CRIPTOATIVOS: CRIPTOGRAFIA DO ANONIMATO E TENTATIVAS DE REGULAÇÃO

CRYPTOASSETS: ANONYMITY CRYPTOGRAPHY AND REGULATION ATTEMPTS

MARCOS VINICIUS LIPIENSKI

Mestre em Direito Processual Civil pela Universidade Federal de Minas Gerais (2015 – atual). Graduado em Direito pela Universidade Federal de Uberlândia (2008). Atualmente é juiz federal – Tribunal Regional Federal da 1ª Região.

<https://orcid.org/0000-0002-3144-745X>

RESUMO

O objetivo do artigo é, em primeiro lugar, apresentar um panorama das principais tecnologias criptográficas responsáveis notadamente por criar um ambiente de ocultamento no uso de criptoativos, de forma a dificultar o rastreamento para o combate à lavagem de dinheiro e ao financiamento do terrorismo. Depois, buscamos identificar os principais marcos regulatórios concebidos para os criptoativos. Iniciamos essa pesquisa com as diretrizes Gafi/FATF de utilidade; em seguida, estudamos o esquema normativo geral da União Europeia para, depois, tratar do caso específico da Itália. Antes de chegarmos à conclusão, tratamos também das iniciativas regulatórias brasileiras, com destaque para comparação entre essas experiências. A conclusão aborda a necessidade de equilíbrio entre a regulação para suprimir a lavagem de dinheiro e o financiamento do terrorismo e a criação de um ambiente favorável ao desenvolvimento de tecnologias úteis às pessoas nas mais diversas áreas.

Palavras-chave: criptoativos; ocultamento; Gafi/FATF; regulação.

ABSTRACT

The article's objective is, in the first place, to present a panorama of the main cryptographic technologies notably responsible for creating an environment of concealment in the use of cryptoassets, in a way that hinders tracking for fighting money laundering and terrorism financing. Later, we seek to identify the main cryptoassets' conceived regulatory frameworks. We begin this research with GAFI/FATF's useful guidances; then, we study the Europe Union's general normative body to assess Italy's specific case. Before we come to a conclusion, we also analyze Brazil's regulatory initiatives, with emphasis in the comparison between these experiences. The conclusion addresses the necessity of balance amidst regulation to suppress money laundering and terrorism financing and the creation of a favorable environment to the development of useful technologies to the people in many diverse areas.

Keywords: cryptoassets; concealment; Gafi/FATF; regulation.

Recebido: 10-3-2022
Aprovado: 28-4-2022

SUMÁRIO

1 Introdução. 2 Conceitos gerais e recursos criptográficos aplicados ao *bitcoin* e às criptomoedas em geral. 3 A regulação dos criptoativos na Europa. 4 Exemplo concreto: a regulação na Itália. 5 A regulação dos criptoativos no Brasil. 6 Conclusão. Referências.

1 INTRODUÇÃO

A forma relativamente rápida e descentralizada de realização de transações de criptoativos, aliada ao emprego das mais variadas

formas de criptografia, os tornam atrativos para uso na lavagem de dinheiro.

Em razão da pouca familiaridade do mundo jurídico com a criptografia, o artigo inicia com um capítulo destinado a uma descrição de diversos protocolos aplicados a algumas espécies de moedas virtuais e suas funções, notadamente quando contribuem para a ocultação de informações sobre pessoas e valores envolvidos.

Depois, o próximo capítulo trata do progressivo aumento de preocupação e regulação de criptoativos na Europa, principalmente após a ocorrência de atentados terroristas no norte, ao que se segue um relato de como a Itália (historicamente um centro tradicional de combate ao crime organizado e à lavagem de dinheiro), especificamente, lida com a internalização das medidas regulatórias formuladas pela União Europeia.

Uma vez apresentadas as bases do panorama regulatório de criptoativos, bem como a experiência italiana, o capítulo seguinte dedica-se a discorrer sobre a evolução do uso dos criptoativos no Brasil, mediante análise comparativa entre as ainda incipientes propostas legislativas nacionais sobre o tema e aquilo desenvolvido na Europa em acordo com recomendações do Gafi/FATF.

2 CONCEITOS GERAIS E RECURSOS CRIPTOGRÁFICOS APLICADOS AO BITCOIN E ÀS CRIPTOMOEDAS EM GERAL

O *bitcoin* tem a sua origem identificada na publicação, no âmbito de um fórum de criptógrafos Cypherpunk, de um artigo denominado Bitcoin: a Peer-to-Peer Electronic Cash System, de autoria de Satoshi Nakamoto. Seguiu-se, meses depois, a primeira transação e

a disponibilização pública do aplicativo denominado Bitcoin v.0.1 (TEIXEIRA; BOCHI, 2019).

O *bitcoin* fundamenta-se na vontade de criar um sistema eletrônico de transações no qual um terceiro não se faz necessário (*peer-to-peer*), de forma que o seu custo não sofre o acréscimo em razão dessa participação. O sistema de Blockchain, por outro lado, oferece o suporte para evitar transações duplas mediante a utilização de um registro público validado por meio do Proof of Work¹ (ajustável de acordo com o avanço da potência de processamento da mineração), que torna computacionalmente impraticável a atividade de *hackers*, enquanto não detiverem o domínio quase absoluto sobre todo o poder computacional existente:

We have proposed a system for electronic transactions without relying on trust. We started with the usual framework of coins made from digital signatures, which provides strong control of ownership, but is incomplete without a way to prevent double-spending. To solve this, we proposed a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honestnodescontrol a

¹ Sobre Proof of Work: “A ideia toda surgiu em 1993, quando Cynthia Dwork e Moni Naor publicaram um artigo científico sobre funções vinculadas à memória para combater o *spam*. No artigo, eles estavam tentando introduzir um novo método de combate aos *e-mails* de *spam*, que são enviados usando a energia do computador para cada *e-mail* (ou transação). O Proof of Work é uma função difícil de calcular, mas fácil de verificar. A função possui uma mensagem, um endereço de destinatário e alguns outros parâmetros. Neste trabalho, Dwork e Naor chamavam de função de precificação. Os computadores de hoje podem enviar milhões de mensagens de *spam* todos os dias, o que cria um grande problema. No entanto, se os computadores precisarem gastar 10 segundos em cada mensagem, eles poderão enviar apenas 8 mil *spams* por dia. Em 1999, no artigo Proofs of work and bread pudding protocols (Provas de trabalho e protocolos de pudim de pão) publicado por Markus Jakobsson e Ari Juels, o termo ‘Proof of work’ foi introduzido e a notação é criada. Seu objetivo era caracterizar a notação de uma prova de trabalho (PoW), um protocolo no qual um provador demonstra a um verificador que ele gastou um certo nível de esforço computacional em um intervalo de tempo específico.” (BASTIANI, 2019).

majority of CPU power. The network is robust in its unstructured simplicity. Nodes work all at once with little coordination. They do not need to be identified, since messages are not routed to any particular place and only need to be delivered on a best effort basis. Nodes can leave and rejoin the network at will, accepting the proof-of-work chain as proof of what happened while they were gone. They vote with their CPU power, expressing their acceptance of valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them. Any needed rules and incentives can be enforced with this consensus mechanism. (NAKAMOTO, 2008, p. 8).

Tecnologias como o Blockchain são denominadas Distributed Ledger Technologies - DLT, redes *peer-to-peer* que permitem que diversos indivíduos mantenham uma cópia idêntica de um mesmo registro, independentemente de uma autoridade central que verifique, execute e grave transações (WHAT ARE..., c2022).

Apesar de haver publicidade acerca das transações, o que inclusive é elemento essencial para viabilizar tanto o Proof of Work como para dispensar uma instituição financeira intermediária, ainda existe um nível considerável de privacidade garantida. A relação entre publicidade e privacidade, no contexto do *bitcoin*, é possível mediante o sistema de chaves privadas e chaves públicas. Enquanto a chave privada seria o equivalente de uma senha para realizar transações, a chave pública aproximar-se-ia de um endereço na rede *bitcoin*, para onde alguém interessado deveria encaminhar a moeda virtual em caso de interesse de transacionar (como se fosse o *e-mail* de um usuário).

Tanto a chave privada quanto a pública são compostas por 78 dígitos aleatórios, e a cada chave privada corresponde uma única chave pública. Ocorre que, apesar de trabalhoso, é possível identificar e decodificar a chave privada a partir da análise do volume de

transações referentes a uma chave pública específica. Para conferir maior segurança a essa construção, passou-se a utilizar endereços públicos, gerados a partir das chaves públicas, por meio de uma complexa função matemática, e gerar uma camada extra de segurança (CHAVE, 2018).

As características principais do *bitcoin* podem ser resumidas em três, de acordo com a breve exposição: descentralização, pseudoanonimidade e globalidade. A descentralização diz respeito à dispensa de uma autoridade central para possibilitar transações; a pseudoanonimidade se refere à relativa ausência de identificação da pessoa que comercializa a moeda virtual, notadamente em comparação com a utilização de instituições financeiras tradicionais; por fim, a globalidade atine à possibilidade de realização de transações independentemente de fronteiras políticas ou geográficas (ASSIS, 2020).

Existem, hoje, diversas criptomoedas, mas o *bitcoin* responde pelo maior valor. Em novembro de 2021, o mercado de capitalização de criptomoedas excedia pela primeira vez 3 trilhões de dólares, dos quais cerca de 1.3 trilhões correspondiam ao *bitcoin* (BINDSEIL; PAPSDORF; SCHAAF, 2022). As demais moedas variam basicamente de acordo com a aplicação e privacidade para as quais foram direcionadas.

O *ether* é a moeda da denominada *blockchain* de segunda geração, Ethereum. Segunda geração porque, enquanto *bitcoin* é considerada de primeira geração, de construção relativamente simples e com linguagem voltada primariamente para transações, o Ethereum foi concebido como uma plataforma computadorizada descentralizada que roda seus *smart contracts* simultaneamente em inúmeros computadores pelo mundo. Esses *smart contracts*, por sua vez, são aplicativos mais variados possíveis que rodam no ambiente Ethereum

e são ativados mediante transações financeiras. Esses aplicativos são disponibilizados na *blockchain* para qualquer outro usuário e não podem ser deletados a não ser mediante instrução específica de seu criador. As transações no Ethereum são públicas, apesar de não registrarem o nome real dos usuários, no estilo do *bitcoin* (WHAT IS..., 2021).

A tecnologia *blockchain* é dividida em três gerações. A primeira, ou Blockchain 1.0, refere-se à plataforma tecnológica e à moeda virtual; a segunda (Blockchain 2.0) diz respeito aos diversos aplicativos econômicos e financeiros que existem para além de simples transações financeiras; por último, a Blockchain 3.0 trata de aplicações diversas que não envolvem transações financeiras, como arte, saúde etc., com destaque para a governança de *smart cities* (EFANOV; ROSCHIN, 2018).

A par de moedas virtuais que seguem o padrão público (pseudoanônimo) do *bitcoin*, surgiram diversas outras que trazem em si mecanismos para conferir maior grau de anonimidade, as denominadas *privacy coins*.

Dentre as *privacy coins*, destacam-se monero e zcash, em razão de seu volume no mercado.

Monero é a moeda virtual cujo padrão é unicamente privado, em razão da utilização de *stealth addresses* e *ring signatures*. *Stealth addresses* fazem com que o transmissor de moeda utilize um endereço de uso único para cada transação que realizar, de modo a dificultar o rastreamento e a identificação do destinatário e os valores envolvidos (FRANKENFIELD, 2022). Por outro lado, *ring signatures* funcionam de forma que um usuário envie uma mensagem e o destinatário saiba que a assinatura venha de um grupo, porém não revele a identidade

do usuário assinante.² Ainda, *ring confidential transactions*, ou RingCT, ajudam a ocultar o valor das transações (SETH, 2021).

A moeda *zcash* originou-se de uma proposta de alteração do *bitcoin* para que houvesse a adoção de um recurso de privacidade que acabou rejeitado pela comunidade. Por isso, ela possui alguns elementos comuns com o *bitcoin*, como a utilização do mecanismo de consenso Proof of Work, enquanto inova em outros pontos, como por exemplo no algoritmo Equihash em substituição ao SHA-256 (ISMAR, 2021). O *zcash* pode funcionar de forma pública como também permite a habilitação de uma transação protegida mediante protocolo com criptografia *zero-knowledge proof* (especificamente, zk-SNARK, ou zero-knowledge Succinct Non-Interactive Argument of Knowledge, uma espécie que pode ser realizada em milissegundos). Essa tecnologia é interessantíssima, permite convencer um verificador não somente de que o número existe, mas como também o conhece, sem revelar qualquer informação sobre esse número (WHAT ARE..., c2021). Em outras palavras, mais genéricas (porque a tecnologia, ainda em estágios iniciais de desenvolvimento, engloba possibilidades mais vastas de aplicação), permite que uma informação seja validada sem necessidade de expor dados que a demonstrem (ALAMEDA, 2020).

A criptomoeda *grin*, por sua vez, vale-se do protocolo Mumblewimble (nome inspirado em uma magia do universo de Harry Potter cuja finalidade é silenciar a vítima acerca de determinado assunto). Baseado em criptografia de curva elíptica, que confere uma camada extra de proteção às operações, o protocolo ainda combina

² Curiosamente, o artigo citado trata da utilização de *ring signaures* em aplicativos de comunicação remota entre médicos e pacientes, de forma a apresentar uma solução de segurança para os dados médicos do usuário do sistema, o que demonstra um dos possíveis empregos benéficos da tecnologia de sigilo apresentada. Bem por isso, o combate aos crimes não pode impedir radicalmente o avanço do estado da arte para não impedir o progresso tecnológico em prol dos cidadãos.

outros protocolos criptográficos como Confidential Transactions – CTs, CoinJoin, Dandelion e Cut-Through (esse último visa acelerar a análise e confirmação da transação na *blockchain*).

Confidential Transactions são protocolos de *zero knowledge*, explicados logo acima.

CoinJoin é um processo no qual duas ou mais pessoas combinam suas transações de forma a dificultar a identificação do seu produto. Para ser realizado, depende que a transação contenha assinaturas de diversas pessoas, ou seja, receba *inputs* de diversas pessoas, e como resultado, *output* de mesmo valor, porém com a titularidade ofuscada em razão do processamento conjunto (PARMAN, 2021).³

O protocolo Dandelion é uma solução pensada para conferir uma camada extra de proteção às pessoas de uma transação dentro do método utilizado pelo *bitcoin*. Nesse método tradicional, quando um *node* (computador que está na rede *bitcoin*) envia uma transação à rede

³ “Suponha que Maria queira transferir 1 BTC do endereço A para o endereço B. Enquanto Juan deseja transferir 1 BTC do endereço C para o endereço D. Para tornar esta transação privada, os dois decidem usar CoinJoin para fins de combinação de suas transferências em uma única transação que tem duas entradas (A e C) e duas saídas (B e D). O que o CoinJoin faz é pegar as entradas de Maria e João, combiná-las na mesma transação e, a partir delas, misturar essas moedas para gerar as transações que irão para o seu destino. Se a operação exigir o reembolso de uma troca, a transação CoinJoin também irá criar essa transação e a enviará para um endereço de troca sob o controle da pessoa a quem essas moedas pertencem. A operação de pagamento CoinJoin somente será realizada quando Maria e João assinarem criptograficamente as suas respectivas transações. No entanto, o truque que o CoinJoin mostra todo o seu poder na *blockchain*. Normalmente, as transações de Maria e João mostravam um padrão claro de envio de moedas. Ou seja, as moedas vão do seu endereço para o endereço de destino. Porém, no CoinJoin, podemos ver uma única transação na qual várias entradas são unidas e há várias saídas. Isto torna mais difícil para terceiros determinar qual destinatário recebeu qual saída. Mesmo o destinatário da transação não pode determinar de qual endereço os fundos recebidos são provenientes, porque os UTXOs não estão diretamente relacionados a um endereço em si, mas a uma transação de várias entradas, todas elas independentes” (O QUE..., c2022).

bitcoin, ela se propaga para outros *nodes* conectados a ele, conhecidos como *peers*. Essa mensagem é propagada em uma reação em cadeia, no que é conhecido como protocolo de fofoca (*gossip protocol*) do *bitcoin*. Depois, há a difusão, momento no qual cada um desses *nodes* transmite transações com atrasos exponenciais e independentes como forma de anonimizar aquela primeira transação (CURRAN, 2018).

Ocorre que o protocolo utilizado pelo *bitcoin* se mostrou vulnerável à detecção do verdadeiro usuário, daí a pesquisa que originou o Dandelion. Esse protocolo possui duas fases, denominadas *stem* e *fluff*. Durante a primeira fase, anônima, em vez de anunciar a transação para todos os *peers* conectados, transmite-se a mensagem para um único *peer* mediante algoritmo aleatório, e assim sucessivamente. Ainda de forma aleatória, um dos *peers* inicia a fase *fluff*, na qual a transação é comunicada à maioria dos *nodes* da rede, de forma que um observador externo somente conseguirá rastreá-la até um dos *nodes* que receberam a mensagem original na primeira fase (HARPER, 2018).

Para encerrar esse capítulo, devemos tratar do advento da computação quântica, que traz consigo capacidade de cálculo absurdamente maior. Desde o momento da ordem até a inscrição na *blockchain* (no caso do *bitcoin*), existe uma janela de oportunidade para que a transação seja manipulada, pode demorar de dez minutos a um dia. Ocorre que a estimativa de capacidade de processamento para permitir essa invasão é estimada em cerca de 317 milhões de *qubits* (unidade de processamento do computador quântico) para realizar essa operação em uma hora, e provavelmente seis vezes mais para realizá-la em dez minutos. Em perspectiva, o maior computador quântico hoje existente possui 127 *qubits*, o que indica que não é uma hipótese provável por um longo tempo. Ainda, há pesquisas em andamento para garantir a segurança de criptoativos, como aquelas realizadas pelo US National Institute of Standards and Technology e pela Ethereum Foundation, o que pode dificultar a quebra da criptografia mesmo para computadores quânticos.

3 A REGULAÇÃO DOS CRIPTOATIVOS NA EUROPA

As características das moedas virtuais que ocultam identidades e transações estimulam o seu emprego no contexto de lavagem de dinheiro, tráfico de drogas e financiamento do terrorismo. É bem representativa dessa situação o caso Silk Road, um mercado *on-line* criado em 2011, na *dark web*, cujas transações se davam somente mediante *bitcoin* e possuía, em seu auge, cerca de 70% de produtos relacionados a drogas.

A página Silk Road, cujo nome foi inspirado na denominada Rota da Seda, utilizada no comércio da seda entre Oriente e Europa em épocas remotas, operava na *dark web* e dedicava-se quase exclusivamente ao comércio de drogas ilícitas, a ponto de receber a alcunha de Amazon das drogas.

A página foi fechada em 2013 depois de uma operação conjunta entre o FBI, DEA, IRS e Customs. Foram apreendidos mais de 144 mil *bitcoins*, um valor total estimado, à época, de 34 milhões de dólares, bem como presos diversos usuários, incluído o fundador, que foi condenado à prisão perpétua sem possibilidade de fiança em 2015 por crimes ligados à distribuição de drogas, inclusive pela internet, e conspiração para violar leis de narcóticos (FRANKENFIELD, 2022; MULLIN, 2015).

Em razão da crescente preocupação com a disseminação de moedas virtuais e seu potencial para acobertar lavagem de dinheiro e financiamento do terrorismo, em junho de 2014 o Grupo de Ação Financeira contra a Lavagem de Dinheiro e o Financiamento do Terrorismo - Gafi/FATF emitiu o seu primeiro informe a respeito de moedas virtuais, no qual constaram definições terminológicas e uma breve análise de riscos potenciais da utilização da tecnologia, como

a pseudoanonimidade e o alcance global, além da distribuição de estruturas de operação em diversos países lenientes no combate à lavagem de dinheiro e ao financiamento do terrorismo (FINANCIAL ACTION TASK FORCE, 2014).

Em junho de 2015, o Gafi/FATF publicou o documento intitulado, em tradução livre, de Diretrizes para uma abordagem baseada em risco para moedas virtuais, com foco em casas de câmbio (*exchangers*) de moedas virtuais conversíveis, visto que são um ponto de interseção entre elas e moeda *fiat* (moeda em curso legal nos países) (FINANCIAL ACTION TASK FORCE, 2015). Nele, constam diversas recomendações, tais como a obrigação de casas de câmbio de moedas virtuais de atuarem com a devida diligência ao realizar conversões entre moeda *fiat* e virtual mediante a identificação dos usuários e pesquisa sobre seu histórico de transações e a comunicação de transações suspeitas de vínculo com lavagem de dinheiro e financiamento do terrorismo.

Em junho de 2019, novo documento foi editado. Concebido como aprimoramento das diretrizes de 2015, ele buscou se atualizar diante de novas tecnologias e aprimorar explicações e exemplos de regulamentação, bem como indicar eventuais dificuldades que os países podem enfrentar na tentativa de regulação da matéria (FINANCIAL ACTION TASK FORCE, 2019). Houve diversas propostas, dentre as quais destacam-se a obrigação de provedores de serviços de bens virtuais de se registrarem perante autoridades nacionais de sua jurisdição de criação e fiscalização por um órgão estatal que goze de prerrogativas de sanção e que coopere internacionalmente com outros países.

Essa diretriz foi atualizada em 2021, após dois relatórios anuais de acompanhamento, para clarificar, de forma abrangente, as definições de ativos virtuais e provedores de serviço de ativos virtuais; exemplificar como os padrões Gafi podem ser aplicados

a *stablecoins* (moedas virtuais com valor atrelado a alguma moeda fiat); prover direcionamento para riscos e ferramentas para que países possam tratar adequadamente as transações *peer-to-peer*, que não passam por provedores de serviço; proporcionar guia atualizado para licenciamento e registro de provedores de serviço de ativos virtuais; possibilitar maior guia para implementação da regra de viagem (mecanismos para prevenção de lavagem de dinheiro correlatos à transferência internacional de valores, notadamente registro de informações completas sobre as pessoas e o objeto da transação, que devem ser aplicados inclusive nas transações nacionais, caso ocorram mediante ativos virtuais); incluir princípios de compartilhamento de informação e cooperação entre entidades de supervisão de provedores de serviço de moedas virtuais. Apresenta, ainda, significativos relatos de implementação de regulação por diversos países (FINANCIAL ACTION TASK FORCE, 2021).

Na linha dos trabalhos do Gafi, o parlamento da União Europeia editou a Diretiva n. 849/2015/EU (alterada pela Diretiva n. 843/2018/UE), em junho de 2015, relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo. Em sua exposição de motivos, aborda expressamente a necessidade de sujeição de ativos virtuais às obrigações de devida diligência quanto ao cliente, guarda e notificação de operações suspeitas aplicáveis às instituições financeiras relacionadas à lavagem de dinheiro e financiamento do terrorismo. Em seu corpo adota, entre outras medidas, a avaliação baseada em risco idealizada pelo Gafi.

Após ataques terroristas que atingiram o norte da Europa em 2015, o Conselho da União Europeia e o Conselho Europeu solicitaram reforços na normativa relacionada à lavagem de dinheiro e ao financiamento do terrorismo para alcançar moedas virtuais, principalmente por meio

de *exchanges* (INGRAO, 2019). A concretização, na União Europeia, de regulamentação de ativos virtuais nesse contexto de prevenção à lavagem de dinheiro e ao financiamento do terrorismo veio na Diretiva n. 843/2018/UE (UNIÃO EUROPEIA, 2018), de junho de 2018, que efetivamente ampliou a Diretiva n. 849/2015/UE (UNIÃO EUROPEIA, 2015) para alcançar também *exchanges* e serviços de carteiras virtuais (*wallets*). Ela também definiu a moeda virtual como representação digital de valor não emitida, nem garantida por um banco central nem por uma autoridade pública, não necessariamente associada a uma moeda estabelecida legalmente, que não possui a natureza jurídica de moeda ou dinheiro, porém aceita por pessoas físicas ou jurídicas como meio de câmbio e que se pode transferir, armazenar ou negociar por meios eletrônicos.

Em fevereiro de 2022, o Banco Central Europeu atendeu a pedidos do Parlamento e do Conselho Europeu para se manifestar a respeito de uma proposta de regulação na prevenção do uso do sistema financeiro para lavagem de dinheiro e financiamento do terrorismo e uma proposta para uma diretiva acerca de mecanismos a serem adotados por estados-membros para a prevenção do uso do sistema financeiro para lavagem de dinheiro e financiamento do terrorismo. O documento publicado, CON/2022/5, elogia a mudança de terminologia adotada pelas diretrizes 2015 e 2018 da União Europeia para substituir o termo moedas virtuais para criptoativos, numa aproximação da definição do Gafi (uma representação digital de valor que pode ser digitalmente comercializada ou transferida, e pode ser usada para pagamento ou para investimento. Criptoativos não incluem representações digitais de moedas *fiat* ou outros ativos financeiros que são tratados em outras recomendações do Gafi) (EUROPEAN CENTRAL BANK, 2022).

4 EXEMPLO CONCRETO: A REGULAÇÃO NA ITÁLIA

A Itália introduziu, em seu ordenamento, legislação para atender às diretrizes da União Europeia: primeiro, o Decreto Legislativo n. 90, de maio de 2017, em atenção à Diretriz n. 849/2015/UE, e depois o Decreto Legislativo n. 125, de outubro de 2019, que corresponde a atualizações acerca da Diretriz n. 843/2018/UE.

Tais decretos legislativos previram a submissão às normas de prevenção de lavagem de dinheiro aplicáveis a instituições financeiras, também de prestadores de serviços relativos à utilização de moedas virtuais e de prestadores de serviços de carteiras digitais (*wallets*).

Os prestadores de serviços relativos à utilização de moedas virtuais foram primeiro conceituados, no Decreto Legislativo n. 90/2017 (ITÁLIA, 2017), como toda pessoa física ou jurídica que fornece a terceiros, a título profissional, serviços funcionais para utilização, troca, conservação de valores virtuais e sua conversão em moeda de curso legal. Depois, alterou-se a definição no Decreto Legislativo n. 125/2019 (ITÁLIA, 2019) para toda pessoa física ou jurídica que fornece, ainda que *on-line*, serviços funcionais para utilização, troca, conservação de valores virtuais e a sua conversão em moeda de curso legal em representações digitais de valor, inclusive aqueles conversíveis em outros valores virtuais, bem como de serviço de emissão, oferta, transferência e compensação e qualquer outro serviço funcional à aquisição, negociação ou intermediação na troca dessas mesmas moedas.

Trata-se de atualização legislativa para incluir expressamente o exercício dessa atividade *on-line*, bem como incluir também a conversão de uma moeda virtual em outra (além de conversão de

moeda virtual em moeda *fiat*) e, por fim, alcançar qualquer serviço acerca de utilização de valores virtuais (de acordo com a diretriz de 2019 do Gafi). Dessa forma, tais pessoas passaram a ser obrigadas a se licenciarem perante uma autoridade administrativa cuja omissão implica uma sanção administrativa que varia entre 2.065 euros e 10.329 euros. São também obrigados a verificar adequadamente a identidade de seus clientes (*know your client*), bem como a comunicar às autoridades qualquer transação no valor de 15.000 euros ou mais. Possuem, ainda, obrigação de guarda de documentos, datas e informações úteis a prevenir lavagem de dinheiro, bem como de fornecer imediatamente tais documentos quando solicitado (SICIGNANO, 2020).

Por sua vez, os prestadores de serviços de carteiras virtuais foram definidos no Decreto Legislativo n. 125/2019 (ITÁLIA, 2019) como toda pessoa física ou jurídica que fornece, a título profissional, ainda que *on-line*, serviços de salvaguarda de chaves eletrônicas privadas em nome dos clientes para deter, memorizar ou transferir moedas virtuais. A tais pessoas se aplicam as mesmas obrigações que alcançam os prestadores de serviços de utilização de moedas virtuais (SICIGNANO, 2020).

Essas pessoas podem sofrer responsabilidade penal e administrativa em razão da omissão em seus deveres contra lavagem de dinheiro. Além de eventualmente poderem responder, em coautoria, pela própria lavagem de dinheiro, há tipos penais que incidem sobre a utilização de dados falsos na atividade, seja dos clientes, seja das transações realizadas; sobre a violação do dever de comunicação de operações suspeitas; e até os clientes podem incidir em crime por fornecer informações de identidade falsa. Esses tipos penais aplicáveis

à atividade econômica de serviços e guarda de moedas virtuais possuem a contraparte administrativa (SICIGNANO, 2020).⁴

5 A REGULAÇÃO DOS CRIPTOATIVOS NO BRASIL

O Brasil ainda não possui um posicionamento estatal homogêneo acerca das moedas virtuais. O primeiro documento oficial que abordou expressamente as criptomoedas foi o Imposto sobre a Renda da Pessoa Física – Perguntas e Respostas, de 2016, publicado pela Receita Federal, no qual ela afirma que, muito embora as moedas virtuais não possam ser classificadas como moeda, em função da Lei. n. 9.069/1995 (BRASIL, 1995), são equiparadas a ativo financeiro, e por isso devem ser declaradas como outros bens, muito embora não haja regra para a conversão de valores para fins tributários, ante a inexistência de cotação oficial.

Em outubro de 2017, a Comissão de Valores Imobiliários – CVM emitiu uma nota a respeito das Initial Coin Offerings – ICOs, na qual afirma que, a depender das características da moeda virtual, pode representar valor mobiliário sujeito à sua regulação nos termos da Lei n. 6.385/1976 (BRASIL, 1976). Em janeiro de 2018, a CVM expediu o Ofício Circular n. 1 que destaca a impossibilidade de qualificação de

⁴ Para uma visão mais completa a respeito da implementação de medidas de prevenção à lavagem de dinheiro e ao financiamento do terrorismo por parte de diversos países, recomenda-se a do segundo acompanhamento anual da padronização de ativos virtuais e provedores de serviço de ativos virtuais, realizada em 2021. Lá, existe um diagnóstico detalhado sobre o número de países que deram início à implementação das medidas sugeridas pelo organismo, notadamente a Recomendação n. 15, que trata da fiscalização e instituição de obrigações de prevenção para aquelas atividades econômicas. Reportou-se que 58 jurisdições haviam a legislação necessária para implementar a Recomendação n. 15, com 35 delas com regime operacional. Para uma abordagem panorâmica das medidas de fato tomadas por diversos países sobre ativos virtuais, que ultrapassa o objetivo desse trabalho, o leitor interessado deve procurar a diretriz Gafi atualizada sobre abordagem baseada em risco de ativos virtuais e de provedores de serviços de ativos virtuais, também de 2021, na qual constam relatadas tais experiências.

moedas virtuais como ativos financeiros, como forma de vedar a sua aquisição direta por fundos de investimentos regulados pelo art. 3º da Instrução CVM n. 555/2014 (TEIXEIRA; BOCHI, 2019).

A Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro - ENCCLA, em 2017, promoveu a Ação n. 8: Elaborar diagnóstico sobre a atual conjuntura da utilização de moedas virtuais e meios de pagamento eletrônico. Ela foi coordenada pelo Bacen e teve como colaboradores a Agência Brasileira de Inteligência, a Associação Nacional dos Delegados de Polícia Federal, a Associação Brasileira de Magistrados, o Banco do Brasil, a Caixa Econômica Federal, o Banco Nacional de Desenvolvimento Econômico e Social, a Controladoria-Geral da União, o Conselho Nacional do Ministério Público, o Coaf, a Comissão de Valores Mobiliários, a Federação Brasileira de Bancos - Febraban, o Gabinete de Segurança Institucional da Presidência da República, o Ministério Público Federal, o Ministério Público do Estado de São Paulo, o Ministério das Relações Exteriores, a Polícia Federal, a Procuradoria-Geral da Fazenda Nacional, a Secretaria da Receita Federal, a Superintendência de Seguros Privados, a Secretaria de Gestão do Ministério de Planejamento e o Tribunal de Contas da União, e demonstra a preocupação conjunta sobre o tema (BOTTINO; TELLES, 2018).

No âmbito do processo legislativo, o Projeto de Lei n. 2.303/2015 (renumerado para PL n. 4401/2021) (BRASIL, 2015), do deputado Áureo Lídio Moreira Ribeiro, dispõe sobre a inclusão das moedas virtuais e dos programas de milhagem aérea na definição de arranjos de pagamento previstos na Lei n. 12.865/2013 (BRASIL, 2013). Ocorre que, como bem pontuado em outra produção acadêmica, o enquadramento é simplesmente inadequado, uma vez que arranjos de pagamento trabalham com intermediários, figura inexistente em negociações de criptomoeda (BOTTINO; TELLES, 2018).

Em 2019, dois projetos foram protocolizados no Senado, Projeto de Lei n. 3.825/2019 (BRASIL, 2019a), do Senador Flávio Arns, e PL n. 3.949 (BRASIL, 2019b), de Styvenson Valentim. Seguiu-se a apresentação do PL n. 4.207/2020 (BRASIL, 2020), de Soraya Thronicke. No dia 22 de fevereiro de 2022, a Comissão de Assuntos Econômicos - CAE do Senado aprovou um substitutivo do Senador Irajá a essas três matérias, que recomenda a aprovação do PL n. 3.825/2019 e prejudicados os outros dois.

Em justificativa, o Senador Flávio Arns se reporta à necessidade de regulamentação do mercado de criptoativos para evitar a sua exploração criminosa e atender à Quinta Diretriz de Prevenção à Lavagem de Dinheiro da União Europeia quanto à regulamentação de *exchanges*.

O PL n. 3.825/2019 conceitua criptoativo como:

[...] a representação digital de valor denominada em sua própria unidade de conta, cujo preço pode ser expresso em moeda soberana local ou estrangeira, transacionado eletronicamente com a utilização de criptografia e/ou de tecnologia de registro distribuído, que pode ser utilizado como forma de investimento, instrumento de transferência de valores ou acesso a bens ou serviços, e que não constitui moeda de curso legal. (BRASIL, 2019a).

Uma *exchange*, por outro lado, é definida como a pessoa jurídica que oferece serviços referentes a operações realizadas “criptoativos em plataforma eletrônica, inclusive intermediação, negociação ou custódia” (BRASIL, 2019b).

A regulação do mercado, bem como do funcionamento de *exchanges*, é atribuída ao Banco Central do Brasil nesse projeto, a quem caberá, inclusive, fomentar a autorregulação do mercado de criptoativos. Independentemente disso, há diretrizes básicas para o licenciamento de uma *exchange*, bem como a previsão de deveres básicos de guarda de informações e diligência adequada acerca da identidade de seus clientes, além de obrigá-las aos deveres da Lei n. 9.613/1998 (dispõe sobre crimes de lavagem e cria Coaf), da Lei n. 13.506/2017 (dispõe sobre processo administrativo sancionador na esfera de atuação do Bacen e CVM), bem como submete a oferta pública de criptoativos que gerem direito de participação, parceria ou remuneração à CVM (o que mantém o entendimento da CVM segundo o qual, nessas hipóteses, o criptoativo se assemelha a título mobiliário). Por fim, consta a inclusão, na Lei n. 7.429/1986 (dispõe sobre crimes contra o sistema financeiro nacional), de tipo penal específico para gestão fraudulenta de *exchange* de criptoativos, com a conhecida figura da gestão temerária e com pena qualificada para gestão fraudulenta mediante pirâmide financeira (BRASIL, 2019b).

Se, por um lado, o projeto de lei tem o mérito de estabelecer uma autoridade estatal para se encarregar do registro oficial e licenciamento da atividade de *exchanges*, de outro, omitiu-se a respeito de *wallets*, que possuem igualmente informações a respeito de titulares de criptoativos, transações e valores (o que inclusive levou ao seu tratamento idêntico às *exchanges* na imensa maioria das iniciativas regulatórias mundiais).

Pode-se, então, seguir dois raciocínios. Primeiro, é possível argumentar que o legislador brasileiro incluiu as *wallets* no conceito de *exchanges* ao se referir à custódia de criptoativos, o que, se não encontra paralelo na realidade, apresenta utilidade para a regulação. Outra interpretação possível é a de que, realmente, a lei é omissa quanto às *wallets*.

Não se pode, entretanto, afirmar que as *wallets* estão indenes de deveres e de escrutínio estatal em se tratando de monitoramento e prevenção de atividades ligadas à lavagem de dinheiro, se realmente prevalecer a interpretação de que a lei é omissa.

O art. 9º, parágrafo único, inciso IV, da Lei n. 9.613/1998 prevê que se sujeitam às obrigações de devida diligência quanto a clientes, guarda de informações sobre transações e comunicação de operações financeiras suspeitas “as administradoras ou empresas que se utilizem de cartão ou qualquer outro meio eletrônico, magnético ou equivalente, que permita a transferência de fundos” (BRASIL, 1998). E é justamente essa a função das carteiras de moedas virtuais: oferecer uma interface amigável para controle e transações. Percebe-se, também, que a lei disciplina, nessa hipótese, a transferência de fundos, e não de dinheiro ou título mobiliário, o que se enquadra na definição corrente no Brasil e também naquela prevista no Projeto de Lei n. 3.825/2019 (BRASIL, 2019a).

É interessante apontar que a Lei n. 9.613/1998 (BRASIL, 1998), ao tratar das obrigações de devida diligência quanto à identificação de clientes, guarda de informações acerca de transações realizadas, prevê que tais atividades empresariais devam ser cadastradas no órgão regulador ou fiscalizador ou, na sua falta, no Coaf; a mesma coisa para os dados coletados de operações suspeitas. Significa então que, na ausência de lei que crie autoridade expressamente responsável por centralizar as diversas operações relativas à regulação de *exchanges* e *wallets*, existe a fixação de um órgão para realizar tais tarefas, e o mesmo ocorrerá se for aprovada lei que trate apenas de *exchanges*.

A existência de tal recurso dá razão parcial ao argumento de que os mecanismos atualmente existentes são suficientes para combater uma ameaça significativa ao sistema financeiro nacional proveniente

de criptomoedas, que não seriam uma tecnologia disruptiva a ponto de exigir mudanças na forma como se dá o combate à lavagem de dinheiro, visto que o processo seria semelhante àquele que hodiernamente ocorre com moedas *fiat* (HERZOG; HOCH, 2021).

A nosso juízo, então, a atividade fiscalizatória brasileira sobre empresas de exploração de criptomoedas não corre o risco de sofrer o revés ocorrido na Alemanha. A Autoridade Federal Alemã de Supervisão Financeira – BaFin classificava continuamente as plataformas de *bitcoin* como instrumentos financeiros na forma de unidades de contagem, de acordo com a Lei do Sistema de Crédito, para obrigá-las e demais prestadoras de serviço à autorização, inclusive sob ameaça de sanção criminal. Em setembro de 2018, a corte judiciária alemã responsável (*Kammergericht*) afastou tal entendimento, o que causou um vácuo legal sobre a matéria que somente foi preenchido mediante a implementação nacional da Diretiva 2018/843/EU (HERZOG; HOCH, 2021).

6 CONCLUSÃO

As novas tecnologias que possibilitam o desenvolvimento das moedas virtuais são disruptivas para o desenvolvimento tecnológico e aplicáveis nos mais diversos segmentos possíveis. No entanto, o potencial das moedas virtuais para lavagem de dinheiro, financiamento do terrorismo e tráfico de drogas é ainda pouco catalogado pelas autoridades, de modo que não pode ser subestimado.

A simples aquisição ou comercialização de moedas virtuais não configura, em si, conduta reprovável, e nisso reside o desafio de sua regulação: estabelecer um ambiente que permita o desenvolvimento da tecnologia sem deixar de coibir empreitadas criminosas.

Sob esse enfoque, os primeiros passos representados pelas diretrizes do Gafi e União Europeia buscam o equilíbrio mediante uma abordagem baseada na avaliação do risco de cada atividade e parecem adequados. E essa adequação se sustenta mesmo perante a crítica da parcial imprestabilidade de se regular atividades de prestadores de serviço, haja vista que é de amplo conhecimento que as criptomoedas dispensam intermediários para sua circulação e há economias que as aceitam como moeda, o que dificulta até mesmo o rastreamento na transposição para o mundo real por meio de aquisição de bens e serviços.

A regulamentação estatal pode, ademais, contribuir para iniciativas de autorregulação, registradas em algumas dessas moedas, que buscam se afastar da pecha de instrumentos da criminalidade organizada.

O Brasil, embora com certo atraso, busca implementar expressamente as diretrizes do Gafi, notadamente quanto à necessidade de licenciamento para atividades de prestação de serviços relacionados a moedas virtuais. O projeto de lei mais recente e que caminha para aprovação possui lacunas, é verdade, mas elas são supridas pela legislação em vigor quanto à lavagem de dinheiro, como demonstrado.

Por fim, as experiências internacionais, aliadas ao modo de funcionamento das criptomoedas, clamam pela regulamentação semelhante e amplo compartilhamento de informações entre países, a fim de mostrar alguma eficácia à altura do desafio.

REFERÊNCIAS

ALAMEDA, Teresa. **Zero knowledge proof**: how to maintain privacy in a data-based world. [S. l.]: BBVA, 23 June 2020. Disponível em: <https://www.bbva.com/en/zero-knowledge-proof-how-to-maintain-privacy-in-a-data-based-world/>. Acesso em: 8 fev. 2022.

ASSIS, Amanda. Criptomoedas e Direito Penal econômico: uma análise à luz do crime de lavagem de dinheiro. **Revista de Direito Penal Econômico e Compliance**, São Paulo, v. 3, p. 65-82, jul./set. 2020.

BASTIANI, Amanda. **O que é e como funciona o Proof of Work?** [S. l.]: CriptoFacil, 5 dez. 2019. Disponível em: <https://www.criptofacil.com/o-que-e-e-como-funciona-o-proof-of-work/>. Acesso em: 1º fev. 2022.

BINDSEIL, Ulrich; PAPSDORF, Patrick; SCHAAF, Jürgen. The encrypted threat: bitcoin's social cost and regulatory responses. **SUERF Policy Note**, Austria, n. 262, p. 1-20, Jan. 2022. Disponível em: https://www.suerf.org/docx/f_88b3febc5798a734026c82c1012408f5_38771_suerf.pdf. Acesso em: 3 fev. 2022.

BOTTINO, Thiago; TELLES, Christiana. Lavagem de dinheiro, Bitcoin e regulação. **Revista Brasileira de Ciências Criminais**, São Paulo, v. 148, p. 131-176, out. 2018.

BRASIL. Câmara dos Deputados. **PL n. 4401/2021 (n. anterior: PL n. 2303/2015)**. Dispõe sobre a inclusão das moedas virtuais e programas de milhagem aéreas na definição de “arranjos de pagamento” sob a supervisão do Banco Central. Autor: Aureo Lidio Moreira Ribeiro. Brasília, DF: Câmara dos Deputados, 2015. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=1555470>. Acesso em: 12 mar. 2022.

BRASIL. **Lei n. 6.385, de 7 de dezembro de 1976**. Dispõe sobre o mercado de valores mobiliários e cria a Comissão de Valores Mobiliários. Brasília, DF: Presidência da República, 1976. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l6385.htm. Acesso em: 12 mar. 2022.

BRASIL. **Lei n. 9.069, de 29 de junho de 1995.** Dispõe sobre o Plano Real, o Sistema Monetário Nacional, estabelece as regras e condições de emissão do REAL e os critérios para conversão das obrigações para o REAL, e dá outras providências. Brasília, DF: Presidência da República, 1995. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/19069.htm. Acesso em: 12 mar. 2022.

BRASIL. **Lei n. 9.613, de 3 de março de 1998.** Dispõe sobre os crimes de “lavagem” ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselho de Controle de Atividades Financeiras – Coaf, e dá outras providências. Brasília, DF: Presidência da República, 1998. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/19613.htm. Acesso em: 28 fev. 2022.

BRASIL. **Lei n. 12.865, de 9 de outubro de 2013.** Autoriza o pagamento de subvenção econômica aos produtores da safra 2011/2012 de cana-de-açúcar e de etanol que especifica e o financiamento da renovação e implantação de canaviais com equalização da taxa de juros [...]. Brasília, DF: Presidência da República, 2013. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12865.htm. Acesso em: 12 mar. 2022.

BRASIL. **Lei n. 13.506, de 13 de novembro de 2017.** Dispõe sobre o processo administrativo sancionador na esfera de atuação do Banco Central do Brasil e da Comissão de Valores Mobiliários [...]. Brasília, DF: Presidência da República, 2017. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13506.htm. Acesso em: 12 mar. 2022.

BRASIL. Senado Federal. **Projeto de Lei n. 3.825, de 2019.** Disciplina os serviços referentes a operações realizadas com criptoativos em plataformas eletrônicas de negociação. Autoria: Senador Flávio Arns (REDE/PR). Brasília, DF: Senado Federal, 2019a. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=7973487&ts=1645677096932&disposition=inline>. Acesso em: 28 fev. 2022.

BRASIL. Senado Federal. **Projeto de Lei n. 3.949, de 2019.** Dispõe sobre transações com moedas virtuais e estabelece condições para o funcionamento das *exchanges* de criptoativos [...]. Iniciativa: Senador Styvenson Valentim (PODEMOS/RN). Brasília, DF: Senado Federal, 2019b. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/137644>. Acesso em: 12 mar. 2022.

BRASIL. Senado Federal. **Projeto de Lei n. 4.207, de 2020.** Dispõe sobre os ativos virtuais e sobre as pessoas jurídicas que exerçam as atividades de intermediação, custódia, distribuição, liquidação, transação, emissão ou gestão desses ativos virtuais, sobre crimes relacionados ao uso fraudulento de ativos virtuais, bem como sobre o aumento de pena para o crime de “pirâmide financeira”, e altera a Lei n. 9.613, de 3 de março de 1998. Iniciativa: Senadora Soraya Thronicke (PSL/MS). Brasília, DF: Senado Federal, 2020. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/144036>. Acesso em: 12 mar. 2022.

CHAVE pública e privada do bitcoin: entenda o que são e como funcionam. [S. /.]: Portal do Bitcoin, 28 set. 2018. Disponível em: <https://portaldobitcoin.uol.com.br/chave-publica-e-privada-do-bitcoin-entenda-o-que-sao-e-como-funcionam/#:-:text=Chaves%20privadas%2C%20o%20que%20s%C3%A3o,ser%20acessada%20por%20outras%20pessoas>. Acesso em: 2 fev. 2022.

CURRAN, Brian. **What is the dandelion protocol?** complete beginner's guide. [S. /.]: Blockonomi, 4 Oct. 2018. Disponível em: <https://blockonomi.com/dandelion-protocol/>. Acesso em 10 fev. 2022.

EFANOV, Dmitry; ROSCHIN, Pavel. The all-pervasiveness of the blockchain technology. **Procedia Computer Science**, Manchester, v. 123, p. 116-121, 2018. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1877050918300206>. Acesso em: 7 fev. 2022.

EUROPEAN CENTRAL BANK. **Opinion of the European Central Bank, of 16 february 2022:** on a proposal for a directive and a regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (CON/2022/5). Frankfurt: ECB, 16 Feb. 2022. Disponível em: <https://www.ecb.europa.eu/pub/pdf/>

other/en_con_2022_5_f_sign~28d246a36e..pdf?0747dd114f0107799ad0b6fcb202233f. Acesso em: 23 fev. 2022.

FINANCIAL ACTION TASK FORCE. **FATF report:** virtual currencies key definitions and potential AML/CFT risks. Paris: FATF/ OECD, June 2014. Disponível em: <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>. Acesso em: 18 fev. 2022.

FINANCIAL ACTION TASK FORCE. **Guidance for a risk-based approach:** virtual currencies. Paris: FATF/ OECD, June 2015. Disponível em: <https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf>. Acesso em: 19 fev. 2022.

FINANCIAL ACTION TASK FORCE. **Guidance for a risk-based approach to virtual assets and virtual asset service providers.** Paris: FATF/ OECD, 21 June 2019. Disponível em: <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html>. Acesso em: 19 fev. 2022.

FINANCIAL ACTION TASK FORCE. **Updated guidance for a risk-based approach to virtual assets and virtual asset service providers.** Paris: FATF/ OECD, Oct. 2021. Disponível em: <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf>. Acesso em: 26 fev. 2022.

FRANKENFIELD, Jake. **Silk Road (website).** [S. /.]: Investopedia, 26 July 2021. Disponível em: <https://www.investopedia.com/terms/s/silk-road.asp>. Acesso em: 16 fev. 2022.

FRANKENFIELD, Jake. **Stealth address (cryptocurrency).** [S. /.]: Investopedia, 25 Feb. 2022. Disponível em: <https://www.investopedia.com/terms/s/stealth-address-cryptocurrency.asp>. Acesso em: 7 fev. 2022.

HARPER, Colin. The anatomy of anonymity: how dandelion could make bitcoin more private. **Bitcoin Magazine**, [s. /.], 29 Aug. 2018. Disponível em: <https://bitcoinmagazine.com/culture/anatomy-anonymity-how-dandelion-could-make-bitcoin-more-private>. Acesso em: 10 fev. 2022.

HERZOG, Felix; HOCH, Temba. Bitcoins e lavagem de dinheiro: um balanço dos casos e das diretrizes regulamentadoras. **Revista de Direito Penal Econômico e Compliance**, São Paulo, v. 2, n. 8, p. 97-114, out./dez. 2021.

INGRAO, Cristina. Gli strumenti di prevenzione nazionali ed europei in materia di valute virtuali e riciclaggio. **Diritto Penale Contemporaneo - Rivista Trimestrale**, Milano, v. 2, p. 148-158, 2019. Disponível em: https://dpc-rivista-trimestrale.criminaljusticenetwork.eu/pdf/DPC_Riv_Trim_2_2019_ingrao.pdf. Acesso em: 19 fev. 2022.

ISMAR, Bruno. **O que é zcash**: confira como funciona e por que esse ativo foi criado! [S. l.]: Renova Invest, 24 mar. 2021. Disponível em: <https://renovainvest.com.br/blog/o-que-e-zcash-confira-como-funciona-e-por-que-esse-ativo-foi-criado/>. Acesso em: 7 fev. 2022.

ITÁLIA. Presidente della Repubblica. **Decreto Legislativo 25 Maggio 2017, n. 90**. Attuazione della direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo e recante modifica delle direttive 2005/60/CE e 2006/70/CE e attuazione del regolamento (UE) n. 2015/847 riguardante i dati informativi che accompagnano i trasferimenti di fondi e che abroga il regolamento (CE) n. 1781/2006. Roma: Presidente della República, 2017. Disponível em: https://www.gazzettaufficiale.it/atto/stampa/serie_generale/originario. Acesso em: 12 mar. 2022.

ITALIA. Presidente della Repubblica. **Decreto Legislativo 4 ottobre 2019, n. 125**. Modifiche ed integrazioni ai decreti legislativi 25 maggio 2017, n. 90 e n. 92, recanti attuazione della direttiva (UE) 2015/849, nonché attuazione della direttiva (UE) 2018/843 che modifica la direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario ai fini di riciclaggio o finanziamento del terrorismo e che modifica le direttive 2009/138/CE e 2013/36/UE. Roma: Presidente della Repubblica, 2019. Disponível em: https://www.gazzettaufficiale.it/atto/stampa/serie_generale/originario. Acesso em: 12 mar. 2022.

LIN, Chia-Chen; CHANG, Chin-Chen; ZHENG, Yao-Zhu. A ring signature based anonymity authentication scheme for group medical consultation. **Symmetry**, [s. l.], v. 12, n. 12, p. 2009, 2020. DOI: <https://doi.org/10.3390/sym12122009>. Disponível em: <https://www.mdpi.com/2073-8994/12/12/2009>. Acesso em: 7 fev. 2022.

MULLIN, Joe. **Ulbricht guilty in silk road online drug-trafficking trial**. [New York]: Arstechnica, 4 Feb. 2015. Disponível em: <https://arstechnica.com/tech-policy/2015/02/ulbricht-guilty-in-silk-road-online-drug-trafficking-trial/>. Acesso em: 16 fev. 2022.

NAKAMOTO, Satoshi. **Bitcoin: a peer-to-peer electronic cash system**. [S. l.]: Bitcoin, 31 Oct. 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 1 fev. 2022.

O QUE é o CoinJoin? [S. l.]: Bit2me Academy, c2022. Disponível em: <https://academy.bit2me.com/pt/o-que-%C3%A9-coinjoin/>. Acesso em: 10 fev. 2022.

PARMAN, Arman the. A comprehensive bitcoin CoinJoin guide: Everything you need to know about utilizing CoinJoin in your bitcoin transactions. **Bitcoin Magazine**, [s. l.], 6 Dec. 2021. Disponível em: <https://bitcoinmagazine.com/technical/a-comprehensive-bitcoin-coinjoin-guide>. Acesso em: 10 fev. 2022.

RAVISETTI, Monisha. **Quantum hackers could break bitcoin in minutes, but don't panic just yet**. [S. l.]: CNET, 8 Feb. 2022. Disponível em: <https://www.cnet.com/news/quantum-hackers-could-break-bitcoin-in-minutes-but-dont-panic-just-yet/>. Acesso em: 28 fev. 2022.

SETH, Shobhit. **The 6 most private cryptocurrencies**. [S. l.]: Investopedia, 4 July 2021. Disponível em: <https://www.investopedia.com/tech/five-most-private-cryptocurrencies/>. Acesso em: 7 fev. 2022.

SICIGNANO, Gaspare. Gli obblighi antiriciclaggio degli operatori in moneta virtuale: verso l'autocertificazione per gli utenti della blockchain? **Diritto Penale Contemporaneo - Rivista Trimestrale**, Milano, v. 4, p. 146-163, 2020. Disponível em: https://dpc-rivista-trimestrale.criminaljusticenetwork.eu/pdf/DPC_Riv_Trim_4_2020_Sicignano.pdf. Acesso em: 23 fev. 2022.

TEIXEIRA, Tarcísio; BOCHI, Bruno Vicentim. Criptomoedas: uma análise sobre a viabilidade de sua regulação. **Revista dos Tribunais**, São Paulo, n. 1000, p. 699-725, fev. 2019.

UNIÃO EUROPEIA. Parlamento Europeu. **Diretiva (UE) n. 2.015/849 do Parlamento Europeu e do Conselho**. Diretiva (UE) n. 2015/849 do Parlamento Europeu e do Conselho, de 20 de maio de 2015, relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo, que altera o Regulamento (UE) n. 648/2012 do Parlamento Europeu e do Conselho, e que revoga a Diretiva n. 2005/60/CE do Parlamento Europeu e do Conselho e a Diretiva n. 2006/70/CE da Comissão. Estrasburgo: Parlamento Europeu, 2015. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32015L0849>. Acesso em: 12 mar. 2022.

UNIÃO EUROPEIA. Parlamento Europeu. **Diretiva (UE) n. 2.018/843 do Parlamento Europeu e do Conselho**. Diretiva (UE) n. 2018/843 do Parlamento Europeu e do Conselho, de 30 de maio de 2018, que altera a Diretiva (UE) n. 2015/849 relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo e que altera as Diretivas n. 2009/138/CE e 2013/36/EU. Estrasburgo: Parlamento Europeu, 2018. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32018L0843>. Acesso em: 12 mar. 2022.

WHAT ARE distributed ledger technologies (DLTs)? [S. /.]: Hedera, c2022. Disponível em: https://hedera.com/learning/what-are-distributed-ledger-technologies-dlts?gclid=CjwKCAiAl-6PBhBCEiwAc2GOVG027Nan8DR3_RsiOYbalelPGfSwmp8jOzGtoZa-VYTzKAoChyYueBoCozgQAvD_BwE. Acesso em: 3 fev. 2022.

WHAT ARE zk-SNARKs? [S. /.]: ZCash, c2021. Disponível em: <https://z.cash/technology/zksnarks/>. Acesso em: 8 fev. 2022.

WHAT IS Ethereum? [S. /.]: Binance Academy, 17 Nov. 2021. Disponível em: <https://academy.binance.com/en/articles/what-is-ethereum#are-ethereum-transactions-private>. Acesso em: 4 fev. 2022.