos não houvessem optado pela injeção de dinheiro público no setor privado. Independente da análise da eficiência dessa medida, um número considerável de contribuintes se sentiu desconfiado, questionando a legitimidade de governos aplicarem dinheiro público dessa maneira.

O monopólio estatal sobre a moeda era, até então, um paradigma global. Esse cenário permitia que governos elaborassem políticas econômicas que atingissem o poder de compra de toda a população sem necessariamente contar com a sua participação. Entretanto, exatamente 150 dias após o auge da crise econômica, no dia 11 de fevereiro de 2009, um indivíduo – ou um grupo de indivíduos –, sob o pseudônimo de Satoshi Nakamoto, publicou no fórum *P2P Foundation*[1] um novo sistema de transação de ativos completamente independente de bancos ou

1. Disponível em: [http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source]. Acesso em: 11.05.2018.

governos, caracterizando o que muitos consideram a maior invenção desde a *internet*. Este é apontado como o dia do nascimento do *Bitcoin*[2].

Influenciado pelo movimento *cypherpunk*[3], Nakamoto explicitou no fórum seu descontentamento com as entidades financeiras, afirmando que "a raiz do problema das moedas convencionais é a confiança necessária para o seu funcionamento"[4] (tradução livre). Como solução, afirmou ter desenvolvido um sistema descentralizado, sem intermediação de terceiros, em que as transações são realizadas diretamente entre dois indivíduos e sua confiabilidade é baseada em um livro de registro que pode ser acessado por qualquer pessoa.

Em um artigo publicado em 2008, Nakamoto já havia demonstrado as bases para a criação do *Bitcoin*. Descreveu o sistema como "uma forma de dinheiro eletrônico capaz de propiciar que pagamentos *online* sejam enviados diretamente de uma parte a outra sem passar por uma instituição financeira[5]" (tradução livre). Interessante observar que no trabalho Nakamoto utilizou a palavra *cash*, que em português significaria "dinheiro em espécie". Na realidade, é exatamente essa a característica principal do *bitcoin*, ser um objeto de troca muito semelhante ao papel moeda, mas no ambiente virtual.

Até a ascensão dessa tecnologia, todas as transações *on-line* eram realizadas por intermédio de um terceiro que conferia e validava as operações. Empresas como MasterCard, Visa, PayPal, realizam essa função mantendo um registro da identidade de seus clientes e dos valores em suas contas. Quando um indivíduo pretende enviar dinheiro para outro, o intermediário verifica e registra a transação, modificando o saldo disponível na conta de cada um.

Essa metodologia sempre foi necessária para evitar que o dinheiro, no ambiente virtual, fosse gasto duas vezes. Como explica Fernando Ulrich (2017, p. 18),

2. Utilizar-se-á no presente trabalho a palavra *Bitcoin*, grafada com a primeira letra em maiúsculo, para se referir ao protocolo que propicia a troca de moedas. A palavra com grafia em minúsculo, por sua vez, será utilizada para se referir à moeda em si.
3. O termo *cypherpunk*, de acordo com Hughes (1997), diz respeito a um movimento que combina ideias do movimento *cyberpunk*, como o espírito do individualismo no ciberespaço, com o uso de criptografia, a fim de proporcionar o desenvolvimento de programas e sistemas que garantam a privacidade na *internet*.
4. "The root problem with conventional currency is all the trust that's required to make it work". Disponível em: [http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source]. Acesso em: 11.05.2018.
5. "A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution" (NAKAMOTO, 2008, p. 1).

se o dinheiro eletrônico for um simples arquivo, assim como qualquer documento digital no computador, nada impediria que um indivíduo enviasse esse arquivo para outro mantendo uma cópia em seu computador. Essa situação permitiria que, posteriormente, o mesmo arquivo fosse enviado pelo primeiro indivíduo a um terceiro, caracterizando o gasto duplo. Por óbvio, um sistema que permitisse esse acontecimento não gozaria da segurança ou da confiabilidade necessária para se firmar como meio de troca.

O grande mérito de Nakamoto foi resolver essa questão sem a necessidade de um órgão central de fiscalização. Utilizando-se da criptografia e de um livro de registros público, o *Bitcoin* possibilitou que qualquer usuário pudesse participar do processo de verificação da validade da transação, tornando, assim, a moeda descentralizada (ULRICH, 2017, p. 18).

Além da ausência de intermediário, uma transação de *bitcoins* se assemelha a uma de dinheiro em espécie em outros pontos. Primeiramente, assim como quando um indivíduo entrega uma cédula para outro, a operação pelo protocolo, uma vez realizada, não pode ser suspensa, interrompida ou revertida. Aquele que recebeu os *bitcoins* pode devolvê-los, no entanto, essa será outra operação, e não a reversão da primeira.

Para a realização de uma transação desta criptomoeda também não é necessário que uma parte tenha conhecimento da identidade da outra. O proprietário de uma cafeteria, por meio do pagamento em espécie, pode vender uma xícara de café para um indivíduo completamente desconhecido sem ter dúvidas da validade da transação – bastando, para isso, conferir os elementos de segurança das cédulas entregues. A mesma situação ocorre com a transação de *bitcoins*. Como a operação é irreversível e o método de conferência da validade da moeda recebida é seguro, não há necessidade de se verificar ou armazenar os dados do cliente, como ocorre, por exemplo, em pagamentos por cheque.

Atualmente, qualquer indivíduo pode comprar, vender ou realizar pagamentos por meio de *bitcoins* sem precisar se identificar. A criação de uma carteira eletrônica de *bitcoins*[6] é comumente classificada como "pseudo-anônima"[7]

6. A carteira eletrônica um *software* que permite o armazenamento de *bitcoins* para posterior utilização.

7. De acordo com PFITZMANN e KÖHNTOPP (2001, p. 5), pseudônimos são designações identificáveis de um indivíduo ou um grupo de indivíduos na rede. Enquanto a anonimidade significa que o sujeito não é identificável em um conjunto, a pseudo anonimidade é todo o complexo de graus de identificação entre a anonimidade e a identidade. Além disso, como explicam os autores, utilizando-se mais de uma vez de um mesmo

(BURNISKE; TATAR, 2018, p. 85), pois o usuário não precisa disponibilizar sua identificação para criá-la. Como nas contas numeradas da Suíça, não existem nomes conectados às carteiras eletrônicas. No entanto, todas as transações realizadas por elas ficam armazenadas permanentemente no livro de registro, de forma que é possível a qualquer pessoa verificar as transações efetuadas através de determinada carteira (VAN WEGBERG, et al., 2018, p. 421).

Teoricamente, também é possível conseguir associar o endereço do agente com determinada carteira a partir do *Internet Protocol* (*IP*)[8]. No entanto, programas de computador, como o *The Onion Router* (*Tor*) ou o *Windscribe*, garantem um altíssimo nível de sigilo para os usuários. Utilizando diversos computadores ao redor do globo, esses programas permitem que o comando de um dispositivo – por exemplo o acesso ao *Google* – seja enviado aleatoriamente para outros, formando um caminho criptografado antes de chegar ao seu real destino (MCCOY, et al., 2008, p. 64 e DINGLEDINE, et al., 2004). Ao tentar realizar o caminho inverso, somente se chegará ao último computador da rede criptografada utilizada para a efetivação do comando, que poderá estar em qualquer local do planeta, sem nenhuma relação com aquele que emitiu o comando original (TSCHORSCH; SCHEUERMANN, 2016, p. 2101 e VAN WEGBERG, et al, 2018, p. 421).

Por esse motivo diz-se que o *Bitcoin* pode facilmente ser utilizado de maneira anônima. Não havendo como rastrear o endereço correto do computador que envia uma moeda virtual a outro, não será possível constatar o emissor e o destinatário de uma transação, tampouco a origem do dinheiro.

O *Bitcoin*, então, contém o sigilo do papel moeda sem apresentar suas desvantagens operacionais. Assim, por exemplo, dois indivíduos que pretendem realizar uma compra e venda de um artigo de luxo por meio de criptomoedas não terão que lidar com o transporte e armazenamento de um grande volume de cédulas – bastando estar com seus celulares para realizar a transação[9]. Além disso, como as corretoras de *bitcoins* de vários países não são obrigadas a reportar transações financeiras suspeitas para órgãos de fiscalização, e como essa criptomoeda

pseudônimo, o indivíduo pode criar uma reputação, ou seja, um conjunto de atos identificáveis a seu pseudônimo capazes de serem avaliados pelos demais.

8. O *IP* de um usuário de internet é uma identificação única para cada computador conectado à rede. A partir dele é possível rastrear o endereço da conexão.

9. Nesse sentido, explica de forma bem-humorada POPPER (2015, p. 8) ao comparar a criptomoeda ao ouro: "Bitcoin also held certain obvious advantages over gold as a new place to store value. It didn't take a ship to move Bitcoins from London to New York – it took just a private digital key and the click of a mouse."

pode ser capitalizada em praticamente qualquer local do planeta, a capitalização desse ativo e sua reintrodução no sistema financeiro são facilitados.

2. DEFINIÇÃO TERMINOLÓGICA E OBJETO DE ESTUDO

Até julho de 2019, pouco mais de 2600 criptomoedas diferentes estavam em circulação no mundo, com valor de mercado de aproximadamente 268 bilhões de dólares[10]. O *Bitcoin*, sozinho, era responsável por capitalizar mais de metade desse valor. Esses números explicitam a força e a aceitação que as criptomoedas vêm demonstrando nas sociedades atuais.

Para entender esse contexto, primeiramente deve-se atentar aos conceitos e tentar esclarecer as diferenças entre moedas eletrônicas e moedas virtuais.

As moedas eletrônicas – ou dinheiro eletrônico – são valores, correspondentes à moeda corrente em determinado país, armazenados por meios eletrônicos, como um dispositivo móvel ou o *chip* de um cartão[11]. Um cartão recarregável utilizado em transporte público, por exemplo, é uma forma de moeda eletrônica[12].

Moeda virtual, por sua vez, é um termo que diz respeito a um objeto sem correspondência com qualquer equivalente material, que pode ser utilizado como meio de troca em ambientes específicos (SILVEIRA, 2018, p. 93). Até o início desta década, as moedas virtuais eram quase exclusivamente criadas e operadas por empresas produtoras de jogos *on-line*, servindo para a compra e venda de

10. Dados disponíveis em: [https://br.investing.com/crypto/]. Acesso em: 17.07.2019.

11. A Lei 12.685/13 define em seu artigo 6º, inciso VI, a moeda eletrônica como "recursos armazenados em dispositivo ou sistema eletrônico que permitem ao usuário final efetuar transação de pagamento".

12. Explicitou o Banco Central do Brasil (2014, p. 20): "Electronic money, ou e-money, é valor armazenado eletronicamente em um dispositivo, como um chip de um cartão, um computador pessoal ou servidor ou um dispositivo móvel pessoal (celular, por exemplo), que apenas pode ser transferido entre agentes econômicos, eletronicamente. Pertencem a essa categoria os cartões utilizados nos transportes públicos, os gift cards (cartões de presente), os cartões de alimentação ou refeição e os cartões pré-pagos de pedágio". No mesmo sentido, explica Carla Veríssimo de Carli (2006, p. 126), "são elas [moedas virtuais], por exemplo, os cartões com valor acumulado ou depositado – *stores valued devices* – que permitem a 'carga' de um determinado valor no cartão, o qual pode ser usado para compras, pagamentos e transferências de dinheiro via *internet*. É o caso do *Paypal*, sistema criado há seis anos apenas em uso corrente nos Estados Unidos da América, em alguns países da Europa e na China".

itens também virtuais almejados pelos jogadores. Nesse sentido, podem-se citar como exemplos o *Linden Dollar*[13], utilizado no jogo *Second Life*, e o *gold* do jogo *World of Warcraft* (EUROPEAN CENTRAL BANK, 2012, p. 10).

Apesar da maioria dessas moedas poder ser comprada e vendida através de dólares americanos nos *sites* dos jogos, elas nunca excederam, ao menos de forma expressiva, o relativamente pequeno círculo dos *gamers*.

As criptomoedas, por sua vez, são uma espécie do gênero moeda virtual que nasceu a partir da tecnologia apresentada por Nakamoto. A grande diferença dessas é o fato de utilizarem de criptografia assimétrica para descentralizar o sistema de verificação de transações[14] (STELLA, 2017, p. 151). Essa característica possibilitou sua independência perante as empresas produtoras de jogos e, consequente, a expansão da sua utilização. Hoje em dia, já há quem reconheça as criptomoedas como moedas fiduciárias[15] (ULRICH, 2014, p. 84).

Por ser a criptomoeda mais antiga em circulação e a mais utilizada, bem como por sua preponderância no cenário acadêmico e midiático, o presente trabalho se restringirá às dinâmicas de lavagem de dinheiro no âmbito do *Bitcoin*.

No entanto, deve-se ressaltar que outras criptomoedas, como a *Monero* e a *Zcash*, por utilizarem protocolos de registro que dão ainda mais ênfase à privacidade e ao anonimato que o *Bitcoin*, são consideradas mais propícias para a atividade da lavagem de dinheiro. Apesar do presente trabalho, por delimitação temática, jogar luz somente nas transações que envolvem *bitcoins*, deve-se perceber que o terreno das criptomoedas é fértil e apresenta cada dia mais inovações que merecem ser estudadas também no ramo do Direito.

13. Essa moeda virtual recebeu grande atenção da comunidade acadêmica após percepção da existência, no universo virtual, de comportamentos econômicos similares aos observados na economia americana. A respeito, conferir: ERNSTBERGER, Philip. *Linden dollar and virtual monetary policy*, 2009; STOKES, Robert. *Virtual money laundering*: the case of Bitcoin and the Linden dollar. Information & Communications Technology Law, v. 21, n. 3, p. 221-236, 2012; GLASER, Florian et al. *Bitcoin-asset or currency? revealing users' hidden intentions*, 2014.

14. Trabalhos de língua inglesa também se deparam com a necessidade de adotar uma definição terminológica para esses novos conceitos, como explicam Albuquerque e Callado (2015, p. 15) acerca das diferenças de *digital coins*, *digital currencies* e *virtual coins*.

15. Moedas fiduciárias são títulos que não possuem lastro em metais preciosos, mas podem ser utilizadas como meio de troca, unidade de conta e reserva de valor em decorrência da confiança daqueles que a transacionam em quem emitiu o título (MANKIW, 2015, p. 143).

3. *BITCOIN*: BREVES EXPLICAÇÕES SOBRE SEU FUNCIONAMENTO

Para compreender a dinâmica da lavagem de dinheiro através do *Bitcoin* deve-se entender, pelo menos de forma superficial, o seu funcionamento. A tecnologia por trás do protocolo é moderadamente complexa para indivíduos sem domínio em programação de computadores. O presente trabalho, por ser voltado, prioritariamente, para profissionais do Direito, procurará apresentar essa tecnologia de forma simplificada, utilizando de metáforas e comparações que, para leitores com relativa experiência em programação, podem se mostrar simplórias.

Bitcoin é uma rede de estrutura "ponto a ponto" (*peer-to-peer* ou P2P) que se baseia na tecnologia *blockchain* para criar um sistema de envio de valores diretamente de um usuário a outro. A tecnologia *blockchain*, por sua vez, é o método de funcionamento da estrutura, que utiliza-se de criptografia, assinatura digital, função *hash* e do protocolo de verificação *proof-of-work* para possibilitar transações confiáveis.

Uma rede ser *peer-to-peer*[16] significa que todos os seus usuários interconectados são pares, ou seja, que não há hierarquia entre eles (ANTONOPOULOS, 2014, p. 161). No *Bitcoin*, qualquer computador da rede pode assumir as funções de criar e inscrever transações no livro de registro. Da mesma forma, os usuários têm acesso a essas operações e são capazes de trabalhar para atestar a sua validade. A principal característica do *Bitcoin*, como já dito, é que não existe um servidor central que desempenha a função de registro e validação de transações.

Blockchain, por sua vez, é o que até este ponto do trabalho chamou-se de livro de registro. É um protocolo que exerce a função de manter as informações de todas as transações, computando os créditos e débitos dos usuários (BURNISKE; TATAR, 2018, p. 49). No entanto, o *blockchain* apresenta certas particularidades que lhe diferem dos livros de registro comuns, presentes em estabelecimentos comerciais, por exemplo.

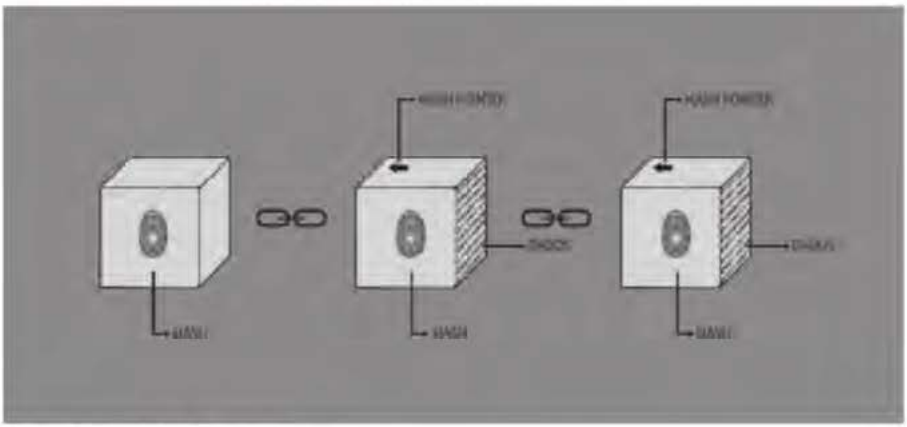
Primeiramente, deve-se mencionar que o *blockchain* é descentralizado, ou seja, todos os usuários do sistema mantêm uma "cópia" dele. Em segundo lugar, como pode-se perceber pelo nome, esse sistema dispõe as informações registradas

16. As primeiras redes construídas com essa arquitetura foram planejadas para disponibilizar arquivos de músicas diretamente entre os usuários. Sobre esse tema, ver a História de Napster. Disponível em: [www.lifewire.com/history-of-napster-2438592]. Acesso em: 13.05.2018.

em forma de cadeia. Cada nova informação será arquivada em ordem cronológica, interligando-se com os dados já armazenados. As informações – que no caso do *Bitcoin* são transações da moeda – são armazenadas em blocos. Para que a informação de um bloco seja considerada válida, ela deve necessariamente corresponder com a do bloco anterior.

Cada bloco contém, além da informação registrada, um número de identificação (*hash*) e a direção do número de identificação do bloco anterior (*hash pointer*). Esse número de identificação, para fins didáticos, pode ser considerado como uma impressão digital. Como essa impressão digital leva em conta o conteúdo do bloco, qualquer modificação em suas informações acarretará sua adulteração.

Figura 1 – Arquitetura do *blockchain*



Fonte: elaborada pelos autores.

Numa abordagem um pouco mais técnica, *hash* é uma função matemática que apresenta três propriedades: a) sua entrada (*input*) pode ser de qualquer ordem de grandeza; b) produz uma saída (*output*) fixa – no caso do *Bitcoin* é de 256-*bits*; e c) é eficientemente computável, ou seja, uma entrada determinada alcançará sempre a mesma saída (NARAYANAN, et. al, 2016, p. 40). Importante, no entanto, é ter em mente que uma pequena modificação no *input* gera um *output* completamente diferente, de forma que qualquer adulteração no bloco gerará uma impressão digital completamente diferente da anterior[17].

17. Mesmo que seja possível que dois valores de *input* diferentes gerem o mesmo *output*, o que se denomina colisão, essa possibilidade é irrisória. Sem entrar nos detalhes matemáticos,

A *hash pointer*, por sua vez, é uma propriedade que liga cada bloco ao anterior. Utilizando da analogia já apresentada, pode-se pensar na *hash pointer* como um pedaço da impressão digital do bloco anterior. Dessa forma, cada bloco que se liga à cadeia, necessariamente preserva uma informação do bloco anterior.

Dessa maneira, qualquer alteração em um bloco poderá ser detectada. Se houver uma modificação, por exemplo, no bloco k, a impressão digital do bloco será completamente diferente da anterior. Consequentemente, o pedaço da impressão digital do bloco posterior ($k + 1$), não será mais compatível com k, acusando uma adulteração (NARAYANAN, et. al, 2016, p. 53).

Pode-se pensar, no entanto, que aquele que modificou um bloco poderia substituir todos os subsequentes para validá-lo. Ocorre que, para adicionar um bloco à cadeia deve-se resolver um "quebra-cabeça" matemático chamado *proof-of-work*. No *Bitcoin*, somente poderá adicionar um bloco à cadeia, aquele usuário que resolver uma função matemática de forma que o resultado – um número binário – inicie-se com um determinado número de *bits* zero. Como a função matemática do *Bitcoin* tem 256-*bits*, para se adicionar um novo bloco à cadeia, o protocolo pode requerer que o usuário tenha que apresentar um *input* que aplicado à função matemática resulte em um *output* cujos primeiros *x bits* sejam zero.

Uma vez que ninguém conseguiu identificar o *input* desta função a partir do *output*, a melhor forma de tentar alcançar o número x de zeros é a tentativa e erro (NARAYANAN, et. al, 2016, p. 49). Portanto, percebe-se que o *proof-of-work* é uma metodologia utilizada para que seja difícil adicionar novos blocos à cadeia. Na realidade, de acordo com o número de computadores tentando exercer essa tarefa, o *Bitcoin* modifica o número de dígitos específicos necessários, com a finalidade de aumentar ou diminuir a dificuldade da tarefa e garantir estatisticamente que o resultado seja alcançado em um período de tempo predeterminado.

Como o sistema é descentralizado e diversos usuários da rede estão trabalhando para conseguir adicionar blocos à cadeia, o usuário que adulterou determinado bloco somente conseguirá resolver os "quebra-cabeças" matemáticos mais rápido que os outros computadores da rede, se for detentor de um poder computacional maior que o de todos os demais usuários em conjunto. Logo, o

pode-se mencionar que Arvind Narayanan, professor na Universidade de Princeton, afirmou que, com a tecnologia atual, demoraria mais de um octilhão de anos para se descobrir uma colisão na SHA-256, *hash* utilizada pelo *Bitcoin* (NARAYANAN, et. al, 2016, p. 42).

adulterador teria que controlar mais de cinquenta por cento[18] dos computadores ligados à rede para conseguir alterar um bloco, o que é virtualmente impossível (BASTIAAN, 2015, p. 2).

O que garante que um usuário não monopolize o poder computacional de toda a rede é o processo que se chama *mineração*. Minerar *bitcoins* nada mais é que "ouvir" transações novas, que ainda não foram registradas, juntá-las em um novo bloco e começar a "brincar" com o "quebra-cabeça" até conseguir um número *x* de zeros para adicionar o novo bloco à cadeia. Aquele usuário – ou grupo de usuários reunidos – que conseguir resolver o problema matemático e adicionar o bloco à cadeia recebe uma recompensa: uma quantidade predeterminada de novos *bitcoins*, bem como a taxa de envio de todas as transações presentes no bloco. Essa recompensa financeira tem como finalidade garantir que sempre existam usuários na rede dispostos a competir pela validação das transações.

Além disso, o *Bitcoin* trabalha com um sistema de assinatura digital. Uma transação de *bitcoins* só poderá ser adicionada a um bloco se tiver sido assinada digitalmente por seu proprietário. Por esse motivo, mesmo sendo os usuários responsáveis pela adição de blocos à cadeia, torna-se praticamente impossível que uma transação falsa seja incluída no *blockchain*[19] (NARAYANAN, et. al, 2016, p. 83).

As assinaturas digitais configuram um esquema de segurança utilizado para conferir validade, até mesmo jurídica, a documentos digitais. Essa tecnologia pretende se assemelhar à assinatura física em dois aspectos: a) primeiramente, deve ser possível que qualquer pessoa identifique que o documento foi criado por um indivíduo específico – ou seja, deve ser verificável; b) em segundo lugar, deve ser impossível que alguém possa copiar essa assinatura de um documento e transpô-la a outro (NARAYANAN, et. al, 2016, p. 83).

Para cumprir esses requisitos, as assinaturas digitais se baseiam em um sistema de correspondência entre uma chave pública (*public key* ou *pk*) e uma chave privada (*secret key* ou *sk*). A chave pública deve ser disponibilizada para todos os usuários que quiserem conferir a autenticidade de um documento. A chave privada, como o próprio nome informa, deve ser de exclusividade de um indivíduo.

18. Sobre o "51% attack" conferir também: EYAL; SIRER, 2018; BRADBURY, 2013 e XU, 2016.

19. Explica Narayanan (et. al, 2016, p. 83): "Even if it is Alice's turn to propose the next block in the chain, she cannot steal other users' bitcoins. Doing so would require Alice to create a valid transaction that spends that coin. This would require Alice to forge the owners' signatures, which she cannot do if a secure digital signature scheme is used. So as long as the underlying cryptography is solid, she's not able to simply steal bitcoins."

A assinatura digital é criada a partir de uma função matemática que leva em conta a mensagem do documento e a chave privada do usuário. A verificação da autenticidade, por sua vez, é realizada a partir de outra função matemática em que se insere a assinatura digital do documento e a chave pública disponibilizada e, em seguida, analisa-se o resultado. Se este for o esperado, aquela mensagem terá sido, necessariamente, assinada pela chave privada correspondente (GALLAGHER; KERRY, 2013, p. 13).

Como a chave privada somente deve ser conhecida pelo seu proprietário, com esse procedimento pode-se garantir a todos os usuários que a mensagem foi assinada por determinada pessoa. Como a função matemática para validação da documentação compreende a mensagem do documento, a assinatura não pode simplesmente ser copiada de um documento para outro.

Todo esse sistema garante a funcionalidade e a segurança do *Bitcoin*. Obviamente, para a utilização do ativo não é necessário que o usuário tenha conhecimento técnico sobre seu funcionamento. Assim como muitas pessoas utilizam o *internet banking* todos os dias sem entender os pormenores de sua tecnologia ou de sua segurança, o *Bitcoin* pode ser utilizado através de aplicativos com interfaces simples por qualquer indivíduo que tenha acesso a um telefone celular com *internet*.

3.1. *As incertezas acerca da natureza jurídica do* bitcoin *e do dever das corretoras de reportar transações suspeitas*

As criptomoedas, até o presente momento, não são formalmente reconhecidas pela legislação brasileira. Por esse motivo, atualmente há uma efervescente discussão doutrinária sobre sua natureza jurídica. Há quem defenda a recepção desses ativos no ordenamento jurídico como unidades comparáveis à moeda estrangeira, assim como fez a Alemanha[20] (THE LAW LIBRARY OF THE CONGRESS, 2014). Outros defendem sua inclusão como *commodities* ou como bens incorpóreos (MORAIS; NETO, 2014). A Comissão de Valores Mobiliários, por sua vez, emitiu uma nota[21], no dia 11 de outubro de 2017, informando que, "a depender do contexto da sua emissão", as criptomoedas podem se enquadrar como valores mobiliários.

20. Publicação da Autoridade Federal de Supervisão Financeira Alemã disponível em: [www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2014/fa_bj_1401_bitcoins.html]. Acesso em: 15.05.2018.

21. Nota disponível em: [www.cvm.gov.br/noticias/arquivos/2017/20171011-1.html]. Acesso em: 15.05.2018.

A investigação sobre a adequada classificação jurídica das criptomoedas no ordenamento jurídico brasileiro, por recorte temático, não poderá ser realizada no presente trabalho. Para o correto enquadramento nas categorias jurídicas existentes, se faz necessário um estudo próprio e aprofundado sobre as características particulares de cada espécie de criptomoeda.

Não obstante não adentrar na discussão, pode-se enunciar, com segurança, que o *bitcoin* não é reconhecido como moeda nacional. A Constituição Federal brasileira determinou, em seu artigo 164, a competência exclusiva do Banco Central na emissão de moedas. Da mesma forma, a Lei 9.069/95 estipulou, em seu artigo 1º, que "unidade do Sistema Monetário Nacional passa a ser o REAL, que terá curso legal em todo o território nacional".

O Banco Central brasileiro, por sua vez, emitiu o Comunicado 31.379[22], informando que as moedas virtuais

> "não são emitidas nem garantidas por qualquer autoridade monetária, por isso não têm garantia de conversão para moedas soberanas, e tampouco são lastreadas em ativo real de qualquer espécie, ficando todo o risco com os detentores."

Também não há como reconhecer – pelo menos atualmente – nenhuma criptomoeda como moeda estrangeira. Decididamente, para tal, a criptomoeda deveria ser apontada oficialmente como moeda em algum país. Conforme o *Regulation of Bitcoin in Selected Jurisdictions*, documento produzido por analistas norte-americanos acerca da natureza jurídica do *bitcoin* em diversas legislações[23], nenhum país considera essa criptomoeda como moeda nacional (THE LAW LIBRARY OF THE CONGRESS, 2014). Além disso, reconhecendo as moedas virtuais como

22. No mesmo Comunicado, afirmou a instituição: "As empresas que negociam ou guardam as chamadas moedas virtuais em nome dos usuários, pessoas naturais ou jurídicas, não são reguladas, autorizadas ou supervisionadas pelo Banco Central do Brasil. Não há, no arcabouço legal e regulatório relacionado com o Sistema Financeiro Nacional, dispositivo específico sobre moedas virtuais. O Banco Central do Brasil, particularmente, não regula nem supervisiona operações com moedas virtuais". Disponível em: [www.bcb.gov.br/pre/normativos/busca/normativo.asp?numero=31379&tipo=Comunicado&data=16/11/2017]. Acesso em: 15.05.2018.

23. Ao mencionar o Brasil, o referido documento comete um equívoco ao apontar a Lei 12.865/03 como dispositivo legal que regula o *Bitcoin*. Ocorre que os pesquisadores norte-americanos entenderam que a referida lei, ao utilizar o termo "moeda eletrônica" como meio de pagamento no Sistema de Pagamentos Brasileiro (SPB), estava se referindo às criptomoedas. Como explicitado no item 2 do presente trabalho, estes dois conceitos não se confundem.

moedas estrangeiras, chegaria-se à conclusão que todas as corretoras de *bitcoin* seriam consideradas corretoras de câmbio, e, com isso, deveriam ser constituídas de acordo com a Resolução 1.770 do Banco Central[24].

Essas ponderações são importantes pois, apesar de não haver definição quanto à natureza jurídica das criptomoedas, no que diz respeito à lavagem de dinheiro, pessoas físicas e jurídicas que intermedeiam recursos financeiros de terceiros, em moeda nacional ou estrangeira, ou que operam com a compra e venda de moeda estrangeira, são submetidas a obrigações de identificação de clientes, manutenção de registros e comunicação e operações financeiras suspeitas de constituírem crime de lavagem de capitais.

Portanto, para avaliar se as empresas corretoras de *bitcoins* são obrigadas, nos termos do artigo 9º da Lei 9.613/98, a adotar tais medidas, deve-se observar se o *bitcoin* pode ser enquadrado em uma dessas categorias.

Como o *bitcoin*, ao menos atualmente, não pode ser classificado na legislação brasileira como moeda nacional ou estrangeira, não há falar que as empresas que realizam a compra e venda desses ativos estejam englobadas nos incisos I e II do referido diploma legal[25].

---

24. O BACEN já se manifestou, respondendo na área destinada a perguntas frequentes de seu *site*, sobre a ilegalidade de corretoras de *bitcoin* realizarem remessas de valores ao exterior, comprovando que essas instituições não são consideradas corretoras de câmbio, o que, consequentemente, aduz o não reconhecimento desse ativo como moeda estrangeira na legislação brasileira. Disponível em: [www.bcb.gov.br/acessoinformacao/legado?url=https:%2F%2Fwww.bcb.gov.br%2Fpre%2Fbc_atende%2Fport%2Fmoedasvirtuais.asp%3Fidpai%3DFAQCIDADAO]. Acesso em: 13.05.2018. Tangenciando esse tema, no entanto, Renato de Mello Jorge Silveira (2018, p. 132 e ss.), apresenta uma discussão sobre a peculiaridade do *bitcoin*. Uma vez que é um ativo existente exclusivamente no meio virtual, o autor defende a impossibilidade de se caracterizar sua compra e venda como transferência internacional, o que impacta diretamente na consideração das corretoras como casa de câmbio, mas também na possibilidade de adequação da conduta na figura típica da evasão de divisas, prevista na Lei 7.492/86.

25. Art. 9º – Sujeitam-se às obrigações referidas nos arts. 10 e 11 as pessoas físicas e jurídicas que tenham, em caráter permanente ou eventual, como atividade principal ou acessória, cumulativamente ou não:

I – a captação, intermediação e aplicação de recursos financeiros de terceiros, em moeda nacional ou estrangeira;

II – a compra e venda de moeda estrangeira ou ouro como ativo financeiro ou instrumento cambial;

(...)

Da mesma forma, seria incorreto afirmar que essas empresas são classificadas, nos termos do inciso IV, como empresas que realizam transferências de fundos. Como visto, o Banco Central Brasileiro se posicionou no sentido de que essa criptomoeda "não tem garantia de conversão para moedas soberanas". Nesse sentido, uma transferência dessa espécie não pode ser considerada transferência de fundos, pois o ordenamento jurídico nacional não garante sua capitalização. Além disso, como se pode depreender de sua redação, esse dispositivo foi criado para tutelar empresas de cartões eletrônicos ou magnéticos que trabalhem com dinheiro eletrônico, ou seja, com valores correspondentes à moeda corrente que podem ser transferidos eletronicamente. Conforme disposto no item 2 do presente trabalho, dinheiro eletrônico e moedas virtuais não são sinônimos.

Portanto, deve-se concluir que, ao menos legalmente, as companhias que realizam atividade de compra e venda de criptomoedas não são obrigadas a implementar práticas de prevenção à lavagem de dinheiro como outros setores do mercado[26].

Tentando modificar essa situação, o Ministério da Economia emitiu, em 03 de maio de 2019, a Instrução Normativa 1.888, a produzir efeitos em agosto, que disciplina "a obrigatoriedade de prestação de informações relativas às operações realizadas com criptoativos à Secretaria Especial da Receita Federal do Brasil".

Essa instrução normativa apresenta como dever das *exchanges* domiciliadas para fins tributários no Brasil notificar as transações envolvendo moedas virtuais, com especificação da data e tipo da operação, nome dos titulares, espécie e quantidade de criptomoedas transacionadas, valor em reais da transação e da taxa cobrada pela corretora, bem como número das carteiras eletrônicas envolvidas na transação.

Às pessoas naturais também se requer a notificação das transações de criptomoedas que ultrapassem o valor de trinta mil reais e que tenham sido realizadas com *exchanges* localizadas no exterior ou com outra pessoa natural.

Parágrafo único. Sujeitam-se às mesmas obrigações:

(...)

IV – as administradoras ou empresas que se utilizem de cartão ou qualquer outro meio eletrônico, magnético ou equivalente, que permita a transferência de fundos.

26. No mesmo sentido é a conclusão de BELLO e SAAVEDRA (2017, p. 166): "Ocorre que a legislação brasileira, em seu estado atual, pautando-se pelo princípio da legalidade, s.m.j., não permite a aplicação dos deveres de informação às *bitcoins exchanges*, ao passo que inegavelmente as moedas virtuais, como é o caso dos bitcoins, não podem ser interpretadas como moeda nacional ou estrangeira e, assim sendo, não se subsumem as disposições contidas no inciso I, do art. 9º da Lei 9.613/98".

Portanto, apesar de não listadas no rol das pessoas obrigadas da Lei de Lavagem de Dinheiro, percebe-se que as corretoras de moedas virtuais passam, agora, a ser alvo de interesse dos órgãos de fiscalização.

Entretanto, deve-se questionar se o Ministério da Economia teria competência para realizar a regulamentação dessa matéria por meio de Instrução Normativa[27]. As Instruções Normativas são atos jurídicos que cumprem o objetivo de esclarecer as leis, a fim de possibilitar a sua aplicação, e não podem criar deveres aos cidadãos (MELLO, 2015, p. 377). Ao que parece, o dever de comunicação imposto a essas empresas não decorre da interpretação da lei de lavagem de dinheiro e, consequentemente, não poderia ser feita por esse meio.

4. LAVAGEM DE DINHEIRO: BREVES REFLEXÕES SOBRE OS ASPECTOS PENAIS DO TIPO

Em atenção às diretrizes internacionais da última década do século XX, o Brasil aprovou, em 1998, seu primeiro diploma legal de combate à lavagem de dinheiro (Lei 9.613/98). A aplicação desta lei, primeiramente, teve como objetivo a supressão do capital utilizado no financiamento de complexas estruturas delitivas, a fim de desmantelar organizações criminosas como os cartéis de drogas latino-americanos. Em 2012, por meio da Lei 12.683, o Poder Legislativo incorporou ao diploma legal novas recomendações e normativas internacionais, aumentando sobremaneira o âmbito de incidência do tipo penal e tornando um tanto quanto confuso seu objetivo.

Atualmente, o crime de lavagem de dinheiro pode ser caracterizado como o

> "ato ou a sequência de atos praticados para mascarar a natureza, origem, localização, disposição, movimentação ou propriedade de bens, valores e direitos de origem delitiva ou contravencional, com o escopo último de reinseri-los na economia formal com aparência de licitude" (BADARÓ e BOTTINI, 2016, p. 30).

27. Nesse sentido, explica Celso Antônio Bandeira de Mello (2015, p. 278): "Se o regulamento não pode criar direitos ou restrições à liberdade, propriedade e atividades dos indivíduos que já não estejam estabelecidos e restringidos na lei, menos ainda poderão fazê-lo instruções, portarias ou resoluções. Se o regulamento não pode ser instrumento para regular matéria que, por ser legislativa, é insuscetível de delegação, menos ainda poderão fazê-lo atos de estirpe inferior, quais instruções, portarias ou resoluções".

Por essa definição e pela leitura do tipo penal[28] pode-se apontar alguns aspectos importantes quanto à possibilidade da prática deste fato típico no âmbito das criptomoedas.

Percebe-se, primeiramente, que, apesar de comumente falar-se em lavagem de dinheiro, esse tipo penal também se aplica à ocultação ou dissimulação de outros bens, direitos ou valores oriundos da prática delituosa. A inexistência de uma definição da natureza jurídica das criptomoedas na legislação brasileira não obsta que o *bitcoin* seja tomado como objeto material do delito. Os bens a que se refere o tipo penal em questão não se limitam a coisas corpóreas. Na realidade, a expressão "bens" é utilizada de maneira ampla, abarcando ativos de qualquer tipo[29], e, portanto, não parece haver dúvidas de que moedas virtuais podem ser objeto material do delito em análise.

Conforme leciona Bottini (2016, p. 110), o tipo penal também indica que os bens objeto de lavagem podem ter relação direta ou indireta com a infração penal antecedente. Bens diretamente provenientes de infração penal seriam o produto do crime, como *bitcoins* recebidos pela venda de armas ou *bitcoins* fruto de roubo ou estelionato[30]. Aqueles indiretamente provenientes de infrações penais seriam bens transformados, substituídos ou adquiridos pelos diretamente provenientes do injusto, como *bitcoins* comprados com dinheiro oriundo de corrupção passiva.

28. O art. 1º da Lei de Lavagem de Dinheiro (Lei 9.613/98) disciplina *in verbis*: "art. 1º. Ocultar ou dissimular a natureza, origem, localização, disposição, movimentação ou propriedade de bens, direitos ou valores provenientes, direta ou indiretamente, de infração penal".

29. A Convenção das Nações Unidas Contra o Crime Transnacional, também reconhecida como Convenção de Palermo, recepcionada no ordenamento jurídico brasileiro pelo Decreto Lei 5.015/2004, caracteriza, em seu art. 2º, "bens" como "ativos de qualquer tipo, corpóreos ou incorpóreos, móveis ou imóveis, tangíveis ou intangíveis, e os documentos ou instrumentos jurídicos que atestem a propriedade ou outros direitos sobre os referidos ativos". Da mesma forma, a Diretiva 2015/849/UE do Parlamento Europeu e do Conselho define bens como "activos de cualquier tipo, tanto materiales como inmateriales, muebles o inmuebles, tangibles o intangibles, así como los documentos o instrumentos jurídicos con independencia de su forma, incluidas la electrónica o la digital, que acrediten la propiedad de dichos activos o un derecho sobre los mismos". Disponível em: [https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32015L0849&from=pt]. Acesso em: 17.05.2018.

30. Por delimitação temática, o presente trabalho não irá adentrar na questão de se *bitcoins* podem ser objeto de roubo, em razão do requisito da corporeidade presente no artigo 157 do Código Penal Brasileiro. No entanto, interessante registrar que o Reino Unido

Importante realizar uma diferenciação: *bitcoins* provenientes, diretamente ou indiretamente, de infração penal podem ser objeto material do delito, mas, *per si*, não configuram lavagem de dinheiro. Ou seja, os *bitcoins* recebidos a partir da entrega de armas proibidas podem ser, como se demonstrará em seguida, movimentados com o objetivo de dissimular sua origem criminosa. Da mesma forma, as notas recebidas por corrupção passiva podem ser utilizadas para a compra de *bitcoins* com a finalidade de ocultar a origem ilícita – e, posteriormente, por exemplo, justificar o acréscimo patrimonial com a elevação da cotação desta criptomoeda. Entretanto, para configurar o delito de lavagem de dinheiro, essas condutas devem estar acompanhadas de um elemento subjetivo: a vontade de lavar o capital (BOTTINI, 2016, p. 33).

De acordo com Zaffaroni e Pierangeli (2015, p. 450), existem tipos penais com elementos ou requisitos subjetivos que excedem o dolo[31]. Esses elementos, especialmente estudados por Fischer no início do século XX, trouxeram grande dificuldade para a teoria clássica do delito, que, insistindo em manter a análise do dolo na culpabilidade, para sustentar um injusto meramente objetivo, se viu obrigada a reconhecer ao menos um elemento subjetivo na tipicidade.

Atualmente, com a análise do dolo e da culpa na tipicidade, mitigaram-se as divergências acerca da possibilidade de tipos penais apresentarem elementos subjetivos. Esses elementos, como explicam Zaffaroni e Pierangeli (2015, p. 452), podem requerer que a conduta do agente "seja dirigida à obtenção de um objetivo que se encontra 'mais além' do puro resultado ou produção da objetividade típica". Ou seja, pode haver tipos penais em que o agente deva realizar uma conduta como passo prévio para outra, mesmo que para a consumação do delito seja suficiente apenas o primeiro comportamento.

presenciou, em 22 de janeiro de 2018, um caso paradigmático: um grupo armado rendeu dois operadores de *Bitcoins* do país e os obrigou a realizar uma transferência da moeda pelo computador. Disponível em: [https://g1.globo.com/economia/noticia/reino-unido-registra-primeiro-roubo-de-bitcoins-a-mao-armada.ghtml]. Acesso em: 17.05.2018.

31. De forma similar é a lição de Santiago Mir Puig (2006, p. 279): "El conocer y querer la realización del tipo – el dolo típico – integra necesariamente la parte subjetiva del tipo doloso, que normalmente no precisa más. Pero en ocasiones la ley requiere que, además, concurran en el autor otros elementos subjetivos para la realización del tipo. Un ejemplo lo ofrece el art. 234 CP, que para la presencia del tipo de hurto exige que el autor tome una cosa ajena 'con ánimo de lucro'. En este caso, el solo tomar una cosa mueble ajena intencionalmente no da lugar todavía al tipo de hurto. Es preciso para ello, que además de conocer y querer tomar la cosa (dolo), el autor lo haga 'con ánimo de lucro'".

A construção teórica acerca dos elementos subjetivos distintos do dolo embasou o entendimento de Bottini no que diz respeito à necessidade de aferição do desígnio ou da intenção de promover a reinserção dos ativos maculados na economia formal com aparência de licitude para caracterização do delito de lavagem de dinheiro. Como pode-se perceber, esse elemento subjetivo especial não se encontra de forma expressa na lei, mas pode ser obtido a partir de uma análise teleológica e a partir da análise da integralidade do sistema penal (BOTTINI, 2016, p. 151).

Deve-se lembrar que a Lei 12.683/2012, que alterou o texto da Lei 9.613/98, procurou tornar mais eficiente a persecução penal dos crimes de lavagem de dinheiro. Esse delito, por sua vez, mesmo que possa ser fracionado, tem em seu cerne a intenção de reinserção dos ativos fruto de ilícito penal no sistema financeiro com a aparência de licitude[32].

Uma ocultação que visa simplesmente manter seguro o produto do crime difere, essencialmente, daquela que tem como finalidade a posterior camuflagem para reintrodução no sistema financeiro. Caso esse fim especial de agir implícito não fosse reconhecido como elementar típica não haveria como diferenciar a tipificação da lavagem de dinheiro em sua primeira modalidade, ou seja, a ocultação, do favorecimento real, tipificado no artigo 349 do Código Penal (BOTTINI, 2016, p. 151).

Esse entendimento foi referendado pelo Supremo Tribunal Federal após o julgamento dos embargos infringentes na Ação Penal 470. Mesmo que não haja concordância entre os ministros acerca dos requisitos suficientes para atestar a intenção de relocação do valor ilícito no sistema formal, parece consolidado que a ocultação da lavagem não se confunde com a mera ocultação para posterior usufruto dos bens[33].

32. Conforme explica De Carli (2006, p. 113): "A essência do processo, portanto, é separar o dinheiro de sua fonte (o delito antecedente); movimentá-lo tantas vezes quanto possível, criando camadas de operações (através de interpostas pessoas, físicas e jurídicas) que o distanciam cada vez mais da origem e tornam imensamente difícil recompor as pistas de auditoria; para, ao final, reinvesti-lo em uma atividade inserida na economia legal, de forma que pareça ser inteiramente legítimo".

33. Interessante ressaltar um trecho do Acórdão dos Sextos Embargos Infringentes da Ação Penal 470, em que o Ministro Luís Roberto Barroso assevera que "o recebimento por modo clandestino e capaz de ocultar o destinatário da propina, além de esperado, integra a própria materialidade da corrupção passiva, não constituindo, portanto, ação distinta e autônoma da lavagem de dinheiro. Para caracterizar esse crime autônomo seria necessário identificar atos posteriores, destinados a recolocar na economia formal a vantagem indevidamente recebida".

Portanto, em que pese a Lei 9.613/98 não prever expressamente a intenção especial de reinserção do capital maculado na economia formal, entende-se, com Bottini (2016, p. 152), que para a consumação da lavagem de dinheiro é imprescindível a demonstração da vontade de alcançar a reinserção no plano subjetivo[34].

Aplicando esse entendimento à lavagem de moedas virtuais, portanto, o indivíduo que recebe *bitcoins* pela venda de armas, por exemplo, não estará cometendo nenhuma modalidade do crime de lavagem de dinheiro pelo simples fato de utilizar-se da criptomoeda. Nesse caso, sequer há necessidade de analisar o elemento subjetivo distinto do dolo, uma vez que não há se pensar em lavagem de dinheiro por omissão imprópria do agente que comete o delito antecedente.

Não obstante, ainda que o agente utilize-se do dinheiro que recebeu pela venda de substâncias ilícitas para realizar a compra de *bitcoins*, o crime previsto no art. 1º, *caput*, da Lei de Lavagem de Dinheiro poderá ser vislumbrado, se, e somente se, o agente realizar a ação com a finalidade de utilizar esses *bitcoins* como forma de reintroduzir o capital maculado no mercado formal com aparência de licitude. Se o agente se utiliza da criptomoeda exclusivamente para guardar o proveito do crime, ou para lucrar ainda mais com a valorização da moeda virtual, não há delito de lavagem de dinheiro.

Além do exame do elemento subjetivo, outra análise deve ser realizada para a constatação da consumação do delito de lavagem de dinheiro nos exemplos acima mencionados. Deve-se pensar se há possibilidade de punição em razão da autolavagem, e, em havendo, quais os requisitos e limites para a configuração dessa modalidade do delito.

A Corte Especial do Superior Tribunal de Justiça, na Ação Penal 458, proveniente do Estado de São Paulo, em caso paradigmático, confirmou a possibilidade

34. Posicionamento divergente é o de Carla De Carli (2013, p. 280) que entende o tipo penal do favorecimento como exclusivamente "tendente a coibir situações em que a vantagem ilícita assegurada não tenha feição econômica". Assim, restringindo sobremaneira o espectro do delito de favorecimento, a autora diferencia os delitos de lavagem de dinheiro e favorecimento real sem a necessidade de utilizar-se do fim especial de agir. No entanto, essa observação acerca do âmbito de incidência do delito de favorecimento parece estar em desacordo com a doutrina desde de Hungria, que a respeito do proveito do crime, lecionava ser: "tôda vantagem ou utilidade, material ou moral, obtida ou esperada em razão do crime anterior, seja direta ou indiretamente: tanto o produto do crime (ex: a *res furtiva*) ou o resultado dêle (ex.: a posse de menor raptada), quanto a coisa que venha a substituir a que foi objeto material do crime (ex.: o ouro resultante da fusão das jóias subtraídas, ou a coisa que veio a ser comprada com o dinheiro furtado), ou, finalmente, o '*pretium criminis*'" (HUNGRIA, 1958, p. 505).

de punição do réu que pratica condutas de ocultação e dissimulação da origem ilícita de bens que ele mesmo auferiu a partir de conduta delitiva. Argumentou-se que o bem jurídico da lavagem de capitais é diverso daquele do delito antecedente[35]. O mesmo entendimento foi sustentado pelo Supremo Tribunal Federal, em 2012, na Ação Penal 470.

Não obstante o firme posicionamento jurisprudencial, Frederico Horta (2016, p. 146), analisando a questão sob a perspectiva do conflito aparente de normas, demonstra que a duplicidade de bens jurídicos não obsta a aplicação do princípio da consunção[36]. Conforme explica, a relação de consunção decorre de uma análise do caso concreto em que percebe-se uma conexão natural entre duas condutas puníveis por tipos penais diversos. Quando uma conduta sancionada por uma norma penal puder ser tomada como forma normal de realização dos pressupostos de outra, pode-se dizer que o desvalor desta já engloba os atos daquela[37].

35. Nos termos da ementa do acórdão: "(...) Não há que se falar em pós-fato impunível, mas em condutas autônomas, caracterizadoras de lavagem de dinheiro, por ter o agente alcançado as vantagens que perseguia com o cometimento do crime. Isso porque, conforme entendimento doutrinário, a lavagem de dinheiro, assim como a receptação é, por definição um crime derivado, acessório ou parasitário, pressupõe a ocorrência de um delito anterior.

IV – É próprio da lavagem de dinheiro, como também da receptação (Código Penal, art. 180) e do favorecimento real (Código Penal, art. 349), que estejam consubstanciados em atos que garantam ou levem ao proveito do resultado do crime anterior, mas recebam punição autônoma.

V – Conforme a opção do legislador brasileiro, pode o autor do crime antecedente, responder por lavagem de dinheiro, dada à diversidade dos bens jurídicos atingidos e à autonomia deste delito" (BRASIL, STJ, 2009).

36. Explica o autor: "Mas nos casos de consunção, como a aparente concorrência das normas incidentes se justifica tão somente por uma conexão corriqueira, normal, porém não necessária entre os injustos que reprimem, ao contrário do que ocorre quando há especialidade, não se pode afirmar que as normas consumida e consuntiva coincidam quanto ao objeto de ofensa. Ora, a prática de um roubo ou de uma extorsão nem sempre importará em lesões corporais leves para a vítima, pois pode ser que o agente sequer empregue violência, mas apenas grave ameaça. Nem todo estelionato envolverá o uso de um documento falso cuja potencialidade lesiva à fé pública venha se exaurir na fraude, pois esta pode ser promovida pelo emprego do simples ardil do agente ou de qualquer outro artifício. E da mesma forma, ainda mais claramente, nem todo homicídio será praticado com emprego de arma de fogo, pondo em risco a incolumidade pública, assim como nem todo estupro importará em injúria, com ofensa ao decoro da vítima" (HORTA, 2016, p. 146).

37. No mesmo sentido, cf. ZAFFARONI; PIERANGELI, 2015, p. 655 e ROXIN, 2014, p. 1011.

A partir dessa reflexão, Horta afirma que a lavagem de dinheiro pode ser considerada uma decorrência comum de alguns crimes antecedentes – como tráfico de drogas e de armas, os crimes contra a administração pública, o sistema financeiro, a ordem tributária ou aqueles praticados por organizações criminosas. Portanto, percebe-se que a punibilidade da autolavagem não deve ser automaticamente aceita no ordenamento jurídico brasileiro. Na realidade, esta deve decorrer da constatação que a lavagem de capitais caracterizou incremento na ofensividade em relação ao que normalmente ocorre no delito antecedente (HORTA, 2016, p. 146).

Esse posicionamento revela especial importância no paradigma das criptomoedas, uma vez que a simplicidade operacional da lavagem de dinheiro por meio do *Bitcoin* poderá propiciar a multiplicação da autolavagem. Atualmente, esse delito se distanciou dos objetivos declarados de conter organizações criminosas complexas e, através da autolavagem, passou a figurar como uma desvantagem que sempre acompanha condenações de crimes que envolvem expressivo fluxo monetário. Como a popularização das criptomoedas pode facilitar sobremaneira a lavagem de produtos de todas as espécies de infrações penais por seus próprios agentes, uma cautelosa reflexão acerca da punibilidade da autolavagem se faz necessária para evitar uma dilatação ainda maior do âmbito de incidência do tipo penal.

5. Lavagem de dinheiro por meio de *bitcoins*

Uma vez analisados alguns aspectos do tipo penal de lavagem de dinheiro, passa-se agora às reflexões acerca das novas modalidades de ocultação e dissimulação de ativos por meio do *Bitcoin*. Deve-se frisar, inicialmente, que o presente trabalho não tem a pretensão de esgotar todas as tipologias de lavagem de dinheiro por meio desta criptomoeda. Na realidade, dependendo da criatividade dos agentes, pode-se incorporar a tecnologia em praticamente todos os métodos já conhecidos de lavagem de capitais – utilizando-se, por exemplo, *bitcoins* como meio de pagando em operações superfaturadas, especialmente em decorrência da volatilidade do preço do ativo. No entanto, essas modalidades não decorrem da estrutura operacional do bitcoin, mas apenas o utiliza como bem com valor de mercado variável – como uma joia ou obra de arte – em práticas já conhecidas de lavagem.

O presente trabalho, no entanto, procurará debruçar-se nos novos métodos que utilizam as características do protocolo *Bitcoin* como forma de camuflar a origem infracional dos ativos. Esses métodos, se utilizados como uma etapa de

layering no percurso da lavagem, têm a capacidade de dificultar ainda mais o rastreio do dinheiro fruto de infração penal.

5.1. *Primeiro passo: adquirir* bitcoins

Como visto, todas as transações de *bitcoins* realizadas ficam gravadas no *blockchain*. Essa característica, por óbvio, é prejudicial àqueles que procuram utilizar o protocolo *Bitcoin* para a lavagem de dinheiro, uma vez que, como explica Van Wegberg (et al., 2018, p. 423), "todo o histórico de transações de qualquer carteira virtual está a um clique das autoridades judiciárias"[38] (tradução livre). Desse modo, o anonimato dos operadores depende da não associação entre a carteira virtual e seu real beneficiário (MÖSER, et al, 2013, p. 1).

Para garantir esse sigilo, como já mencionado, o primeiro passo realizado por indivíduos que pretendem navegar na internet com mais privacidade é a instalação de um *software* capaz de camuflar o *IP* do computador, como o *The Onion Router*[39] ou o *Windscribe*[40]. Esses programas atuam de forma a posicionar outros computadores entre os reais envolvidos na realização de um comando, criando uma rede criptografada de pelo menos três pontos. Esse caminho torna virtualmente impossível rastrear o endereço daquele que realizou determinada tarefa

38. "Owing to the blockchain concept, all historic information on any bitcoin address and transactional information is just one mouse-click away for law enforcement authorities" (VAN WEGBERG; et al., 2018, p. 423).

39. O Grupo de Ação Financeira Internacional (GAFI) define o *Tor* como: "an underground distributed network of computers on the Internet that conceals the true IP addresses, and therefore the identities of the network's users, by routing communications/transactions through multiple computers around the world and wrapping them in numerous layers of encryption. Tor makes it very difficult to physically locate computers hosting or accessing websites on the network. This difficulty can be exacerbated by use of additional tumblers or anonymisers on the Tor network. Tor is one of several underground distributed computer networks, often referred to as darknets, cypherspace, the Deep web, or anonymous networks, which individuals use to access content in a manner designed to obscure their identity and associated Internet activity" (GAFI, 2014, p. 6). Disponível em: [www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf]. Acesso em: 19.05.2018.

40. O Windscribe é "um conjunto de ferramentas que funcionam juntas para bloquear anúncios, rastreadores e *web beacons*, restaurar o acesso a conteúdo bloqueado e [...] garantir a sua privacidade online". Ele utiliza de uma Rede Virtual Privada (VPN) para camuflar o *IP* do usuário e dificultar o rastreio das informações disponibilizadas na utilização da internet. Disponível em: [https://prt.windscribe.com]. Acesso em: 17.07.2019.

na internet (MCCOY, et al., 2008, p. 64 e DINGLEDINE, et al., 2004). Interessante observar que o *site* oficial do *Bitcoin* aconselha seus usuários a esconderem seus *IPs*[41].

Após a instalação de algum serviço de camuflagem de *IP*, o agente que pretende realizar uma operação de lavagem de dinheiro pelo *Bitcoin* deverá criar uma carteira eletrônica. Além de, como mencionado na introdução do trabalho, não se vincularem com um documento ou com o nome do beneficiário[42], essas carteiras também podem, ao contrário de contas bancárias, ser criadas sem custo e instantaneamente (NARAYANAN, et al., 2016, p. 63). Assim, um mesmo indivíduo pode administrar quantas carteiras quiser, espalhando seus *bitcoins* em pequenos montantes[43] (VAN WEGBERG, et al, 2018, p. 421). Contando que as carteiras tenham sido criadas e utilizadas somente em computadores que tenham algum programa de camuflagem de *IP*, as possibilidades de identificação do seu proprietário são bem reduzidas (UNODC, 2014, p. 45).

Com a criação de uma ou várias carteiras eletrônicas, deverá o agente adquirir *bitcoins*. Essa operação pode ser realizada de quatro maneiras principais[44]:

41. Informa o *site*: "Because the Bitcoin network is a peer-to-peer network, it is possible to listen for transactions' relays and log their IP addresses. Full node clients relay all users' transactions just like their own. This means that finding the source of any particular transaction can be difficult and any Bitcoin node can be mistaken as the source of a transaction when they are not. You might want to consider hiding your computer's IP address with a tool like Tor so that it cannot be logged". Disponível em: [https://bitcoin.org/en/protect-your-privacy]. Acesso em: 19.05.2018.

42. Como explica Möser, et al, (2013, p. 1): "Bitcoin, by contrast, is designed with pseudonymous identities. Account numbers are public keys of a specific asymmetric encryption system. Account ownership is established by knowing the corresponding private key. Everyone with a computer can create valid key pairs from large random numbers and thus open one or many Bitcoin accounts".

43. Aconselham os desenvolvedores do *Bitcoin*: "To protect your privacy, you should use a new Bitcoin address each time you receive a new payment. Additionally, you can use multiple wallets for different purposes. Doing so allows you to isolate each of your transactions in such a way that it is not possible to associate them all together. People who send you money cannot see what other Bitcoin addresses you own and what you do with them. This is probably the most important advice you should keep in mind". Disponível em: [https://bitcoin.org/en/protect-your-privacy]. Acesso em: 19.05.2018.

44. O agente pode também "minerar" *bitcoins*. Entretanto, para o escopo do presente trabalho essa opção não será levada em consideração por dois motivos: a) primeiramente, ao minerar bitcoins, as criptomoedas recebidas serão novas, sem nenhum rastro, e, consequentemente, sequer precisarão ser objeto de lavagem; b) o preço e a tecnologia

a) pode-se comprar de qualquer indivíduo que tenha *bitcoins* e queira vendê-los; b) pode-se acessar *sites* de corretoras de *bitcoins* (*exchanges*) e realizar a compra; c) pode-se começar a receber *bitcoins* pela disponibilização de bens e serviços (lícitos ou ilícitos); ou d) pode-se realizar a compra em um caixa eletrônico de *bitcoins*.

Para se realizar a lavagem de dinheiro, preferencialmente, o agente procurará realizar a compra desses ativos de pessoas físicas que tenham *bitcoins*. Essa é, provavelmente, a melhor forma de manter a privacidade, uma vez que a relação entre vendedor e comprador é de curta duração e pode ser realizada de forma anônima. Ocorre que, a compra de criptomoedas dessa forma é especialmente arriscada, uma vez que o comprador não terá a segurança de que o indivíduo que oferece as moedas irá, realmente, enviá-las após o depósito do dinheiro.

Para solucionar o problema da confiança, várias empresas de *exchange* foram criadas. Essas companhias atuam como casas de câmbio, comprando e vendendo *bitcoins* aos interessados, de acordo com o preço do mercado. Adquirir expressiva quantidade de criptomoedas dessas empresas é tarefa mais simples que procurar por pessoas naturais.

Atualmente, corretoras de *bitcoins* já são uma realidade no mercado brasileiro, movimentando milhões de reais anualmente. Para transacionar com as principais empresas do ramo, a bem da verdade, deve-se realizar um cadastro *on-line*, que consiste no envio de uma foto que contenha o rosto da pessoa e um documento de identificação com o número do Cadastro de Pessoas Físicas.

No entanto, apesar de grandes *exchanges* nacionais já adotarem práticas de conhecimento do cliente, é difícil garantir que essas empresas atuem de forma a notificar transferências suspeitas. Da mesma forma, é praticamente impossível impedir que outras corretoras menores ou que *exchanges* sediadas no exterior que realizam transações com clientes brasileiros procedam de acordo essas diretrizes[45] (UNODC, 2014).

necessárias para tal tarefa não nos parece ser um atrativo no que diz respeito a sua utilização exclusivamente para a lavagem de dinheiro.

45. O Escritório das Nações Unidas sobre Drogas e Crime, em seu Manual para Detecção e Investigação de Lavagem de Dinheiro através de Moedas Virtuais, aponta a falta de regulamentação como um fator importante na ampliação dos riscos de envolvimento de corretoras com o crime em questão. Nesse sentido: "Even in cases where there is not deliberate efforts made to make transactions anonymous in this way, the lack of a regulatory requirement to retain records means that the administrating authorities and exchanges may not keep information that would be vital to an investigation. In particular,

Portanto, para se adquirir criptomoedas sem que essas transações de grande monta cheguem ao conhecimento dos órgãos fiscalizadores pode-se utilizar tanto *exchanges* nacionais dispostas a não incluir as transações suspeitas em suas notificações, quanto corretoras estrangeiras, especialmente aquelas sediadas em países que não apresentam grande preocupação com a lavagem de capitais. A principal barreira a se enfrentar nessa tarefa é, se forem utilizados bancos como intermediários na compra de criptomoedas, o dever destes de comunicação[46].

É possível também que as corretoras recebam em suas sedes valores em espécie para a compra de *bitcoins*. A esse respeito, até agosto de 2019, essa compra sequer seria considerada como objeto de notificação obrigatória. Após esta data, deverá o agente procurar corretoras dispostas a descumprirem a determinação de notificação.

A principal forma, no entanto, de se adquirir *bitcoins* após a criação de uma carteira é o recebimento dessa moeda em troca de bens ou serviços prestados. Como já mencionado, o dono de uma cafeteria pode possibilitar que seus clientes, que já têm *bitcoins*, enviem estas criptomoedas e, em troca, recebam suas bebidas. Essa transação também pode ser utilizada por aqueles que pretendem cometer delitos com a finalidade de obter lucro. Traficantes de armas podem, por exemplo, realizar a venda dos produtos ilícitos através da *internet* e receber o pagamento em *bitcoins*[47].

---

information on funding sources, transaction records and customer due diligence records may only be retained for as long as the information is required commercially, if it is gathered at all. Retention periods may therefore not be adequate for investigative purposes, particularly cross-jurisdictional investigations. Additionally, given the lack of regulation, there may be no obligation on the administrating authorities/virtual currency exchanges to report suspicious transactions" (UNODC, 2014, p. 46).

46. Nesse ponto, para dificultar que os bancos reportem as transações, pode o agente utilizar-se de antigas e conhecidas técnicas de dissimulação, como "laranjas", empresas de fachada ou a divisão de valores maiores em menores no depósito e movimentação.

47. Deve-se ressaltar o famoso caso Silk Road. Esse *site*, registrado na rede *Tor* em 2011, funcionava como um mercado *on-line*, aos moldes do *eBay*, interligando indivíduos de modo anônimo. Entre as mercadorias disponíveis para compra e venda encontravam-se drogas, armas e identidades falsas (CHRISTIN, 2013 e BARRATT, 2012). O sistema de pagamento do site utilizava a mesma metodologia do *PayPal*. Entretanto, não se aceitava nenhuma moeda soberana, apenas bitcoins. Um indivíduo que desejasse realizar uma compra escolhia o produto e efetuava o pagamento enviando bitcoins a uma carteira administrada pelo próprio site. A partir daí, o site informava ao vendedor que a transferência havia sido realizada e este enviava o produto, geralmente pelo correio,

Crimes cibernéticos, em especial, costumam utilizar desse meio de pagamento. Condutas como *hackers* invadindo dispositivos informáticos, criptografando dados pessoais ou empresariais e requerendo "resgate" em *bitcoins* não são infrequentes atualmente (YOUNG; YUNG, 2017 e TUTTLE, 2016). Além disso, de acordo com a Europol, cerca de 40% dos pagamentos de criminosos a criminosos investigados por crimes informáticos na Europa são realizados através de *bitcoins* (EUROPOL, 2015, p. 46). A grande vantagem dessa forma de obter criptomoedas é a supressão da crítica fase de contato com agentes obrigados a reportar transações suspeitas.

Uma última maneira possível de se adquirir as criptomoedas anonimamente é por meio de um caixa eletrônico[48]. A utilização dos caixas eletrônicos de *bitcoin* se assemelha muito à operação de um terminal de recarga de cartões de ônibus ou metrô. O usuário deve digitalizar a *QR Code* referente à sua carteira virtual, e, em seguida, inserir a quantia, na moeda corrente, que deseja comprar em *bitcoins* (HYMAN, 2015, p. 295).

Assim como os bancos, alguns fabricantes de caixas eletrônicos de *bitcoins*, a fim de evitar a compra completamente anônima da criptomoeda, estão incorporando sistemas de biometria em seus produtos. No entanto, como não há determinação para tal, nada impede que empresas produzam caixas eletrônicos sem esses sistemas.

No âmbito da lavagem de dinheiro, é simples perceber que o agente de um delito pode, facilmente, depositar o produto do crime nesses caixas eletrônicos, sem se identificar[49]. Se este agente depositar em uma carteira eletrônica criada em

para algum endereço fornecido pelo comprador. Após a entrega, o site direcionava os *bitcoins* pagos pelo comprador à carteira do vendedor. Em 2013, o Silk Road foi fechado pelo Federal Bureau Investigation (FBI) e um indivíduo foi preso por supostamente administrar o site. Estima-se que este mercado tenha movimentado 9.5 milhões de *bitcoins*, o equivalente, à época, a 1.2 bilhões de dólares (GAFI, 2014, p. 11).

48. Segundo os dados disponibilizados pelo *Coin ATM Radar*, os caixas eletrônicos de criptomoedas vêm crescendo uma média de 100% ao ano desde 2016. Atualmente, existem mais de 4000 desses equipamentos no mundo, sendo dois deles localizados na Avenida Paulista, na cidade de São Paulo. Disponível em: [https://guiadobitcoin.com.br/numero-de-caixas-eletronicos-de-bitcoin-cresce-100-ao-ano/]. Acesso em: 17.07.2019.

49. De acordo com HYMAN (2015, p. 287): "Bitcoin and other 'virtual currencies' are becoming more popular with each passing day. Most recently, Bitcoin Automated Teller Machines ("Bitcoin ATM") have been gaining publicity as the machines become more popular with Bitcoin users. Prior to the advent of the Bitcoin ATM, Bitcoin already had an increased potential for money laundering because the area in which it operates is

um computador que continha um *software* como o *Tor*, dificilmente esses *bitcoins* poderão ser rastreados ao seu portador.

Todos os métodos até aqui demonstrados podem ser utilizados para a aquisição de *bitcoins*. Essa é a etapa mais complicada da lavagem de dinheiro através de criptomoedas, uma vez que é nesse momento que deve ser evitado o sistema antilavagem implementado no país. Como se demonstrará a seguir, uma vez vencido esse passo, o distanciamento dos *bitcoins* de sua origem é tarefa simples, a ser realizada com um computador com acesso à *internet*.

5.2. Segundo passo: embaralhar

O segundo passo para dissimular a origem infracional das criptomoedas adquiridas é a lavagem propriamente dita. Por óbvio, poderá o autor de um delito apenas comprar *bitcoins* para futuramente capitalizá-los em outro país, ou comprar bens de consumo com esses *bitcoins*. No entanto, como explicitado no item 3 do presente trabalho, todas as transações realizadas por meio de *bitcoins* ficam registradas no *blockchain* para acesso público. Se o agente quiser diminuir ainda mais as chances de ser rastreado, principalmente se for utilizar os bitcoins em transações lícitas posteriormente, ele poderá utilizar programas de computador desenvolvidos especialmente para distanciar essas moedas de sua origem infracional.

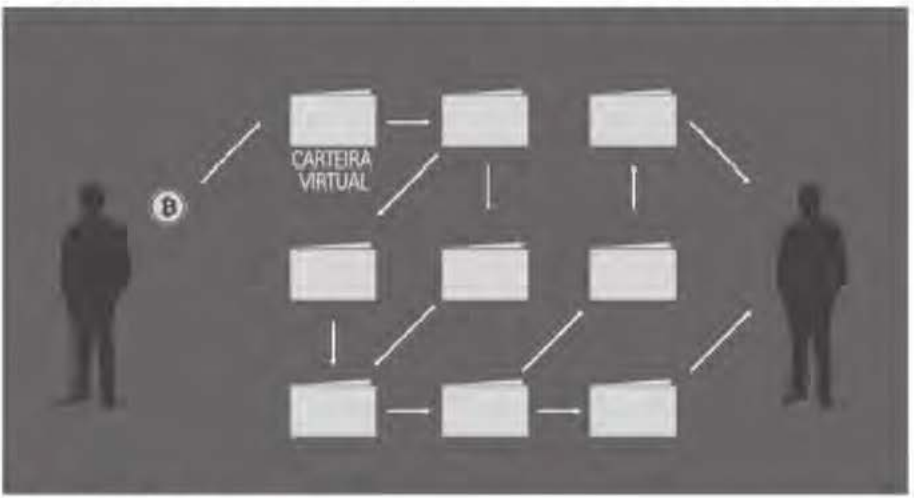
Os protocolos projetados para dissimular transações de *bitcoins* e ofuscar sua procedência são, geralmente, classificados em três gerações. A primeira delas constitui um grupo de *servers* – chamados de *tumblers*, *blenders* ou *mixers*[50] – de-

semi self-regulated. With the addition of Bitcoin ATMs, there is an even higher risk of money laundering because users can exchange cash for Bitcoins and, in some cases, vice versa via the Bitcoin ATM. For example, Drug Dealer Dan, who just completed a cash for drugs transaction, takes his 'hard earned' cash and deposits it into a Bitcoin ATM. Once the cash is deposited, the Bitcoin ATM exchanges the cash for Bitcoins at the going rate. With little to no personal information necessary for the exchange, Drug Dealer Dan is now free to purchase items using his Bitcoin Wallet or exchange the Bitcoins for cash at another Bitcoin ATM. Voila! His 'dirty' cash has been cleaned". O jornal britânico Daily Mail apontou a utilização dessa técnica por traficantes de drogas no país. Disponível em: [www.dailymail.co.uk/news/article-5142033/Drug-dealers-using-bitcoin-cashpoints-launder-money.html]. Acesso em: 20.05.2018.

50. O termo *mixer* faz referência à técnica apresentada por David Chaum (1981, p. 84) para esconder o destinatário e a mensagem de *e-mails*. O GAFI define *Mixer* como: "a type of anonymizer that obscures the chain of transactions on the blockchain by linking all transactions in the same bitcoin address and sending them together in a way that makes them look as if they were sent from another address. A mixer or tumbler

senvolvidos para camuflar transações de *bitcoins* através do emprego de um grande número de carteiras eletrônicas entre duas – ou mais – controladas por um mesmo cliente (VAN WEGBERG, et al., 2018, p. 423).

Figura 2 – Funcionamento simplificado de *mixers* de primeira geração



Fonte: elaborada pelos autores.

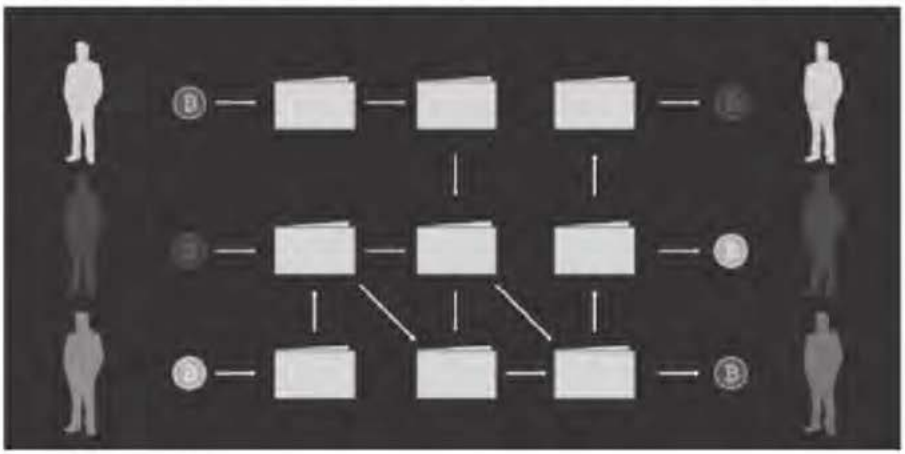
Utilizando-se desses *servers*, um indivíduo que pretenda distanciar-se de *bitcoins* maculados pode enviar suas criptomoedas e, pagando uma taxa, esse programa irá realizar diversas transações, passando esses *bitcoins* por diversas carteiras diferentes, dividindo-os em pequenas frações e reunindo-as, e, após certo tempo, devolverá moedas muito mais distantes de sua origem infracional[51] (SAT, et al, 2016, p. 246 e VAN WEGBERG, et al., 2018, p. 423).

sends transactions through a complex, semi-random series of dummy transactions that makes it extremely difficult to link specific virtual coins (addresses) with a particular transaction. Mixer services operate by receiving instructions from a user to send funds to a particular bitcoin address. The mixing service then "comingles" this transaction with other user transactions, such that it becomes unclear to whom the user intended the funds to be directed" (GAFI, 2014, p. 6).

51. Como explica VAN WEGBERG (et al., 2018, p. 423): "The typical mode of operation is that bitcoin mixing services provide customers with a newly generated bitcoin address to make a deposit. The bitcoin mixing service pays out other bitcoins from its reserve to bitcoin addresses provided by the customer, after deducting a mixing fee. To provide more anonymity, the pay-outs are spread out over time and some randomness is introduced in the division of amounts and/or the mixing fee".

Apesar de aparentemente simples, a qualidade desses serviços pode melhorar muito dependendo da quantidade de usuários que disponibilizam seus *bitcoins* para lavagem e da quantidade de bitcoins que o próprio *server* tenha como fundo para integrar na dissimulação (VAN WEGBERG, et al., 2018, p. 428). Havendo muitos indivíduos interessados no serviço, a moeda enviada por cada um deles, após passar por diversas transações, será direcionada a outro, sem nenhuma relação com seu dono anterior. Esse sistema torna ainda mais difícil o rastreio da origem do *bitcoin* (SAT, et al, 2016, p. 246).

Figura 3 – Funcionamento mais completo de *mixers* de primeira geração



Fonte: elaborada pelos autores.

Apesar de conseguirem desempenhar bem a tarefa de embaralhar e desordenar bitcoins, *servers* deste tipo não ficaram tão populares na comunidade das criptomoedas. Pode-se perceber que, para que o programa realize a tarefa de lavar *bitcoins*, os usuários devem enviar suas moedas para as contas fornecidas pelos desenvolvedores, o que requer confiança que estes não irão simplesmente receber as criptomoedas e desaparecer (HERRERA-JOANCOMARTÍ, 2014, p. 12 e RUFFING, et al., 2014. p. 348). Pela própria natureza *peer-to-peer* do *Bitcoin*, e principalmente após o ocorrido com a Mt. Gox[52], esses serviços não são uma

52. A Mt. Gox era uma corretora de bitcoins sediada em Tóquio, no Japão. Em 2013, a empresa efetuava o equivalente a 70% das transações desta criptomoeda no mundo. Em fevereiro de 2014, no entanto, a companhia decretou falência, anunciando que setecentos e quarenta mil bitcoins, à época avaliados em trezentos e cinquenta milhões de dólares, foram furtados de suas carteiras em razão de uma falha em sua segurança. (FRUNZA, 2015, p. 65).

unanimidade entre os entusiastas de criptomoedas[53] (SAT, et al, 2016, p. 246 e BISSIAS, et al., 2015, p. 150).

Sua pequena infiltração, no entanto, não significa sua inexistência. Muitos desenvolvedores procuram demonstrar a segurança de seus *servers* exibindo em fóruns seu tempo de atuação no "mercado" e as opiniões dos usuários. Ademais, novos *mixers* já utilizam, para encobrir ainda mais o rastro do dinheiro, outras criptomoedas no processo de embaralhamento, tornando o serviço mais efetivo e atrativo ao público específico.

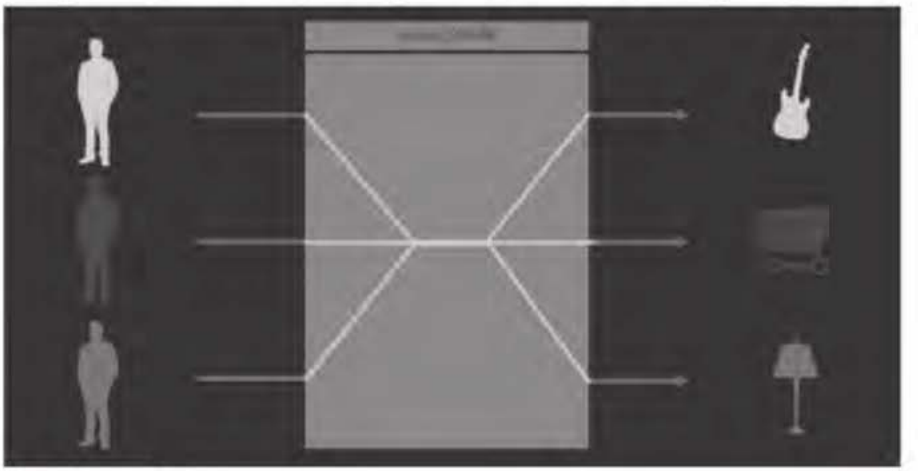
Mixers de segunda geração, com a intenção de solucionar o imbróglio da necessidade de confiança, basearam-se em pagamentos *peer-to-peer* por grupos. Pode-se citar como precursor dessa geração o protocolo CoinJoin[54], capaz de juntar em uma transação global vários usuários que, anteriormente, realizavam transações individuais (MAXWELL, 2013). Assim, ao invés de receber os *bitcoins*

53. Como explicam os pesquisadores da Universidade de Massachusetts: "the use of a trusted third party has well-known problems of its own: Not only must Alice and Bob trust that a centralized mix, Trent, will not steal their coins, but they must also trust that he will not help others – or be attacked by others – that want to link Alice and Bob's old and new addresses" (BISSIAS, et al, 2014, p. 150).

54. Conforme explicam os pesquisadores da Universidade de Shenzhen, na China: "The CoinJoin transaction combines many inputs and outputs and put them into a single transaction so that an input in the CoinJoin transaction is difficult to be corresponded to an output" (SHENTU; YU, 2015, p. 6). Existe uma pequena discordância no que se refere à classificação deste protocolo. Enquanto os pesquisadores chineses o mencionam como um exemplo de *mixer* de primeira geração, uma vez que seu funcionamento é baseado em um sistema centralizado, SAT (et al, 2016) o classificam como de segunda geração, pois sua tecnologia é, em geral, utilizada para a criação de protocolos mais complexos que englobam, além dessas transações com múltiplos *inputs* e *outputs*, a seleção e associação de usuários diversos e desconhecidos em transações comunitárias. A esse respeito, por exemplo, pode-se conferir o trabalho de ZIEGELDORF (et al, 2018), que elaboraram o CoinParty, um método de unir múltiplas transações de usuários desconhecidos a partir do CoinJoin: "In this section, we present, CoinParty, a novel mixing service that fulfills our requirements stated in §1.1. The core idea of CoinParty is to realize the insecure centralized mixing model securely in a decentralized fashion via threshold cryptography: In the centralized model, users deliver their funds in escrow to the mixing service and are paid back at a later point with the funds of some random other user. The main difference introduced by CoinParty is a set of mixing peers that replace the centralized mixing service with a distributed mixing protocol, thereby obviating the need for a trusted third party and protecting against theft from the centralized mixing service itself. This approach allows us, for the first time, to combine the advantages of previous centralized and decentralized approaches in one system".

maculados de um usuário e depois devolvê-los lavados, os *mixers* de segunda geração garantem privacidade a partir da associação anônima, e muitas vezes aleatória, de vários usuários que pretendiam realizar transações individuais. Esses usuários associados realizam, em conjunto, uma única transação no *blockchain*, que, no entanto, corresponde a todas as individuais. Por esse motivo, o rastreamento de quantas e quais criptomoedas exatamente foram direcionadas para quais usuários é dificultada[55] (SAT, et al, 2016, p. 247).

Figura 4 – Funcionamento simplificado de um *mixer* de segunda geração



Fonte: elaborada pelos autores.

Como esses protocolos propiciam que as transações sejam registradas no *blockchain* de maneira conjunta, tornando praticamente impossível, para qualquer usuário, identificar qual indivíduo transacionou com qual, é razoavelmente

55. Explica Kristov Atlas: "A mixing service implementing a protocol such as CoinJoin or CoinSwap allows a bunch of Bitcoin users to get together and craft a single Bitcoin transaction in multiple stages, ultimately sending their bitcoins to each other's destination addresses. None of the participants, other than the mixing server, need to know the relationship between their starting and destination addresses. This can be performed multiple times with multiple parties to further complicate analysis of the Blockchain. This approach is often referred to as trust-less mixing". Disponível em: [https://letstalkbitcoin.com/the-first-three-generations-of-bitcoin-mixing-technology]. Acesso em: 20.05.2018. No mesmo sentido, explica HERRERA-JOANCOMARTÍ (2014, p. 13): "The idea is that multiple users can jointly create a transaction with multiple input addresses and multiple output addresses. To be a valid transaction, the transaction should be signed by all users participating in the mixing".

simples que um agente, a fim de distanciar a origem infracional de seus *bitcoins*, realize uma transação entre duas carteiras eletrônicas que ele mesmo controla. A título de exemplo pode-se pensar que os *bitcoins* de origem infracional, presentes em uma carteira, podem ser transferidos para outra em uma transação realizada em conjunto com outras lícitas – como compras de bens de consumo ou remessas de *bitcoins* de um indivíduo a outro – de forma a dificultar o rastreio da origem dos ativos.

Um experimento realizado pelo departamento de Sistemas e Informação da Universidade de Münster, na Alemanha, testou *mixers* de primeira e segunda gerações disponíveis na *internet* e, posteriormente, utilizou técnicas de engenharia-reversa para tentar detectar o modo de operação e rastrear o caminho dos *bitcoins*. No experimento, os pesquisadores concluíram que dos três serviços utilizados, dois obtiveram sucesso em camuflar as transações, sendo impossível rastreá-las novamente às primeiras carteiras utilizadas (MÖSER, et al, 2013, p. 10).

Inspirando-se nesse trabalho, pesquisadores da Technische Universiteit Delf, na Holanda, realizaram um experimento completo de lavagem de *bitcoins*, passando desde a fase da compra das criptomoedas até o saque dos valores lavados por empresas regulamentadas, como a Western Union ou PayPal. Os pesquisadores descobriram que, dos cinco *mixers*[56] utilizados, três se mostraram fraudulentos, recebendo os *bitcoins* e nunca enviando seus respectivos valores aos endereços fornecidos. No entanto, os dois programas que desempenharam a tarefa contratada o fizeram de forma a impossibilitar o rastreio dos *bitcoins* (VAN WEGBERG, et al., 2018).

Ao testar os serviços de *exchanges on-line*, que prometiam a conversão de *bitcoins* em moedas correntes, depositando os valores referentes aos *bitcoins* enviados a suas carteiras eletrônicas em contas de serviços como o PayPal e o Western Union, os pesquisadores descobriram que apenas uma corretora, das cinco testadas, não cumpriu a tarefa (VAN WEGBERG, et al., 2018). Vale ressaltar, no entanto, que na metodologia do trabalho os pesquisadores explicam que escolheram serviços mal avaliados em fóruns *on-line* de propósito a fim de testá-los. Assim, é perceptível que com uma busca em fóruns da *internet* pode-se evitar a contratação de serviços fraudulentos. Além disso, sempre pode-se testar os serviços com pequenas quantias antes de realizar as transferências reais.

56. Neste experimento, em especial, não é possível avaliar se os serviços utilizados são classificados como *mixers* de primeira ou segunda geração uma vez que, por escolha dos autores, não foram divulgados os nomes ou os endereços *on-line* dos *mixers* utilizados.

Por fim, existem também os *mixers* de terceira geração, que, na realidade, são criptomoedas, criadas com base na estrutura do *Bitcoin*, mas que modificam certas características para dar mais ênfase à privacidade (SAT, et al, 2016, p. 247). Como já mencionado no item 2 deste trabalho, moedas como a *Monero* e a *Zcash* podem ser o futuro da lavagem de dinheiro no ambiente virtual.

A *Monero*, por exemplo, utiliza-se de um sistema de assinatura digital conhecido como *ring signatures* (MÖSER, 2018 e NOETHER, 2015). Nesse sistema, quando um indivíduo assina uma transferência da criptomoeda para outro, a operação aparece no livro de registro conjuntamente à assinatura de outros usuários do protocolo. Não há como saber qual das carteiras presentes na transação de fato foi responsável pelo envio daquela criptomoeda (BURNISKE; TATAR, 2018, p. 87). A *Zcash*, por sua vez, apresenta um modelo de livro de registro – chamado zk-SNARKs – em que é possível realizar "transações blindadas", nas quais não há indicação sequer dos endereços das carteiras eletrônicas envolvidas (QUESNELLE, 2017).

Percebe-se, portanto, a existência de métodos de lavagem de *bitcoins* razoavelmente simples, que, ao mesmo tempo, garantem alta possibilidade de sucesso na empreitada. Após a utilização desses métodos de lavagem, o usuário terá *bitcoins* limpos.

5.3. *Terceiro passo: integrar*

A reinserção dos *bitcoins* no mercado formal, com aparência de licitude é o terceiro, e mais simples, passo da lavagem de dinheiro. Uma vez distanciados de sua origem, os *bitcoins* que passaram pelo processo de lavagem estarão disponíveis em carteiras eletrônicas, podendo ser utilizados na compra de bens e produtos ou vendidos de forma lícita para corretoras de *bitcoins* – mesmo para aquelas que adotam um sistema de prevenção à lavagem de dinheiro.

Acredita-se que o mercado de *bitcoins* está em ampla expansão e, em decorrência disso, quanto mais empresas passarem a aceitar essa moeda como meio de pagamento, mais simples sua reinserção no mercado formal. Interessante mencionar que, atualmente, o próprio agente da lavagem pode constituir uma empresa e efetuar pagamentos fictícios provenientes das mais diversas carteiras controladas por ele mesmo à sua empresa sob pretexto de prestação de algum serviço. Os *bitcoins* já lavados poderão ser declarados, tributados e inseridos no mercado financeiro com aparência lícita.

Outra peculiaridade reside no fato de a Receita Federal brasileira somente exigir a inclusão de informações acerca das criptomoedas na Declaração de Imposto

de Renda a partir do ano de 2017. Em decorrência disso, aquele que comprou *bitcoins* até este ano pode declará-los e informar que realizou a compra desses ativos em baixíssimas cotações, atribuindo os ganhos financeiros à volatilidade da criptomoeda.

Vale ressaltar, por fim, que a existência de caixas eletrônicos e corretoras, tanto físicas quanto *on-line*, registradas em diversos países, facilita sobremaneira que os bitcoins lavados sejam "sacados" em qualquer local do mundo. Segundo Van Wegberg, (et al., 2018, p. 429), diversas *exchanges* se encontram na *internet* dispostas a proporcionar saques anônimos de *bitcoins*. Para tal, basta que o agente envie as moedas virtuais a uma determinada carteira para que a corretora devolva o valor correspondente, descontada uma parcela a título de pagamento pelo serviço, através de depósitos em contas do PayPal ou de envios de papel moeda pelo Western Union.

Como se pode perceber, todo o processo de lavagem de dinheiro por meio de *bitcoins* pode ser realizado de forma razoavelmente simples. Apesar disso, pode-se dizer que esses métodos não são conhecidos e debatidos no ambiente acadêmico. Jogar luz nessas modernas tipologias de lavagem de dinheiro pode ser uma forma iniciar esse debate, a fim de auxiliar a elaboração de medidas de prevenção mais adequadas à realidade das criptomoedas.

A partir de agora, portanto, passa-se a uma breve reflexão acerca das modificações legislativas no sistema jurídico brasileiro para a prevenção da lavagem de capitais.

6. Possíveis modificações legislativas

Em 1989 foi criado o Grupo de Ação Financeira Internacional (GAFI), um órgão intergovernamental que tem como finalidade fortalecer a cooperação internacional e alinhar as legislações de seus países membros no combate à lavagem de dinheiro e ao financiamento do terrorismo. Este órgão emitiu quarenta recomendações[57] que constituem um guia para os países adotarem como exemplo em suas legislações de prevenção à criminalidade transnacional.

A Recomendação de número 15 determina que os países membros devem identificar e avaliar os riscos de lavagem de dinheiro que possam surgir ou ser incrementados nas hipóteses de desenvolvimento de novos produtos ou no uso de

57. As recomendações do GAFI podem ser consultadas em: [www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf]. Acesso em: 22.05.2018.

novas tecnologias em produtos já existentes. Nesse sentido, a ascensão das criptomoedas é uma circunstância que passa a fazer parte da preocupação e dos esforços internacionais para diminuição dos riscos de lavagem de dinheiro[58].

No entanto, grande parte dos esforços acadêmicos e legislativos no que diz respeito à restrição de oportunidades de cometimento do delito de lavagem de dinheiro por meio de *bitcoins* se concentra na criação de deveres de *compliance*.

Compliance é um programa de organização interno de empresas que tem como objetivo prevenir o cometimento de crimes através da identificação antecipada de condutas potencialmente lesivas, da elaboração de práticas para evitar esses comportamentos e do treinamento de funcionários para adotarem condutas de acordo com essas práticas (BRODT; FARIA, 2016, p. 195).

A legislação de lavagem de dinheiro apresenta mecanismos de *compliance* como o dever de conhecimento e registro da identidade do cliente, da natureza e propósito de suas transações e o dever de diligência para as pessoas obrigadas nos termos de seus artigos 9º e 10º (BRODT; FARIA, 2016, p. 215). Como explicam Estellita e Wunderlich (2014, p. 24) esse dispositivo legal "impôs uma espécie de cooperação privada obrigatória para o controle dos processos de lavagem de dinheiro, justamente para pessoas físicas e jurídicas que atuam em setores importantes na captação e transferência de recursos financeiros".

No entanto, é importante refletir se tais instrumentos, utilizados principalmente no marco do controle estatal sobre a moeda, podem ser transpostos, de forma efetiva, para o ambiente descentralizado das criptomoedas. A mudança de paradigma principal das moedas virtuais criptografadas é exatamente a ausência de um ente central, de um órgão de controle que possa ser submetido a colaboração involuntária[59].

Assim, se um indivíduo que pretende comprar *bitcoins* pode transacionar com qualquer corretora, sediada em qualquer local do planeta, não parece ser suficiente a mera regulamentação de corretoras nacionais, a fim de limitar a compra

58. Em 2014 o órgão publicou um relatório específico acerca dos riscos de lavagem de dinheiro e financiamento ao terrorismo por criptomoedas. Disponível em: [www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf]. Acesso em: 22.05.2018.

59. Como explica Marc Goodman (2015, p. 305): "Because funds are not stored in a central location, accounts cannot readily be seized or frozen by police, and tracing the transactions recorded in the blockchain is significantly more complex than serving a subpoena on a local bank operating within traditionally regulated financial networks".

de ativos de maneira anônima[60]. Aqueles que cogitam fazer uso do sistema para a lavagem de capitais provavelmente encontraram oportunidades em *exchanges* sediadas em países que não apresentam preocupações com métodos antilavagem.

Além disso, o próprio requerimento de informações sobre a identidade de partes envolvidas em uma transação de *bitcoins* – prática de importância central na atual dinâmica antilavagem de dinheiro – é uma demanda que não pode ser, ao menos em algumas hipóteses, fornecida pela *exchange*. Deve-se entender que, ao comprar as criptomoedas por meio de uma corretora de *bitcoins*, em geral, o indivíduo apenas compra o direito sobre tais ativos, que estão sob a administração da corretora em alguma carteira virtual da qual o beneficiário não tem efetivo acesso. Nesse momento, evidentemente, há como estipular a obrigação de identificação do cliente. No entanto, a partir do momento que esse cliente requer a transferência das *bitcoins* armazenadas pela corretora para outra carteira eletrônica, não é possível à corretora ter ciência de quem é o titular dessa carteira.

Como já demonstrado, a criação de carteiras eletrônicas para armazenar *bitcoins* não é tarefa exclusiva das *exchanges*. Pelo contrário, qualquer indivíduo com acesso à *internet* pode criar um par de chaves pública e privada para transacionar no protocolo (NARAYANAN, et al., 2016, p. 63). Portanto, a única forma de se reconhecer o titular da carteira a qual são dirigidas as moedas é a partir de uma declaração prestada pelo próprio cliente. Essa situação, por óbvio, em muito fragiliza a qualidade das informações prestadas pelas corretoras.

Além disso, ao comprar *bitcoins*, as corretoras podem ser obrigadas a requerer e manter o registro dos vendedores, mas, principalmente em razão difícil vinculação dos *bitcoins* com seus reais beneficiários, verificar a qualidade dessas informações pode ser uma tarefa de onerosa realização, especialmente levando-se em conta o elevado número de transações que podem ocorrer diariamente.

Deve-se ressaltar ainda que várias corretoras de criptomoedas são *startups*, constituídas por entusiastas da tecnologia e, muitas vezes, com poucos ou até nenhum funcionário além dos sócios. Compreender a estrutura organizacional dessas empresas se mostra importante para evitar que a legislação crie obrigações inatingíveis, com potencial de inviabilizar a própria operacionalidade da empresa.

Portanto, até pode-se pensar na inclusão das *exchanges* de *bitcoins* como obrigadas a reportar transações suspeitas, mas, primeiramente, deve-se realizar essa

60. Questiona Renato de Mello Jorge Silveira (2018, p. 141): "Haveria, pois, sentido em regulamentação em um único país, quando internacionalmente ainda não existem controles efetivos?"

determinação por meio do Congresso Nacional, com a inclusão, no artigo 9º da Lei de Lavagem de Dinheiro, de um inciso relativo a empresas que tenham como atividade principal ou eventual a compra e venda de criptomoedas.

No que diz respeito à regulamentação, deve o Banco Central do Brasil ou o Conselho de Controle de Atividades Financeiras (COAF) procurar estabelecer de maneira clara os deveres das corretoras de *bitcoins*, levando em consideração as características do empreendimento e das corretoras, a fim de evitar a criação de leis onerosas ou que tenham como finalidade apenas atrelar, objetivamente, a responsabilidade penal sobre eventuais transações que caracterizem lavagem de dinheiro aos membros dessas empresas[61]. Especialmente, devem ser estipulados critérios para o reconhecimento e posterior notificação de transações consideradas suspeitas, tarefa não realizada no âmbito da Instrução Normativa 1.888, bem como regras de conduta em caso de notificações inalcançáveis ou com indícios de informações inverídicas.

No que tange à identificação, em razão do vínculo entre essas empresas e seus clientes ser, na grande maioria das vezes, exclusivamente *on-line*, pode-se pensar em exigir que as corretoras solicitem a foto de um documento de identificação com número no Cadastro de Pessoas Físicas, a foto do titular ao lado de seu documento e comprovantes de endereço e de rendimentos. Além disso, a fim de evitar fraudes, interessante determinar que as companhias confiram os dados disponibilizados pelos clientes com cadastros como o da Receita Federal.

Além da implementação de políticas de *compliance* nas *exchanges*, a fim de evitar a compra de *bitcoins* anonimamente, julga-se prudente também a criação de regulamentação específica para a criação de caixas eletrônicos de criptomoedas. Pode-se, por exemplo, exigir que somente possam utilizá-los pessoas previamente cadastradas no site de sua administradora – que serão submetidos às regras de identificação supramencionadas. Além disso, há a possibilidade de implementação de verificadores de biometria, como alguns caixas eletrônicos já adotam, a fim de registrar os dados dos indivíduos presentes na transação.

Outra importante forma de fiscalizar a lavagem de dinheiro por meio de criptomoedas parece prescindir de qualquer modificação legislativa. Compreendendo a fundo o modelo operacional do protocolo *Bitcoin*, pode-se elaborar formas de fiscalização e reconhecimento de indícios de lavagem de dinheiro. Para tal

61. Vale lembrar que o descumprimento de alguma norma de *compliance*, por si só, não pode ser visto como circunstância suficiente para configuração de delito omissivo impróprio por descumprimento de dever legal de garante daquele que na empresa exerce a posição de *chief compliance officer*. Nesse sentido, cf. PINTO; BRENER, 2018, p. 350.

objetivo pode-se aproveitar de uma das principais características do protocolo: a transparência de seu livro de registros.

No *Bitcoin*, da mesma forma que é fácil realizar uma transação sem deixar rastros, também é fácil cometer um erro e colocar a perder anos de transações anônimas. Acessar uma carteira eletrônica por um computador não protegido por criptografia ou juntar em uma mesma carteira virtual *bitcoins* lavados e maculados, por exemplo, são condutas suficientes para estabelecer a correlação entre *bitcoins* e seus beneficiários[62].

A utilização de *softwares* que consigam, através de algoritmos, identificar o caminho do dinheiro, alertar sobre possíveis transações suspeitas e relacioná-las a seus operadores pode ser mais eficiente que os deveres de notificação. Diversos protocolos[63] estão sendo elaborados nesse sentido, cabendo às autoridades fiscalizadoras brasileiras se atentarem ao seu surgimento e procurarem entender qual a melhor forma de utilização.

7. Considerações finais

Praticamente todas as novidades no campo da tecnologia, à primeira vista, geram insegurança, desconforto ou medo naqueles que desconhecem seu funcionamento ou procuram prever sua utilização. No caso do *Bitcoin* não seria diferente.

Não há dúvidas que a tecnologia *blockchain* é capaz de proporcionar uma revolução no sistema financeiro, na forma de registrar documentos e de assegurar a veracidade das informações. Se bem aproveitada, em muito facilitará a estrutura dos Estados modernos, desburocratizando tarefas e garantindo mais confiança às certificações. Por outro lado, sua popularização pode, também, incentivar o

62. A título de exemplo, pode-se citar a situação descrita por Van Wegberg (2018, p. 429): "From a 'criminal perspective', we did make a vital mistake in our cash-out. Whereas there was no link between our 'tainted' bitcoins and 'laundered' bitcoins at the day of the experiment, we cleaned up the experiment and retrieved the invested bitcoins four days later. In this clean-up, remaining 'tainted' bitcoins and 'laundered' bitcoins were sent to our bitcoin address at a regular bitcoin exchange. This 'mistake' linked our identity directly back to the 'tainted' bitcoins, negating all our previous efforts to stay anonymous. Of course, this step was intentional – as the experiment was completed and remaining bitcoins were to be collected – it does show how easily it is to make a mistake and render the attempted launderer vulnerable".

63. Cf. MAKSUTOV, et al., 2019; WATKINS, et al., 2003; KAMINSKY, 2011 e KOSHY, et al., 2014.

surgimento de novas modalidades delitivas, bem como a modernização de antigas estratégias criminosas. Essas circunstâncias, ao invés de desincentivar o uso ou sustentar o discurso da necessária proibição desses ativos, devem ser analisadas com rigor teórico para embasar decisões legislativas acerca da melhor forma de regulamentação.

A introdução e popularização de meios de troca não emitidos por entes centrais, especialmente com a possibilidade de utilização de forma anônima, é, sem dúvidas, uma modificação que influencia tanto a ingerência estatal na política monetária, quanto as formas de controle e vigilância estatal sobre os cidadãos.

Compreender esse novo momento é crucial para encarar os desafios que as criptomoedas trarão em seu marco regulatório. A dificuldade de se rastrear e, principalmente, atrelar transações de bitcoins a seus reais operadores, apesar de muito debatida no âmbito acadêmico internacional, parece ainda não ter sido objeto de detida pesquisa no Brasil.

O presente trabalho procurou delimitar o problema a ser enfrentado e indicar um possível caminho para os debates que conciliasse a necessidade de fiscalização estatal com as particularidades desse novo ativo. Espera-se, assim, que as reflexões apresentadas possam evidenciar, também no cenário nacional, as discussões acerca do marco regulatório das criptomoedas e propiciar, especialmente na seara penal, uma contribuição para a elaboração de uma regulamentação exequível e eficiente.

Referências

ALBUQUERQUE, Bruno Saboia de; CALLADO, Marcelo de Castro. Understanding bitcoins: facts and questions. *Revista Brasileira de Economia*, Rio de Janeiro, v. 69, n. 1, p. 3-16, Mar. 2015. Disponível em: [www.scielo.br/scielo.php?script=sci_arttext&pid=S0034-71402015000100003&lng=en&nrm=iso]. Acesso em: 15.05.2018.

ANTONOPOULOS, Andreas M. *Mastering bitcoin*: unlocking digital cryptocurrencies. "O'Reilly Media, Inc.", 2014.

BADARÓ, Gustavo Henrique; BOTTINI, Pierpaolo Cruz. *Lavagem de dinheiro*: aspectos penais e processuais penais: comentários à Lei 9.613/1998, com as alterações da Lei 12.683/2012. São Paulo: Ed. RT, 2012.

BANCO CENTRAL DO BRASIL. FAQ – Sistema de Pagamentos Brasileiro (SPB). Brasília, Março de 2014. Disponível em: [www4.bcb.gov.br/pec/gci/port/focus/faq%207-sistema%20de%20pagamentos%20brasileiro.pdf]. Acesso em: 12.05.2018.

BARRATT, Monica J. SILK ROAD: EBAY FOR DRUGS: The journal publishes both invited and unsolicited letters. *Addiction*, v. 107, n. 3, p. 683-683, 2012.

BASTIAAN, Martijn. *Preventing the 51%-attack*: a stochastic analysis of two phase proof of work in bitcoin, 2015. Disponível em: [http://referaat.cs.utwente.nl/conference/22/paper/7473/preventingthe-51-attack-astochastic-analysis-of--two-phase-proof-of-work-in-bitcoin.pdf]. Acesso em: 19.05.2018.

BELLO, Douglas Sena; SAAVEDRA, Giovani Agostini. Breves notas sobre compliance e prevenção à lavagem de dinheiro em bitcoins exchanges. *DELICTAE: Revista de Estudos Interdisciplinares sobre o Delito*, v. 2, n. 3, p. 159-159, 2017.

BISSIAS, George et al. Sybil-resistant mixing for bitcoin. In: *Proceedings of the 13th Workshop on Privacy in the Electronic Society*. ACM, 2014. p. 149-158.

BRADBURY, Danny. The problem with Bitcoin. *Computer Fraud & Security*, v. 2013, n. 11, p. 5-8. 2013.

BURNISKE, Chris; TATAR, Jack. *Cryptoassets*: the Innovative Investor's Guide to Bitcoin and Beyond. McGraw-Hill, 2018.

CHAUM, David L. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, v. 24, n. 2, p. 84-90. 1981.

CHRISTIN, Nicolas. Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace. In: *Proceedings of the 22nd international conference on World Wide Web*. ACM, 2013. p. 213-224.

DE CARLI, Carla Veríssimo. Dos crimes: aspectos objetivos. In: DE CARLI, Carla Veríssimo. *Lavagem de dinheiro*: prevenção e controle penal. 2. ed. Porto Alegre: Verbo Jurídico, 2013.

DE CARLI, Carla Veríssimo. Lavagem de dinheiro: ideologia da criminalização e análise do discurso. Dissertação (Mestrado em Direito) – Faculdade de Direito da Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, p. 231, 2006.

DINGLEDINE, Roger; MATHEWSON, Nick; SYVERSON, Paul. *Tor*: The second-generation onion router. Naval Research Lab Washington DC, 2004.

ESTELLITA, H.; WUNDERLICH, A. Sigilo. *Deveres de informação e advocacia na lei de lavagem de dinheiro*. Livro Homenagem a Miguel Reale Júnior. Rio de Janeiro: Editora GZ, 2014. v. 1. p. 17-30.

EUROPEAN CENTRAL BANK. *Virtual Currency Schemes*, Outubro de 2012. Disponível em: [www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf]. Acesso em: 13.05.2018.

EUROPOL. The internet organised crime threat assessment. 2015. Disponível em: [www.europol.europa.eu/sites/default/files/publications/europol_iocta_web_2015.pdf]. Acesso em: 19.05.2018.

EYAL, Ittay; SIRER, Emin Gün. Majority is not enough: Bitcoin mining is vulnerable. *Communications of the ACM*, v. 61, n. 7, p. 95-102, 2018.

FARIA, Aléxia Alvim M.; Brodt, Luis Augusto Sanzo. Criminal compliance em lavagem de dinheiro: uma introdução conceitual e regulamentar. In: Flávia Siqueira; Luis Augusto Sanzo Brodt. (Org.). *Limites ao poder punitivo*: diálogos na ciência penal contemporânea. Belo Horizonte: D'Plácido, 2016. v. 1. p. 191-240.

FEATHERSTONE, Mike; BURROWS, Roger (Ed.). *Cyberspace/cyberbodies/cyberpunk*: Cultures of technological embodiment. Sage, 1996.

FRUNZA, Marius-Cristian. *Solving modern crime in financial markets*: analytics and case studies. Academic Press, 2015.

GAFI, Grupo de Ação Financeira da América Latina. *Informe de Tipologias Regionales*. 2016. Disponível em: [www.gafilat.org/index.php/es/biblioteca-virtual/gafilat/documentos-de-interes-17/tipologias-17/354-tipologias-regionales-2016/file]. Acesso em: 20.05.2018.

GAFI, Grupo de Ação Financeira. *Virtual currencies*: key definitions and potential AML/CFT risks. 2014. Disponível em: [www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf]. Acesso em: 20.05.2018.

GALLAGHER, P; KERRY, C. Federal Information Processing Standards (FIPS) publication 186-4: *Digital Signature Standard (DSS)*, 2013. Disponível em: [https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf]. Acesso em: 24.05.2018.

GOODMAN, Marc. *Future crimes*: everything is connected, everyone is vulnerable and what we can do about it. Anchor, 2015.

HERRERA-JOANCOMARTÍ, Jordi. Research and challenges on bitcoin anonymity. In: *Data privacy management, autonomous spontaneous security, and security assurance*. Cham: Springer, 2014. p. 3-16.

HORTA, Frederico Gomes de Almeida. Sobre a punibilidade da "autolavagem" (selflaudering): um problema de concurso aparente de normas. In: *Direito penal, processo penal e constituição III* [Recurso eletrônico on-line] organização CONPEDI/UNICURITIBA. DEODATO, Felipe Augusto Forte de Negreiros; LEAL, Rogério Gesta (Coords.). Florianópolis: CONPEDI, 2016. p. 133-152.

HUGHES, Eric. *A cypherpunk's manifesto*. Disponível em: [www. activism. net/cypherpunk/manifesto. Html, 1993]. Acesso em: 03.08.2004.

HUNGRIA, Nélson. *Comentários ao código penal, vol. IX*. Rio de Janeiro: Forense, 1958.

HYMAN, Mitchell. Bitcoin ATM: A Criminal's Laundromat for Cleaning Money. *Thomas L. Rev.*, v. 27, p. 296, 2015.

KAMINSKY, Dan. Black Ops of TCP/IP. *Presentation*. Black Hat USA, 2011. Disponível em: [http://dankaminsky.com/2011/08/05/bo2k11/]. Acesso em: 24.05.2018.

KOSHY, Philip; KOSHY, Diana; MCDANIEL, Patrick. An analysis of anonymity in bitcoin using p2p network traffic. In: *International Conference on Financial Cryptography and Data Security*, Springer, Berlin, Heidelberg, p. 469-485, 2014.

MAKSUTOV, Artem A. et al. Detection of Blockchain Transactions Used in Blockchain Mixer of Coin Join Type. In: *2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus)*, IEEE, p. 274-277, 2019.

MAXWELL, Gregory. CoinJoin: Bitcoin privacy for the real world. In: *Post on Bitcoin forum*. 2013. Disponível em: [https://bitcointalk.org/index.php?-topic=279249.0]. Acesso em: 13.05.2018.

MCCOY, Damon et al. Shining light in dark places: Understanding the Tor network. In: *International symposium on privacy enhancing technologies symposium*, Springer, Berlin, Heidelberg, p. 63-76, 2008.

MELLO, Celso Antônio Bandeira de. *Curso de direito administrativo*. 32. ed., revista e atualizada até a Emenda Constitucional 84, de 2.12.2014. São Paulo: Editora Malheiros, 2015.

MORAIS, Carlos Yury Araújo; NETO, João Batista Brandão. *Tributação das operações com criptomoedas*. Teresina: Arquivo Jurídico, 2014.

MÖSER, Malte; BÖHME, Rainer; BREUKER, Dominic. An inquiry into money laundering tools in the Bitcoin ecosystem. In: *2013 APWG eCrime Researchers Summit*. Ieee, p. 1-14, 2013.

MÖSER, Malte et al. An empirical analysis of traceability in the monero blockchain. *Proceedings on Privacy Enhancing Technologies*, v. 2018, n. 3, p. 143-163, 2018.

MIR PUIG, Santiago. *Derecho penal parte general*. 8. ed. Editorial Reppertor, 2006.

NAKAMOTO, Satoshi. *Bitcoin*: a peer-to-peer electronic cash system. 2008. Disponível em: [https://bitcoin.org/bitcoin.pdf]. Acesso em: 11.05.2018.

NARAYANAN, Arvind et al. *Bitcoin and cryptocurrency technologies*: a comprehensive introduction. Princeton University Press, 2016.

NOETHER, Shen. Ring signature confidential transactions for monero. *IACR Cryptology ePrint Archive*, v. 2015, p. 1098, 2015.

PFITZMANN, Andreas; KÖHNTOPP, Marit. Anonymity, unobservability, and pseudonymity – a proposal for terminology. In: *Designing privacy enhancing technologies*, Springer, Berlin, Heidelberg, p. 1-9, 2001.

PINTO, Felipe Martins; BRENER, Paula Rocha Gouvêa. Responsabilidade corporativa e *compliance*: novas estratégias de prevenção à criminalidade econômica. In: FORTINI, Cristiana (Coord.). *Corrupção e seus múltiplos enfoques jurídicos*. Belo Horizonte: Fórum, 2018. p. 339-353.

POPPER, Nathaniel. *Digital gold*: bitcoin and the inside story of the misfits and millionaires trying to reinvent money. New York: Harper, 2015.

QUESNELLE, Jeffrey. *On the linkability of Zcash transactions*. arXiv preprint arXiv:1712.01210, 2017.

ROXIN, Claus. *Derecho penal*: parte general – tomo II. Pamplona: Thomson Reuters Civitas, 2014.

RUFFING, Tim; MORENO-SANCHEZ, Pedro; KATE, Aniket. Coinshuffle: Practical decentralized coin mixing for bitcoin. In: *European Symposium on Research in Computer Security*. Cham: Springer, 2014. p. 345-364.

SAT, Diana Mergenovna et al. Investigation of money laundering methods through cryptocurrency. *Journal of Theoretical and Applied Information Technology*, v. 83, n. 2, p. 244, 2016.

SHENTU, QingChun; YU, JianPing. *Research on Anonymization and De-anonymization in the Bitcoin System*. arXiv preprint arXiv:1510.07782, 2015.

SILVEIRA, Renato de Mello Jorge. *Bitcoin e suas fronteiras penais*: em busca do marco penal das criptomoedas. Belo Horizonte: Editora D'Plácido, 2018. p. 205.

STELLA, Julio Cesar. Moedas Virtuais no Brasil: como enquadrar as criptomoedas. *Revista da Procuradoria-Geral do Banco Central*, v. 11 n. 2, p. 259, 2017.

THE LAW LIBRABRY OF THE CONGRESS. *Regulation of Bitcoin in Selected Jurisdictions*. Washington, 15 de Janeiro de 2014. Disponível em: [www.loc.gov/law/help/bitcoin-survey/regulation-of-bitcoin.pdf]. Acesso em: 15.05.2018.

TSCHORSCH, Florian; SCHEUERMANN, Björn. Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Communications Surveys & Tutorials*, v. 18, n. 3, p. 2084-2123, 2016.

VIANNA, Túlio Lima. *Fundamentos de direito penal informático*. Rio de Janeiro: Forense, 2003.

TUTTLE, Hilary. Ransomware attacks pose growing threat. *Risk Management*, v. 63, n. 4, p. 4, 2016.

ULRICH, Fernando. *Bitcoin*: a moeda na era digital. São Paulo: Instituto Ludwig Von Mises Editora, 2017.

UNODC, United Nations Office on Drugs and Crime. *Basic Manual on the Detection and Investigation of the Laundering of Crime Proceeds Using Virtual Currencies*, 2014. Disponível em: [www.imolin.org/pdf/imolin/FULL10-UNODCVirtualCurrencies_final.pdf]. Acesso em: 19.05.2018.

VAN WEGBERG, Rolf; OERLEMANS, Jan-Jaap; VAN DEVENTER, Oskar. Bitcoin money laundering: mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin. *Journal of Financial Crime*, v. 25, n. 2, p. 419-435, 2018.

WATKINS, R. CORY et al. Tracking dirty proceeds: exploring data mining technologies as tools to investigate money laundering. *Police Practice and Research*, v. 4, n. 2, p. 163-178, 2003.

XU, Jennifer J. Are blockchains immune to all malicious attacks? *Financial Innovation*, v. 2, n. 1, p. 25, 2016.

YOUNG, Adam L.; YUNG, Moti. Cryptovirology: The birth, neglect, and explosion of ransomware. *Communications of the ACM*, v. 60, n. 7, p. 24-26, 2017.

ZAFFARONI, Eugênio Raúl; PIERANGELI, José Henrique. *Manual de direito penal brasileiro*: parte geral. 11. ed. rev. e atual. São Paulo: Ed. RT, 2015.

ZIEGELDORF, Jan Henrik et al. Secure and anonymous decentralized Bitcoin mixing. *Future Generation Computer Systems*, v. 80, p. 448-466, 2018.

Pesquisas do Editorial

Veja também Doutrinas

- A natureza jurídica do *bitcoin* no sistema legal brasileiro, de Edilton Meireles – *RT* 1004/147-167 (DTR\2019\40594);
- *Bitcoin* e demais *cryptocoins*, de Emylha Maryá Vieira Domingos Luz – *RDB* 85/69-87 (DTR\2019\39064);
- *Bitcoin*: internet do dinheiro e o direito, de Ana Beatriz dos Santos Borges – *RDB* 81/119-139 (DTR\2018\19493);
- Lavagem de dinheiro, *bitcoin* e regulação, de Thiago Bottino e Christiana Mariani da Silva Telles – *RBCCrim* 148/131-176 (DTR\2018\19794); e
- O desafio legislativo do *bitcoin*, de Bruno Marques Bensal Roma e Rodrigo Freitas da Silva – *ReDE* 20/109-128 (DTR\2016\24309).