UNIVERSIDADE CATÓLICA PORTUGUESA

Branqueamento e criptomoedas

Uma análise das novas entidades obrigadas do sistema preventivo

João Pedro da Cunha Teixeira

Mestrado em Direito

Faculdade de Direito | Escola do Porto

2022

UNIVERSIDADE CATÓLICA PORTUGUESA

Branqueamento e criptomoedas

Uma análise das novas entidades obrigadas do sistema preventivo

João Pedro da Cunha Teixeira

Orientador: Pedro Miguel Freitas

Mestrado em Direito

Faculdade de Direito | Escola do Porto

2022

À minha família e aos meus amigos que me apoiaram nos desafios académicos e pessoais.

“Opinion is the medium between knowledge and ignorance”

-Platão

Agradecimentos

Ao meu orientador, Senhor Professor Doutor Pedro Miguel Freitas, quero agradecer pelo apoio e disponibilidade que prestou ao longo da realização deste trabalho.

À Carolina e à Vanessa, por me ajudarem em todo o meu percurso académico.

À Francisca e ao Bernardo, pelo conhecimento que partilharam comigo e por me motivarem sempre que precisei.

À minha família, por ser o meu apoio incondicional em todos os desafios.

RESUMO: O crime de branqueamento acompanhou o fenómeno evolutivo caracterizado pela globalização e modernização tecnológica. Surgiram novos meios de execução do crime que merecem hoje a atenção dos ordenamentos jurídicos. Um destes meios traduz-se na utilização das criptomoedas para a ocultação da origem ilícita das vantagens.

A presente dissertação tem como objetivo analisar criticamente o modo pelo qual as criptomoedas foram incluídas nos atuais sistemas de prevenção de branqueamento. Para tal, será estudada a junção do branqueamento e das criptomoedas, os instrumentos legislativos que se dedicam à prevenção da utilização do sistema económico-financeiro para este crime e quais foram as suas alterações que permitiram englobar as criptomoedas.

ABSTRACT: Money laundering kept up with the evolutionary phenomenon characterized by globalization and technological modernization. New means of executing the crime have emerged that deserve the attention of legal systems today. One of these is the use of cryptocurrencies to hide the illicit origin of the advantages.

The present dissertation aims to critically analyze how cryptocurrencies were included in current money laundering prevention systems. To this end, we'll study the interflow between money laundering and cryptocurrencies, the legislative instruments dedicated to preventing the use of the economic-financial system for this crime and what were their changes that allowed the inclusion of cryptocurrencies.

PALAVRAS-CHAVE: branqueamento, criptomoedas, blockchain, sistema preventivo.

KEY WORDS: money laundering, cryptocurrencies, blockchain, preventive system.

Abreviaturas e siglas

Al. – Alínea

ATMs – Automatic Teller Machines

DCIAP – Departamento Central de Investigação e Ação Penal

ECB – European Central Bank

GAFI/FATF – Grupo de Ação Financeira Internacional / Finantial Action Task Force

ICO – Initial Coin Offering

IMF – International Monetary Fund

N.º – Número

P. – Página

P2P – Peer-to-peer

PoS – Proof of Stake

PoW – Proof of Work

Pp. – Páginas

UIF – Unidade de Informação Financeira

VASP – Virtual Assets Service Provider

VPNs – Virtual Private Networks

Índice

1. Introdução

O branqueamento consiste na prática de atos de dissuasão da origem das vantagens que provêm de um ilícito anterior. Este não é um novo tipo de crime, sendo que sua a origem reporta-se a várias décadas. Não obstante, este fenómeno tem acompanhado a evolução da sociedade e adaptando-se aos seus moldes através do aparecimento de novos meios de execução do crime.

Esta prática, que é suscetível à criminalidade económico-financeira organizada devido à necessidade de desvinculação da origem das vantagens em quantias avultadas, aproveitou a globalização e o desenvolvimento tecnológico que moldaram profundamente a sociedade para modernizar os seus meios de execução.

As criptomoedas, produto destes fenómenos sociais, surgiram como alternativa ao sistema financeiro tradicional, apresentando-se como um novo meio de transação de valores monetários desvinculado das instituições intermediárias.

A evolução do branqueamento também passou pela utilização das criptomoedas na sua execução. Hoje, este novo tipo de branqueamento é uma realidade cada vez mais significativa e que merece a atenção dos ordenamentos jurídicos internacionais.

O regime jurídico nacional atual é composto por dois elementos: o Código Penal, que criminaliza o branqueamento no seu artigo 368.º-A; e o sistema preventivo da Lei n.º 83/2017, que institui medidas de prevenção de utilização de algumas instituições para o branqueamento.

A presente dissertação tem como objetivo analisar as recentes alterações dos sistemas de prevenção da utilização do sistema financeiro para efeitos de branqueamento europeu e nacional que incluíram as entidades relevantes no ecossistema das criptomoedas.

Nos primeiros dois capítulos será estudado o crime de branqueamento, a sua origem, as suas fases de execução e a sua evolução legislativa a nível nacional e internacional. Também será feita uma análise das criptomoedas como nova realidade, explicando sua origem e funcionamento para entender a permeabilidade da sua utilização na prática de crimes, em especial o de branqueamento.

Os últimos dois capítulos serão dedicados à análise das alterações aos sistemas preventivos a nível europeu e nacional que introduziram as criptomoedas e das futuras

alterações de tais sistemas, avaliando se as abordagens tomadas são necessárias ou suficientes para acautelar de modo adequado este meio de branqueamento.

Isto dito, questiona-se: quais alterações foram feitas, tanto a nível nacional como europeu, para que se inclua as criptomoedas no sistema de prevenção de branqueamento? Serão estas alterações suficientes para prevenir a prática deste crime através da utilização deste novo meio de transações?

2. O branqueamento

2.1. Conceito de branqueamento

O conceito de branqueamento não é pacífico na doutrina, tanto a nível nacional como internacional, surgindo várias conceções elaboradas na tentativa de descrever a sua total amplitude.

De acordo com a caracterização apresentada pelo Grupo de Ação Financeira Internacional (GAFI ou *Financial Action Task Force* / FATF), organização que tem servido de base na promoção de estratégias internacionais na luta contra o branqueamento, este é o conjunto de processos ou práticas utilizadas para camuflar a origem ilícita de vantagens provenientes da prática de crimes (FATF/GAFI, 2022).

Originalmente, a este fenómeno associou-se a designação de "branqueamento de capitais", tradução da expressão inglesa *money laundering*, inspirada na dissimulação de vantagens monetárias obtidas através de negócios de lavandarias levada a cabo por Al Capone, um dos notórios nomes da criminalidade organizada, na década de 1920 dos Estados Unidos da América (KYC-Chain, 2019).

Nesta época, conhecida como a "era da proibição", o branqueamento emergiu dado a necessidade de "encobrir" volumes avultados dos capitais que resultavam do crime sobretudo ligado ao tráfico de álcool, cuja comercialização e produção viu-se criminalizada.

A evolução do branqueamento como fenómeno, agora associado a novos crimes e meios de execução, abriu portas a outros tipos de objeto de branqueamento para além de capitais.

Por conseguinte, atualmente não será adequado restringir o objeto do branqueamento a bens monetários (capitais), uma vez que pode ser objeto de branqueamento qualquer bem ou vantagem que provenha de origem ilícita sem qualquer restrição para além das vantagens monetárias, ainda que estas sejam as mais comuns.

Assim, a expressão a adotar deverá ser "branqueamento" quando descrito no Código Penal e como prática criminosa de modo abstrato, que engloba todas as vantagens para além dos capitais. Já será verdadeiramente um "branqueamento de capitais" quando falemos especificamente do encobrimento de vantagens monetárias e do sistema preventivo vocacionado para as instituições que auxiliem a transação de bens monetários.

2.2. Fases do branqueamento

Como o objetivo primordial do crime de branqueamento é o encobrimento das vantagens obtidas de uma prática criminosa antecedente, este será naturalmente um processo complexo, composto por várias atuações distintas.

Com vista a alcançar um melhor entendimento do dinamismo do crime de branqueamento, a doutrina e jurisprudência nacional e internacional, seguindo o entendimento do GAFI, tem desconstruído a prática do crime em três fases essenciais: a colocação, a circulação e a integração (Braguês, 2009, p. 9 a 16; Choo, 2013, p. 8; Duarte, 2002, p. 35 a 39; FATF/GAFI, 2018, pp. 18 e 19, 2022).

A primeira fase, denominada de colocação (ou *placement*), é caracterizada pela introdução dos bens ou vantagens provenientes de origem ilícita no sistema financeiro. Para tal, o agente recorrerá a operações como depósitos bancários, casinos, casas de câmbio ou adquirindo bens não monetários de elevado valor como arte, antiguidades, comércio imobiliário, entre outros.

Tendo em consideração o elevado valor das vantagens normalmente associadas ao crime de branqueamento, assim como a ausência de qualquer disfarce da sua origem ilícita precedente até que alguma transação ocorra, esta fase será inevitavelmente a mais vulnerável à deteção por parte das autoridades de investigação (Forgang, 2019, p. 10) e onde haverá maior controlo das instituições intermediárias que possam estar envolvidas.

De seguida, na fase da circulação (*layering*), o agente procede a uma série de transações financeiras de modo a criar "camadas" (*layers*) que desassociam as vantagens da sua origem. Este será o momento crucial para que a proveniência dos bens seja indetetável, quebrando o seu *papertrail*, isto é, os elementos documentais relevantes que permitem sequenciar o trajeto das vantagens até à sua origem.

Esta fase pode operar através de variadas formas, recorrendo a distintas técnicas conforme o tipo de vantagens, nomeadamente o acesso a fundos de investimento, aquisição de ações e obrigações, transferências para contas anónimas, o recurso a paraísos fiscais e entidades *offshore* no caso do branqueamento de capitais.

Por fim, surge a fase da integração (*integration*), onde as vantagens encontram-se desassociadas da sua origem e aparentemente provenientes de fonte lícita, ou seja, já "branqueadas", e reintegram a esfera patrimonial do agente em circuitos económicos correntes.

Não obstante a vantagem prática que esta tripartição do crime de branqueamento possa ter, especialmente em meio de investigação e prevenção do crime, é necessário enfatizar que o branqueamento pode, por vezes, não respeitar todas as fases acima descritas.

Assim, por exemplo, a fase de colocação pode não existir quando as vantagens do crime estejam já inseridas no sistema financeiro e idóneas a sofrer as operações típicas da fase de circulação. Tal pode acontecer quando as vantagens do crime sejam obtidas por meio em que se possa proceder diretamente à circulação sem que se tenha de introduzir no sistema financeiro.

2.3. Evolução legislativa internacional

A evolução dos mercados financeiros, promovida pela revolução tecnológica e pelo fenómeno da globalização ao longo das últimas décadas, alertou a comunidade internacional para o perigo da consequente cosmopolização da criminalidade organizada, em especial na vertente económico-financeira.

O crime de branqueamento, propício a este tipo de criminalidade, beneficiou desta evolução que não só permitiu novos meios de execução do crime, como permitiu o *fórum shopping* através do aproveitamento de ordenamentos jurídicos deficitários na legislação do branqueamento para lá executar o crime.

Muito rapidamente, o branqueamento viu-se caracterizado como transnacional, o que levou à necessidade da criação instrumentos jurídicos harmonizados e com base na cooperação internacional para combater o fenómeno (Duarte, 2002, p. 41).

Esta procura de uma ordem jurídica internacional uniformizada quanto à criminalização do branqueamento e cooperação entre os vários Estados para a sua prevenção foi iniciada pela Convenção das Nações Unidas contra o Tráfico Ilícito de Estupefacientes e Substâncias Psicotrópicas, de 1988, designada Convenção de Viena.

A Convenção surgiu no âmbito do combate ao tráfico de drogas e, apesar de não definir estas condutas como "branqueamento", incumbiu aos Estados a iniciativa legislativa nas respetivas ordens jurídicas nacionais quanto à sua tipificação penal[1].

[1] *Vide* artigo 3.º, n.º 1, al. b).

Através desta Convenção, tal tipificação do crime de branqueamento começou por ser direcionado às vantagens provenientes de crimes de tráfico de estupefacientes e de substâncias psicotrópicas. Para além da criminalização das condutas típicas do branqueamento, foi dado realce a matérias como auxílio judiciário, extradição, medidas de perda dos produtos obtidos e cooperação entre os Estados[2].

Em 1990 surgiu a Convenção Relativa ao Branqueamento, Deteção, Apreensão e Perda dos Produtos do Crime do Conselho da Europa, denominada de "Convenção de Estrasburgo", que marcou o primeiro alargamento do crime de branqueamento a vantagens provenientes de outros crimes para além dos relacionados com tráfico de droga.

No mesmo sentido, a Convenção das Nações Unidas contra o Crime Organizado Transnacional de 2000, ou "Convenção de Palermo", acompanhou a evolução do crime de branqueamento e alargou o seu âmbito de aplicação, relacionando as vantagens com outros crimes para além dos previstos na Convenção de Viena.

Ademais, esta convenção promoveu a criação de um sistema de prevenção focado nas instituições financeiras, as quais deveriam seguir deveres de identificação de clientes, de manutenção de registos, de comunicação de transações suspeitas e de cooperação com as autoridades nacionais competentes para a investigação do branqueamento[3].

Na perspetiva do Direito da União Europeia, o legislador europeu atuou desde cedo de modo paralelo às convenções internacionais, vinculando os Estados-Membros através das Diretivas dedicadas à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo (designadas *Anti-Money Laundering Directives*).

A primeira destas, a Diretiva 91/308/CEE do Conselho da União Europeia, deu seguimento à Convenção de Viena impondo a criminalização do crime relacionado com o tráfico de estupefacientes, mas promovendo o seu alargamento nas legislações nacionais.

Para além da tipificação do crime, a Diretiva impôs a criação do sistema preventivo orientado na imposição de medidas de diligência quanto à clientela (*customer due diligence*) às entidades financeiras, cuja utilização dos seus serviços é especialmente vulnerável no âmbito de branqueamento de capitais. Estas instituições financeiras sobre as quais recaíam os deveres foram designadas de "entidades obrigadas".

---

[2] *Vide* artigos 5.º a 9.º.
[3] *Vide* artigo 7.º.

A Diretiva 2001/97/CE do Parlamento Europeu e do Conselho (segunda Diretiva relativa à prevenção do branqueamento) alargou o anterior leque de entidades obrigadas, passando a incluir instituições fora do escopo financeiro tais como notários, casinos, agentes imobiliários, entre outros.

Em 2005 a terceira Diretiva relativa à prevenção do branqueamento, a Diretiva 2005/60/CE do Parlamento Europeu e do Conselho, revogou a anterior com vista a aprofundar os deveres de identificação da clientela e de controlo das operações a que as entidades obrigadas deveriam assumir.

Novamente, em 2015 o sistema preventivo foi reformulado pela nova Diretiva. Surge então a quarta Diretiva, 2015/849 do Parlamento Europeu e do Conselho que revogou a antecedente.

O aumento dos mercados digitais e do recurso a ativos virtuais como ferramenta de branqueamento de capitais levou a que o legislador europeu alterasse o regime de 2015 através da Diretiva 2018/843 do Parlamento Europeu e do Conselho, a quinta Diretiva.

Esta recente alteração introduziu no catálogo de entidades obrigadas algumas instituições essenciais na aquisição e armazenamento de criptomoedas para que estas apliquem as medidas de prevenção de branqueamento da Diretiva.

Importa também realçar o papel crucial do GAFI, que guiou a produção legislativa a nível internacional relativa à prevenção do branqueamento. Criado em 1989 na Cimeira do G-7 em Paris[4], o organismo intergovernamental é hoje composto por 37 países e duas organizações internacionais, a Comissão Europeia e o Conselho de Cooperação dos Estados Árabes do Golfo.

Surgiu com o objetivo de promover uma estratégia e cooperação internacional de prevenção do branqueamento e, desde 2001, de combate ao financiamento de terrorismo. Em 1990 o GAFI publicou as "40 Recomendações do GAFI" que aconselharam medidas a adotar pelos Estados para que alcançassem uma harmonia legislativa eficiente na matéria.

Estes textos que têm sido âmbito de revisão e alteração ao longo dos anos não têm valor vinculativo para os Estados ou organizações internacionais, comportando-se como um instrumento de *softlaw* ao invés de *hardlaw*.

Estas Recomendações desenvolvidas pelo GAFI serviram de orientação para vários elementos legislativos, nomeadamente as referidas cinco Diretivas relativas à prevenção

[4] Organização composta pelos 7 países mais industrializados do mundo, são estes Alemanha, Canadá, Estados Unidos, França, Itália, Japão e Reino Unido e também representada a União Europeia.

do branqueamento de capitais que vincularam os Estados-Membros, assim como o sistema preventivo nacional.

2.4. Evolução legislativa nacional

Em 1993 o legislador português tipificou as condutas do branqueamento de capitais no ordenamento jurídico através do Decreto-Lei n.º 15/93, de 22 de janeiro, reproduzindo na legislação nacional o exposto na Convenção de Viena de 1988.

Assim, tal como a Convenção o fez no seu artigo 3.º, nº 1, b), o legislador descreveu no artigo 23.º do Decreto-Lei as condutas de conversão e transferência de bens com o objetivo de ocultar ou dissimular a sua origem ilícita quando esta ilicitude resultasse da prática de crimes de tráfico de estupefacientes.

O Decreto-Lei n.º 313/93, de 15 de setembro, transpôs a primeira Diretiva relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais, criando um sistema preventivo para além da tipificação do crime de branqueamento. Surge, então, uma dualidade de abordagens no ordenamento jurídico interno: a tipificação do crime de branqueamento no Código Penal e o sistema preventivo focado nas entidades financeiras da Lei que transpõe a Diretiva[5].

Nesta senda, este diploma impôs obrigações e deveres de diligência quanto à clientela para a prevenção do branqueamento a um catálogo de entidades que prestam serviços de natureza financeira, cujo incumprimento levaria a consequências em sede contraordenacional.

De seguida, o Decreto-Lei n.º 325/93, de 2 de dezembro, inspirado na Convenção de Estrasburgo de 1990, trouxe alterações ao crime de branqueamento e ao sistema preventivo.

Assim, quanto ao crime de branqueamento, alargou o seu conceito de modo que este deixasse de estar relacionado apenas a bens provenientes de crimes de tráfico de estupefacientes e passasse a incluir origens de crimes de terrorismo, tráfico de armas, extorsão de fundos, rapto, lenocínio, corrupção e outras infrações de relevo.

Já quanto ao sistema preventivo das entidades obrigadas, viu-se uma ampliação o catálogo de tais entidades para além das entidades financeiras, incluindo agora casinos, entidades que exerçam atividades de mediação imobiliária, entre outros.

[5] Não será feita uma análise extensiva do crime de branqueamento do Código Penal, uma vez que o escopo da tese se centra na análise do regime preventivo. Quanto à tipificação do Código Penal, no capítulo 3.6. será feita uma breve integração das condutas de branqueamento através da utilização de criptomoedas na vertente objetiva do tipo legal do crime.

Tanto o Decreto-Lei n.º 313/93, de 15 de setembro, como o Decreto-Lei n.º 325/93, de 2 de dezembro, foram revogados pela Lei n.º 11/2004, de 27 de março, que transpôs a segunda Diretiva relativa à prevenção de branqueamento e que levou a que o crime de branqueamento deixasse de estar previsto em legislação extravagante e passasse a estar tipificado no Código Penal, no seu artigo 368.º-A.

A terceira Diretiva foi transposta em 2008 através da Lei n.º 25/2008, de 5 de junho que, acompanhando a evolução do regime de preventivo internacional, voltou a reformular o regime de prevenção do branqueamento, aumentando o catálogo de entidades obrigadas e os respetivos deveres e obrigações.

A entrada em vigor da Lei n.º 83/2017, de 18 de agosto transpôs a quarta Diretiva e ditou o atual regime do combate ao branqueamento de capitais e ao financiamento do terrorismo a nível nacional.

À luz deste, quando uma entidade se enquadre na lista taxativa dos artigos 3.º e 4.º da referida Lei, cairá no escopo deste regime e, consequentemente, ser-lhe-ão aplicados os respetivos deveres e obrigações apresentados no artigo 11.º e seguintes.

Neste âmbito, destacamos alguns deveres de especial importância na prevenção do branqueamento: o dever de controlo, de identificação e diligência de clientela nos casos do artigo 23.º; o dever de comunicação ao DCIAP e UIF de suspeitas de branqueamento ou financiamento de terrorismo descrito no artigo 43.º; o dever de colaboração com as autoridades e o dever de não divulgação ao cliente de informações relativas a investigações previstos nos artigos 53.º e 54.º, respetivamente; e o dever de abstenção de execução de operações quando haja suspeitas de a origem de bens estar associada a prática de atividades criminosas, consagrado no artigo 47.º.

A Lei n.º 58/2020, de 31 de agosto que procedeu à transposição da quinta Diretiva e que alterou a Lei n.º 83/2017 veio aperfeiçoar este regime, incluindo entidades cruciais nas transações e detenção de criptomoedas. Passaram então a ser incluídas nas entidades obrigadas aquelas que exerçam atividades relacionadas com ativos virtuais[6].

3. As criptomoedas

3.1. Evolução das criptomoedas

O nascimento das criptomoedas está intrinsecamente ligado a um movimento liberal que surgiu na década de 80 e que promoveu a prossecução da privacidade do

[6] *Vide* alínea o) do n.º 1 do artigo 4.º.

indivíduo, especialmente no sistema económico-financeiro, tanto de um ponto de vista da intervenção estadual como de instituições privadas.

Vários ativistas defensores destes ideais acreditavam que a modernização da tecnologia levaria à possibilidade de invasão da esfera privada das pessoas através de uma vigilância por parte dos governos e empresas de aspetos da vida privada das pessoas (De Filippi & Wright, 2018, p. 18).

Estas personalidades defendiam que "os computadores poderiam ser usados para interferir nos estilos de vida, hábitos, locais e associações a partir de dados recolhidos em transações quotidianas dos consumidores" (tradução da minha autoria) (Chaum, 1985, p. 1030).

Tais preocupações manifestaram-se no plano económico-financeiro o que motivou alguns matemáticos, programadores e criptógrafos ativistas, autoproclamados de "*cypherpunks*", a defender a necessidade da criação de um sistema descentralizado de entidades intermediárias e a imprescindibilidade da fusão de criptografia[7] com as transações financeiras para que estas mesmas se mantivessem privadas (Hudges, 1993).

A concretização da teoria de junção da encriptação com os dados das transações foi iniciada pelo criptógrafo americano DAVID CHAUM em 1983, com a publicação do seu estudo "*Blind Signatures For Untraceable Payments*". Neste, CHAUM propôs um sistema de transferência de dinheiro eletrónico que utilizaria um método de encriptação baseado em assinaturas digitais[8], chamado *blind signatures* ou assinaturas cegas (Chaum, 1983, p. 200).

Em 1990, CHAUM aplicou a sua teoria através da criação da moeda virtual *DigiCash* e, em 1994, foi realizado a primeira transação eletrónica (Gates, 2017, p. 19). Contudo, não conseguiu separar a moeda virtual das entidades intermediárias devido ao "problema do gasto duplo" (*double spending*) das moedas, o qual se resume à necessidade de verificação das transações para evitar que um utilizador pudesse enviar ou usufruir da mesma moeda, gastando-a ou enviando-a duplamente.

[7] A criptografia ou encriptação permite a codificação de uma mensagem para que esta apenas possa ser entendida pelo recetor e não por outra entidade externa (Richards, 2021).

[8] O método de encriptação através de assinaturas digitais utilizaria chaves públicas e privadas: permitiria que a parte remetente da mensagem a assinasse com a sua chave privada (uma chave única que apenas a remetente conhece) e, uma vez enviada, a parte recetora poderia verificar a veracidade da assinatura utilizando a chave pública (uma chave única que pode ser conhecida por terceiros) da parte remetente. Apenas com a conjugação das chaves públicas e privadas correta pode a assinatura ser verificada.

A facilidade de replicar dados de um sistema operacional exige que haja um controlo da veracidade dos mesmos, contrariamente ao que acontece com notas e moedas, que têm um suporte físico (De Filippi & Wright, 2018, p. 19).

Este problema é facilmente ultrapassado no sistema bancário tradicional, onde o banco verifica as transações e controla cronologicamente as mesmas para que não haja falsificações no sistema ainda que este seja puramente online.

De igual modo, a empresa de CHAUM teve de funcionar como entidade central que monitorizava as transações, o que levou a que a *DigiCash* nunca fosse uma moeda virtual verdadeiramente descentralizada das instituições.

Em 1998, NICK SZABO tentou resolver o problema do duplo gasto com a teoria para uma nova moeda virtual, "*Bit Gold*", cujo sistema de verificação das transações funcionaria através da validação destas por parte dos próprios utilizadores do sistema.

Para tal, as pessoas que participassem neste sistema abdicariam de poder computacional para a resolução de "puzzles" criptográficos cujas soluções seriam anexadas aos dados das transações, diferenciando-as e validando-as no sistema (Gates, 2017, p. 20).

Todos estes desenvolvimentos e tentativas ao longo das décadas contribuíram para que em 2008 SATOSHI NAKAMOTO, cuja identidade é até hoje desconhecida, conseguisse passar as teorias para um sistema funcional.

Assim, no seguimento da publicação do seu estudo "*Bitcoin: A Peer-to-Peer Electronic Cash System*" (Nakamoto, 2008), NAKAMOTO criou a Bitcoin em 2009, uma moeda virtual que utiliza um sistema de criptografia de assinaturas digitais com chaves públicas e privadas e uma base de dados geral e distribuída que permitia a verificação das transações pelos utilizadores. Tal tecnologia veio a ser conhecida posteriormente como tecnologia *blockchain*.

Este novo meio de pagamento viu-se livre de entidades intermediarias e, portanto, de qualquer escrutínio das transações. Consequentemente, a Bitcoin começou a ser utilizada como o principal meio de pagamento nos mercados virtuais ilegais, como o mercado *Silk Road* entre 2011 e 2013, que se dedicavam à compra e venda de produtos e serviços ilegais. Isto resultou na reputação negativa das criptomoedas nos seus primeiros anos. (Forgang, 2019, p. 5).

Não obstante, devido ao crescimento da utilização da Bitcoin, algumas empresas como a Microsoft, Expedia e, mais recentemente, a Tesla começaram a aceitar Bitcoins como um meio de pagamento para os seus produtos e serviços (Martucci, 2021).

Entretanto, muitas outras criptomoedas surgiram, algumas baseadas em protocolos idênticos ao da Bitcoin e outros diferentes e mais eficazes, como o caso da moeda Ethereum.

3.2. Definição de Criptomoedas

A definição de criptomoedas e o seu enquadramento no sistema económico-financeiro depende de uma prévia análise e distinção dos vários tipos de moedas: moedas fiduciárias, moeda eletrónica (*e-money*), moedas digitais (*digital currencies*) e moedas virtuais (*virtual currencies*).

As moedas fiduciárias (moeda no seu sentido mais tradicional) são as moedas com estatuto de curso legal e que e são normalmente usadas e aceites como meio de troca no país de emissão, como o Euro.

Segundo o Banco de Portugal, a designação de um bem como moeda dependerá da verificação de três funções essenciais: meio de troca, unidade de conta e reserva de valor, para a qual sua estabilidade de valor ao longo do tempo é fundamental (Banco de Portugal, 2020, p. 3). As moedas fiduciárias podem assumir forma física, como moedas e notas, ou não física, como a moeda eletrônica.

Quanto às moedas digitais, estas são representações de valor monetário guardadas ou transferidas por qualquer meio eletrónico. Podem representar o valor denominado em curso legal ou o seu próprio valor baseado na lei de oferta e procura e não na moeda fiduciária (Girasa, 2018, p. 8). Dentro destas, podemos ter a moeda eletrónica e as moedas virtuais.

O legislador europeu, na Diretiva 2009/110/CE do Parlamento Europeu e do Conselho, de 16 de setembro de 2009, definiu moeda eletrónica como o

> valor monetário armazenado eletronicamente, inclusive de forma magnética, representado por um crédito sobre o emitente e emitido após receção de fundos para fazer operações de pagamento e que seja aceite por uma pessoa singular ou coletiva diferente do emitente de moeda eletrónica.

De modo mais abreviado, o GAFI considerou a moeda digital como um mecanismo de transferência digital de moedas fiduciárias, isto é, que têm o estatuto de curso legal (FATF/GAFI, 2014, p. 4). Um exemplo será o pagamento de um produto ou serviço através de *Paypal*.

Já quanto às moedas virtuais, o Banco Central Europeu (ECB) definiu-as, em 2015, como "uma representação digital de valor, não emitida por um banco central, instituição

de crédito ou instituição de moeda eletrónica, que, em algumas circunstâncias, pode ser usada como uma alternativa ao dinheiro" (European Central Bank, 2015, p. 4).

Podemos subdividir três tipos de moedas virtuais: (1) as moedas virtuais fechadas, que apenas podem ser usadas em sistemas virtuais fechados (ex.: as moedas utilizadas dentro de um videojogo); (2) as moedas virtuais que estão unilateralmente relacionadas com a economia "real", que podem ser adquiridas com moedas fiduciárias mas não podem ser inversamente vendidas (ex.: *Facebook Credits*); e (3) as moedas virtuais com uma relação bilateral com a economia "real", isto é, que podem ser adquiridas e vendidas por moedas fiduciárias a uma taxa de conversão (ex.: Bitcoin) (European Central Bank, 2015, p. 6).

As criptomoedas enquadram-se nesta última subcategoria de moedas virtuais, ou seja, são moedas virtuais que podem ser compradas e vendidas através da moeda "tradicional".

Isto dito, podemos caracterizar as criptomoedas como uma representação digital de valor convertível em moeda fiduciária e vice-versa, independente de qualquer instituição intermediária (descentralizada). Baseiam-se num mecanismo matemático de criptografia e as informações relativas às suas transferências são guardadas numa base de dados distribuída por toda a rede.

3.3. A tecnologia *blockchain* como base das criptomoedas

A tecnologia *blockchain* é a base de funcionamento das criptomoedas e das suas transações. É uma base de dados que grava dados em "blocos" que são juntos entre si e inseparáveis.

A sua origem coincide com a criação da primeira criptomoeda, Bitcoin, em 2008, através da publicação do seu estudo "*Bitcoin: A Peer-to-Peer Electronic Cash System*" no qual SATOSHI NAKAMOTO descreveu o funcionamento da primeira *blockchain* que serviria de base para o registo de dados de transações de Bitcoins (apesar de nunca intitular esta tecnologia como "*blockchain*" no seu estudo).

Esta tecnologia conduziu à realização de um objetivo primordial na criação das criptomoedas: a criação uma base de dados descentralizada, isto é, independente de qualquer entidade que controlasse a verificação dos dados registados, mas que impedisse qualquer moeda fosse duplamente gasta ou transacionada.

A descentralização pôde ser alcançada devido ao seu funcionamento como uma base de dados distribuída: as adições de dados são efetuadas por qualquer membro da rede, criando um novo "bloco" de dados que é partilhado com todos os membros da rede

(World Bank Group, 2017, p. 1). Estes membros da rede estarão encarregues de coletivamente validar as adições feitas que, uma vez validadas, integrarão na base de dados num novo bloco.

Cada bloco de informação é composto por um "título" e pelo corpo que contém dados ou informações (no caso das criptomoedas, os dados das transações). O "título" de cada bloco contém uma referência do título (o código *hash*) do bloco anterior e da data em que este novo foi adicionado, criando uma conexão sucessiva entre os títulos dos blocos que referenciam sempre o anterior, elaborando uma "corrente" (*chain*) de blocos em que uma vez adicionados não podem ser alterados ou removidos.

O mecanismo de verificação coletiva de novos blocos, denominado "mecanismo de consenso" (*consensus mechanism*), que NAKAMOTO propôs foi o essencial para resolver o problema do duplo gasto de moedas. Como se trata de uma rede descentralizada, as novas informações não serão validadas por uma entidade intermediária (como um banco que verifica a veracidade de uma transação), serão validadas pelos próprios membros da rede em conjunto.

Estes mecanismos podem ser estruturados de variadas formas, sendo que as duas estruturas mais relevantes são *Proof of Work* (PoW) e *Proof of Stake* (PoS) (Houben & Snyers, 2018, p. 18). Sem descartar a importância das restantes estruturas de mecanismos de consenso, focar-nos-emos numa breve análise do funcionamento do PoW, que serve de base para as principais criptomoedas no mercado atual como a Bitcoin, Monero, Litecoin, entre outras.

O mecanismo PoW recorre a um processo chamado mineração (*mining*) que, nas palavras de DAVID SILVA RAMALHO e NUNO IGREJA MATOS, consiste num "sistema de esforço e recompensa em que vários utilizadores da rede competem entre si para decifrar um código que simultaneamente lhes permitirá receber uma compensação (…) e introduzir um conjunto de transacções na blockchain" (Ramalho & Matos, 2020, p. 86).

Neste sistema, os participantes resolverão operações matemáticas investindo poder computacional que irá permitir adicionar novos blocos à *blockchain*. Os participantes que se dedicam a estas operações são designados mineradores ou "*miners*".

As operações por eles realizadas consistem numa junção da informação previamente gravada na *blockchain* com a informação que será gravada no seguinte bloco (que aguarda numa "lista de espera" conhecida por *memory pool* ou *mempool*), criando um novo bloco intrinsecamente ligado aos anteriores.

Chegando à solução da operação necessária para adicionar a nova informação à *blockchain*, esta será verificada pelos membros da rede como correta e a nova informação integrará na base de dados.

Quando um participante apresenta uma solução válida de um destes problemas matemáticos e, consequentemente, prova o seu investimento (daqui surge o nome "*Proof of Work*"), será recompensado monetariamente. Esta recompensa trás incentivo aos participantes que ajudem a base de dados crescer e, no caso das criptomoedas, promove a sua circulação (Nakamoto, 2008, p. 4).

O crescimento da blockchain resulta no aumento progressivo da complexidade das operações a que a mineração se dedica. Atualmente, esta complexidade exige um poder computacional tão elevado que o custo da eletricidade e o hardware necessário fez com que a mineração da principal moeda Bitcoin não fosse rentável a nível individual (Ramalho & Matos, 2020, p. 88).

Outros mecanismos de consenso surgiram como alternativas mais eficientes quanto aos custos necessários para promover o crescimento da rede, tal como o mecanismo PoS.

3.4. Principais entidades que participam no ecossistema das criptomoedas

O ecossistema das transações de criptomoedas consiste em novas entidades que não estão presentes nos esquemas financeiros tradicionais de moeda fiduciária (European Central Bank, 2015, p. 7). A análise destes novos participantes essenciais para o funcionamento de uma criptomoeda é necessária para uma subsequente interpretação da extensão normativa do legislador.

Em primeiro, salientamos os utilizadores das criptomoedas, a entidade mais comum neste ecossistema. O GAFI define o utilizador como "pessoa ou entidade que obtém moedas virtuais e que as usa para comprar bens ou serviços, reais ou virtuais; ou que as transfere a título pessoal para outra pessoa; ou que as detém como um investimento pessoal" (tradução da minha autoria) (FATF/GAFI, 2014, p. 7).

O utilizador pode obter as criptomoedas através de vários modos tais como a troca com moeda fiduciária num serviço de câmbio, participação em atividades em que seja premiado com ativos virtuais (por exemplo, na distribuição inicial de uma criptomoeda), a prática da atividade de mineração, entre outros.

Os *miners* são as entidades que se dedicam ao processo de mineração através da disponibilização de poder computacional para a resolução de problemas matemáticos necessários para a validação das transações, promovendo o crescimento de uma

blockchain baseada no sistema PoW (sem descartar a possibilidade de atividades equivalentes noutros sistemas para além deste).

O nome que se deu a este processo e às pessoas que a ele se dedicam é uma analogia ao esforço da mineração de minerais do solo (European Central Bank, 2015, p. 7). Os *miners* podem exercer a atividade individualmente como também podem exercer em grupo que gere um negócio dedicado à mineração, designados *pools of miners* (Commission Staff Working Document, 2017, p. 85).

As criptomoedas são geralmente adquiridas através de mercados de câmbio (*virtual currency exchanges*), entidades que prestam serviços de troca de ativos virtuais cobrando uma taxa de transação (Houben & Snyers, 2018, pp. 26 e 27). Podem dedicar-se à troca entre moedas virtuais e moedas fiduciárias (*crypto-to-fiat exchanges*) ou entre moedas fiduciárias entre si (*crypto-to-crypto exchanges*).

Ambos podem ser centralizados, quando a entidade encarregue do mercado participa diretamente como intermediário na compra e venda, ou descentralizados (*peer-to-peer exchanges* ou *P2P exchanges*), quando o próprio mercado não compra nem vende os ativos virtuais, apenas permitindo a negociação direta entre as partes (Haffke et al., 2020, p. 4).

As carteiras digitais armazenam as chaves públicas e privadas do utilizador que serão necessárias para as transações das criptomoedas. Através do acesso às carteiras, o utilizador pode também consultar o saldo, ver o histórico das movimentações e realizar novas transações.

Podemos distinguir as carteiras online (também denominadas *hot storage*), nas quais o armazenamento das chaves é realizado através de *software* na internet, e as carteiras offline (*cold storage*), onde o armazenamento é realizado através de dispositivos *hardware*, isto é, dispositivos físicos.

As carteiras digitais podem ser adquiridas através dos prestadores de carteiras, que se dedicam à venda de *software* e/ou *hardware* que permitem o armazenamento das chaves criptográficas por parte do utilizador e o acesso às redes *blockchains*. Já os prestadores de serviços de custódia de carteiras guardam as chaves privadas dos utilizadores em nome destes (Houben & Snyers, 2018, p. 27).

Por fim, resta mencionar o papel de algumas das entidades que participam na fase inicial de cada criptomoeda: os criadores da criptomoeda e as entidades encarregues da sua distribuição inicial.

Os criadores da criptomoeda são entidades que desenvolvem as bases tecnológicas do funcionamento da criptomoeda e as respetivas regras, é o caso de SATOSHI NAKAMOTO e a Bitcoin.

Já as entidades encarregues da distribuição inicial da criptomoeda (os *coin offerors*) distribuem unidades de criptomoedas após o seu lançamento inicial mediante pagamento por parte dos interessados ou, por vezes, sem qualquer contrapartida monetária, de modo a incentivar a circulação e a sua adoção em massa num processo conhecido por "*airdrop distribution*" (European Central Bank, 2015, p. 7).

3.5. Risco de utilização de criptomoedas para a prática de crimes

A criação das criptomoedas teve como principal objetivo a introdução de uma alternativa à moeda fiduciária no sistema económico-financeiro, um novo método de transacionar valores monetários que não dependesse de uma instituição central e que fosse imune a qualquer intervenção na privacidade dos seus utilizadores.

Esta ausência de uma entidade controladora em conjunto com o foco na privacidade dos utilizadores abriu portas a transações sem medidas de controlo e, consequentemente, possibilitou o uso das criptomoedas como instrumento auxiliar da prática de crimes.

Não obstante as diferenças de cada criptomoeda e das tecnologias em que se baseiam, existe um conjunto de características gerais deste tipo de ativos que reforça o risco da sua utilização na prática de ilícitos, destacando-se: o anonimato, a descentralização, a natureza tipicamente internacional, a incoerência normativa internacional na sua regulação e o imediatismo e irreversibilidade das transações.

A tecnologia *blockchain* baseia-se no princípio de distribuição da base de dados por toda a rede. Este tipo de base de dados aplicado ao universo das criptomoedas significa que lá serão guardadas todas as informações relativas às suas transações, incluindo os dados do remetente, do destinatário, o montante, a data de cada transferência e o montante de cada conta, algo que pode ser acedido por todos os utilizadores.

Apesar disto, as criptomoedas são caracterizadas por um anonimato quanto à identidade dos seus utilizadores. A cada utilizador é atribuída uma chave pública que funciona como endereço pessoal, contudo, os protocolos das criptomoedas não exigem que a este endereço esteja associado qualquer informação sobre a verdadeira identidade de quem a detém, ao contrário do que acontece com o sistema financeiro tradicional. Há então uma separação entre o endereço do utilizador e a sua verdadeira identidade.

Alguns autores defendem que este anonimato típico das criptomoedas pode, por vezes, traduzir-se num quase-anonimato ou *pseudonimização* (Ramalho & Matos, 2020,

p. 94) visto que como as informações de todas as transações são guardadas na base de dados, é geralmente possível identificar a verdadeira identidade do utilizador se for investido um elevado esforço para tal (U. Breu & G. Seitx, 2018, p. 6), algo que não pode acontecer com meios totalmente anónimos como no caso do pagamento em dinheiro físico.

Neste sentido o Fundo Monetário Internacional caracteriza as criptomoedas como meios "mais transparentes do que dinheiro, mas mais anónimos do que outras formas de pagamento online" (tradução da minha autoria) (IMF Staff Discussion Note, 2016, p. 9).

Note-se que existem criptomoedas dedicadas a contornar esta *pseudonimização*, acrescentando para o efeito uma nova camada de privacidade, as denominadas "moedas de privacidade" (*privacy coins*). Para tal, moedas como Monero adotam um protocolo que muda os endereços dos utilizadores a cada transação e não revela as informações das transações na sua base de dados (Forgang, 2019, p. 8).

O anonimato que as criptomoedas permitem alcançar, seja este parcial ou completo, abre portas à sua utilização na prática de crimes, criando obstáculos na sua investigação ao dificultar ou impossibilitar a descoberta da verdadeira identidade dos agentes do crime.

Uma segunda característica que potencia este risco de prática de ilícitos é a descentralização e a respetiva ausência de entidade intermediária. No sistema económico-financeiro tradicional, o foco regulatório é direcionado para as entidades intermediárias que se assumem como núcleos das transações, tais como os bancos. Assim, estas instituições identificam os clientes e transações suspeitas, prevenindo a prática de crimes através dos seus serviços.

Um exemplo de tal regulação é o próprio esquema europeu de prevenção de branqueamento de capitais e financiamento de terrorismo que, mais tarde, se alargou para outras instituições para além das financeiras tradicionais.

O ecossistema das criptomoedas baseia-se em bases de dados *blockchain* que dispensa qualquer instituição intermediária, o que resulta na dificuldade em aplicar os sistemas preventivos já existentes na ordem jurídica e fragilizando a estrutura de combate ao crime.

Os desafios regulatórios são ainda mais evidentes quando se considera a natureza intrinsecamente internacional das criptomoedas. Trata-se de um sistema de transferências baseado na constante atualização dos utilizadores quanto às informações de toda a base de dados, o que implica que as criptomoedas são, obrigatoriamente, acompanhadas pelo

fenómeno da internet. É através da internet que se realizam e se validam transferências para que sejam consensualmente aceites pela rede.

Consequentemente, todos estes fenómenos relacionados com o funcionamento de uma criptomoeda não serão confrontados com barreiras estaduais: vários utilizadores, *miners* e entidades que prestam os serviços de câmbio podem operar na mesma rede *blockchain* em países ou continentes completamente distintos.

Nesta senda, a ausência de coerência legislativa num fenómeno naturalmente internacional trará dificuldades na abordagem preventiva e, por outro lado, permite aos agentes do crime atuar em ordenamentos legislativos que não tenham adotado medidas eficientes para a prevenção destes fenómenos.

Por fim, as transferências de criptomoedas são imediatas e irreversíveis. O imediatismo das transferências deve-se ao facto do constante funcionamento de uma *blockchain* e dos seus *miners*.

A tentativa de adição das novas transferências realizadas e em espera na *memory pool* por parte dos *miners* será sempre o mais imediato possível, isto porque o primeiro *miner* que conseguir encontrar a solução para a junção dos dados necessários para introduzir a nova transferência na rede receberá o respetivo incentivo monetário, ou seja, há um incentivo para que o *miner* seja o mais rápido possível.

Uma vez adicionada a transação, a nova formulação da *blockchain*, que inclui agora os dados da nova transferência, será distribuída por cada utilizador para que a rede se mantenha atualizada. Reverter uma transação implicaria alterar as "cópias" da base de dados de todos os utilizadores que participam nessa *blockchain* (de Barros, 2019, p. 10), o que não será possível devido à inexistência de uma entidade central encarregue de gerir e alterar os dados já previamente guardados pelos utilizadores.

Vários estudos foram realizados para analisar se efetivamente estas características das criptomoedas levam à sua utilização na prática de crimes. O caso mais evidente é a participação das criptomoedas na compra e venda de produtos e serviços ilícitos.

Rapidamente se chegou à conclusão que as criptomoedas são o meio de pagamento preferido nos mercados ilícitos online, onde são negociados produtos ilegais tais como armas, estupefacientes, material pornográfico ilegal, documentos falsificados e serviços ilegais como *software* dedicado a realizar ataques informáticos (Tziakouris, 2018, p. 93).

Num estudo realizado em 2019, concluiu-se que entre janeiro de 2017 e março de 2018, 99.8 % dos endereços que transacionavam nos mercados ilícitos da *Dark Web*[9] operavam através de Bitcoin e que, desses, mais de 80 % se destinavam a fins ilícitos (Lee et al., 2019, p. 2).

Em 2020 NAOKI HIRAMOTO e YOICHI TSUCHIYA dedicaram-se a examinar a dimensão destes mercados ilícitos onde as transações são efetuadas através de criptomoedas (Hiramoto & Tsuchiya, 2020, pp. 1 e 2). Para tal, os autores analisaram o volume de mercado assim como o meio e valor médio das transferências dos sete mercados com maior relevância na *Dark Web* que operaram entre 2011 e 2017: *SilkRoad, Silk Road 2.0, Agora, Evolution, Nucleus, Abraxas* e *AlphaBay*.

Nesta investigação os autores concluíram que o volume de vendas dos mercados correspondeu a 161 milhões de dólares em 2013, 227 milhões de dólares em 2014 e 366 milhões de dólares em 2015 (Hiramoto & Tsuchiya, 2020, p. 6).

Ademais, a grande maioria das transações correspondiam a valores inferiores a 100 dólares, o que demonstra que a compra de produtos ilícitos destina-se maioritariamente para consumo próprio e não para a sua revenda (Hiramoto & Tsuchiya, 2020, p. 2).

3.6. Utilização de criptomoedas no crime de branqueamento

A facilidade de acesso aos meios tecnológicos necessários para as transações de moedas virtuais em conjunto com as características que propiciam a sua utilização para a prática de crimes aqui enunciadas possibilitaram a utilização das criptomoedas no branqueamento de capitais. Surgiu, então, um novo modo de dissimulação da origem criminosa do património.

Analisaremos de seguida como é que o recurso aos ativos virtuais pode integrar-se na estrutura tripartida do crime, sem descartar a possível ausência de alguma das fases tradicionais.

Na fase da colocação, o agente do crime irá, geralmente, introduzir as vantagens de origem ilícita no sistema financeiro através da compra de criptomoedas. Para adquirir as criptomoedas de modo anónimo, é comum recorrer a mercados de câmbio em ordenamentos jurídicos com legislação deficitária na prevenção do branqueamento e a ATMs (*Automatic Teller Machines*) que oferecem simplicidade nas transações devido à sua abundância e por permitir criar novas carteiras virtuais (Teichmann & Falker, 2020, p. 7).

[9] *Dark Web* refere-se a uma parcela da internet que apenas é acessível através de *software* específico, como o motor de pesquisa "Tor Browser" (Hiramoto & Tsuchiya, 2020, p. 2).

A instantaneidade das transações entre moedas fiduciárias e criptomoedas proporciona a rápida movimentação dos valores para instituições em países estrangeiros, processo que seria tradicionalmente mais demorado e consequentemente mais escrutinado (Ramalho & Matos, 2020, p. 104).

Uma vez adquiridas as criptomoedas e já na fase de circulação, o agente do crime poderá executar várias transações para encobrir a origem das vantagens. Para isso, recorre-se a um processo chamado *chain-hopping*, realizando trocas entre a criptomoeda original por muitas outras diferentes através de vários mercados de câmbio e várias contas para desorientar o seu registo eletrónico e dificultar a descoberta da sua origem (Kelly, 2017).

Novamente, nesta fase o imediatismo das transações deixa pouco espaço para a deteção de suspeitas de branqueamento por parte dos mercados de câmbio e faculta um processo de circulação rápido (Choo, 2015, p. 303).

A fase de circulação poderá ainda ser facilitada através do recurso aos prestadores de serviços de mistura (denominados *mixers* / *tumblers*). Estes são mecanismos de reforço de anonimização e de obscurecimento da origem das criptomoedas transacionadas (FATF/GAFI, 2014, p. 6).

Para poder alcançar um maior anonimato, o misturador recolhe as criptomoedas dos utilizadores que pretendem usufruir do serviço num mesmo endereço, no qual executa uma série de transações com criptomoedas de outros utilizadores e de seguida envia para um endereço do recetor.

Deste modo, o processo de circulação será autonomizado e o registo de transações será aleatorizado, o que dificultará a descoberta da proveniência e do recetor e destinatário das criptomoedas.

Todo o processo de circulação, seja qual for o seu método, poderá ser executado através de motores de navegação dedicados à privacidade do utilizador como o Tor Browser e utilizando de VPNs (*Virtual Private Networks*), que dificultará a descoberta da verdadeira identidade do autor das transações e adiciona outra camada de anonimato (Teichmann & Falker, 2020, p. 8).

Finalmente, na fase da integração, as várias criptomoedas são convertidas diretamente ou para moedas fiduciárias ou utilizadas na compra direta de bens e serviços. Esta última fase beneficia das mesmas vantagens da fase da integração, visto que a venda de criptomoedas poderá ser feita nos mesmos moldes em que foi inicialmente comprada, isto é, através de mercados de câmbio, ATMs, entre outros.

Note-se que este esquema tripartido do crime de branqueamento pode por vezes sofrer alterações com a utilização destas novas tecnologias. Tal acontecerá, por exemplo, se o agente de um crime precedente receber as suas vantagens já em criptomoedas prontas para circular. Neste caso, não haverá a fase de colocação, uma vez que as vantagens já se encontram à partida no sistema financeiro.

A própria ação de colocação e integração pode ser idónea a dissimular a origem das vantagens: o agente pode adquirir uma criptomoeda dedicada à privacidade, as ditas moedas de privacidade, tal como Monero ou Zcash e, de seguida, reconverter para moeda fiduciária, sem proceder a qualquer transação entre criptomoedas.

Neste caso houve colocação e integração, mas não houve a fase de circulação, uma vez que a simples compra de uma moeda de privacidade pode dissimular a origem do dinheiro.

Apesar do processo *chain-hopping* ser o mais comum dos esquemas de branqueamento, outras modalidades podem surgir através da utilização de criptomoedas. É o caso dos casinos online, através dos quais o agente pode transferir os seus fundos de criptomoedas para o casino online e de seguida retirá-los sem que gaste um montante mínimo de dinheiro.

Muitos destes casinos online aceitam como pagamento criptomoedas e alguns não possuem regras de fiscalização adequadas como acontece nas instituições financeiras (Forgang, 2019, p. 16).

A lavagem de dinheiro também pode ocorrer nos modelos mais tradicionais de transferências entre diferentes contas através do esquema de branqueamento denominado *smurfing*. Neste, várias pessoas executam as transações de compra e venda de criptomoedas em nome do agente do crime para que estas transações entre utilizadores diferentes e de menores valores dificulte qualquer suspeita da prática de branqueamento (Forgang, 2019, p. 14).

O branqueamento também pode ser conduzido através da aquisição de ativos virtuais em ICOs (*Initial Coin Offerings*). Numa ICO a entidade encarregue procura o investimento por parte dos utilizadores no novo ativo virtual, que comprarão o produto na espectativa da valorização crescente do seu valor.

Nesta situação, um agente de um crime procedente que tencione encobrir a origem ilícita das vantagens pode comprar estes ativos virtuais diretamente de um utilizador que os detenha após adquiridos numa ICO. Com isto, o agente do crime adquiriu um ativo

virtual que legitima a origem da vantagem, através da suposta aquisição numa ICO, desvinculando a sua origem ilícita (A.V., 2018, p. 210).

Não haverá dúvidas que todos estes meios de branqueamento através das criptomoedas enquadrar-se-ão no tipo legal do artigo 368.º-A do Código Penal, cujo tipo objetivo consiste nas ações descritas nos n.ºs 3 e 4 do artigo.

Neste sentido, facilmente se chega à conclusão de que a aquisição de criptomoedas com as vantagens do crime seguidas dos processos anteriormente descritos serão ações de conversão e transferência de vantagens, com o fim de dissimular a sua origem ilícita ou impedir a perseguição criminal e que levarão à ocultação ou dissimulação da sua verdadeira natureza.

Como se trata de um crime comum, não será necessária qualquer característica específica do agente que o pratica. Todavia, já será essencial analisar o tipo ilícito que origina as vantagens a branquear. Estas serão todas as vantagens patrimoniais, ou seja, direitos ou coisas que provenham diretamente da prática dos crimes precedentes a que se refere o n.º 1 do artigo[10], assim como os bens que sejam adquiridos através destas vantagens (Albuquerque, 2021, p. 1233).

Ora, se um agente adquire criptomoedas com as vantagens de um crime precedente que se enquadre neste n.º 1 e, por qualquer meio, oculte ou dissimule tais vantagens, como por exemplo através do recurso aos serviços de mistura de criptomoedas, responderá pelo crime de branqueamento do Código Penal.

Apesar da prática do crime de branqueamento através de criptomoedas não ser mais comum do que os outros meios mais tradicionais, alguns artigos apontam para o seu progressivo crescimento e alertam para os seus perigos.

Segundo Rob Wainwright, Diretor Executivo da Europol entre 2009 e 2018, cerca de 3 a 4% das vantagens provenientes da prática de crimes anuais do continente europeu, que equivale ao valor de 3,5 mil milhões a 4,7 mil milhões de euros, são branqueados através do uso de criptomoedas (Marsali, 2018).

Já a empresa CipherTrace, que se dedica ao estudo de criptomoedas, analisou 45 milhões de transações realizadas entre 2009 e 2018, concluindo que mais de 2 mil milhões de euros foram branqueados utilizando apenas Bitcoins e que 97% das transações de

[10] O n.º 1 do artigo 368.º-A do Código Penal adota um critério misto (Albuquerque, 2021, p. 1233), ao incluir uma cláusula geral, que alude a todos os factos ilícitos típicos puníveis com pena de prisão de duração mínima superior a seis meses ou de duração máxima superior a cinco anos, e um catálogo de crimes previsto nas alíneas do n.º 1 do artigo, ampliado pela Lei n.º 58/2020.

Bitcoins vindas de fontes criminosas foram recebidas por serviços de câmbio com fraca ou inexistente regulação de prevenção de branqueamento (CipherTrace Cryptocurrency Intelligence, 2018, pp. 2 e 3).

4. O sistema preventivo europeu e nacional

4.1 A quinta Diretiva e o seu conceito de moedas virtuais

A crescente utilização das criptomoedas como instrumento para o branqueamento de capitais mereceu resposta legislativa supraestadual que se baseou na inclusão das entidades cruciais do mercado de ativos virtuais no regime de prevenção da utilização do sistema financeiro para fins de branqueamento previamente existente.

Como exposto anteriormente, o crime de branqueamento ultrapassa as fronteiras estaduais e torna-se gradualmente mais internacional com o evoluir da tecnologia e do desenvolver de novos meios de atuação de execução.

Por este motivo entendeu-se que abordagens legislativas díspares levariam a uma eficácia enfraquecida no combate ao branqueamento ao permitir o acesso por parte dos agentes do crime a instituições financeiras e não financeiras que não estivessem abrangidos pelas mesmas exigências preventivas impostas no seu país.

Terá sido esta a lógica que levou o legislador europeu, em 1991[11], a harmonizar a legislação dos Estados-Membros através da transposição de medidas ditadas nas Diretivas, implementando um sistema preventivo homogéneo.

Neste sentido, leia-se o considerando 4 da quarta Diretiva relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo:

> O branqueamento de capitais e o financiamento do terrorismo ocorrem com frequência num contexto internacional. As medidas adotadas exclusivamente a nível nacional, ou mesmo a nível da União, sem ter em conta a coordenação e cooperação internacionais, terão efeitos muito limitados. (…)

Com o aparecimento das criptomoedas e a intensificação da sua utilização para fins ilícitos, inclusive para o branqueamento, emergiu a necessidade de integrar as entidades cruciais na troca e armazenamento das criptomoedas no quadro legislativo.

Para tal, e aproveitando o progressivo aditamento de novas entidades obrigadas no modelo preventivo, o legislador europeu optou por reutilizar esse mesmo instrumento jurídico para o ecossistema das moedas virtuais.

[11] A Diretiva 91/308/CEE do Conselho da União Europeia que promoveu pela primeira vez as medidas de prevenção de branqueamento focalizadas nas instituições financeiras.

A quinta Diretiva vem então introduzir no sistema de prevenção de branqueamento algumas das entidades relacionadas com o mundo das criptomoedas, surgindo como entidades obrigadas os prestadores de serviços de câmbio entre moedas virtuais e moedas fiduciárias e os serviços de custódia de carteiras.

Ambas as entidades remetem para o conceito de "moedas virtuais" que, por sua vez, vem descrito na al. d) do n.º 2 do artigo 2.º da Diretiva. Consequentemente, a definição de moedas virtuais apresentada pelo legislador tem especial relevância, dado que determinará a inclusão ou exclusão das entidades consoante o enquadramento das moedas virtuais com que estas se relacionam na definição apresentada pela Diretiva.

As moedas virtuais surgem neste contexto definidas como:

> uma representação digital de valor que não seja emitida ou garantida por um banco central ou uma autoridade pública, que não esteja necessariamente ligada a uma moeda legalmente estabelecida e não possua o estatuto jurídico de moeda ou dinheiro, mas que é aceite por pessoas singulares ou coletivas como meio de troca e que pode possa ser transferida, armazenada e comercializada por via eletrónica.

Retira-se daqui dois pontos essenciais para a inclusão de uma representação digital de valor no conceito de moeda virtual apontada pela Diretiva. Em primeiro, são expostos dois requisitos negativos que excluem uma representação digital de valor deste âmbito: a emissão ou garantia desta por um banco central ou autoridade pública; e o estatuto jurídico de moeda ou dinheiro. Caso alguma representação digital de valor seja emitida por parte do Estado ou seja legalmente admitida como moeda fiduciária, não será, para efeitos desta Diretiva, considerada moeda virtual.

Note-se que não se exclui desta definição toda e qualquer moeda virtual que esteja relacionada com moedas fiduciárias. É esclarecido pelo próprio texto que o facto de as moedas estarem ligadas às moedas fiduciárias não revela para efeitos de exclusão destas. Assim, as denominadas *stablecoins*, cujo valor se associa ao de uma moeda fiduciária ou ao de mercadorias (tal como o ouro) (Herting, 2020), podem ser consideradas como moedas virtuais (Haffke et al., 2020, p. 134).

Em segundo, são impostos dois requisitos positivos para que uma representação de valor seja abarcada pela definição: estas moedas têm de poder ser transferidas, armazenadas e comercializadas eletronicamente; e têm de ser aceites por pessoas singulares ou coletivas como meio de troca.

O primeiro requisito não parece apresentar problemas quanto à sua extensão ou interpretação já que a grande maioria das moedas virtuais podem ser transferidas,

armazenadas e comercializadas, sendo irrelevante se de facto são efetuadas estas ações pelo utilizador. Caso uma moeda não possa ser armazenada pelo utilizador, a sua relevância no crime de branqueamento será inexistente.

O mesmo já não se pode dizer quanto ao segundo requisito, que exige que a representação de valor seja aceite como "meio de troca". A Diretiva não aprofunda mais sobre o significado de "meio de troca", o que levou a que alguns autores apresentassem críticas quanto a esta incerteza normativa que pode levar a interpretações desfavoráveis quanto à inclusão de alguns tipos de criptomoedas e, por conseguinte, prejudicar a eficácia da própria Diretiva no combate ao branqueamento.

A expressão "meio de troca" é referida apenas uma outra vez pelo legislador, no considerando 10 da Diretiva. Neste, é clarificada a variedade de funções que as criptomoedas podem ter e, perante estas, a intenção do legislador em incluir a generalidade das criptomoedas no âmbito da Diretiva, independentemente das suas eventuais utilidades. Lê-se então:

> Embora as moedas virtuais possam ser frequentemente utilizadas como meio de pagamento, também podem ser utilizadas para outros fins e ter aplicações mais vastas, como, por exemplo, meio de troca, investimento, produtos de reserva de valor ou utilização nos casinos em linha. A presente diretiva tem por objetivo abranger todas as utilizações potenciais das moedas virtuais.

O legislador deliberadamente discriminou a utilidade de meio de troca das outras aqui referidas, o que causa dificuldades de interpretação do artigo 3.º da Diretiva quando este se refere apenas às moedas virtuais que evidenciem a utilidade de meio de troca e não quando estiver presente uma das outras funções.

LARS HAFFKE, MATHIAS FROMBERGER e PATRICK ZIMMERMANN, apoiados por outros autores, apontam duas possíveis interpretações do conceito de "meio de troca". Considerando "meio de troca" num sentido mais abrangente, ficariam integradas todas as outras finalidades das criptomoedas, uma vez que efetivamente são utilizadas como meios de troca no sentido comum da palavra quando trocadas por moedas fiduciárias ou virtuais, produtos ou serviços.

Contudo, esta interpretação conflitua com o texto da Diretiva, uma vez que estaria em desacordo com o próprio texto da lei que faz a distinção clara do "meio de troca" e das restantes funções individualizadas no considerando 10 (Haffke et al., 2020, p. 135). Se a expressão "meio de troca" englobasse os fins de investimento, produtos de reserva

de valor e de utilização nos casinos em linha, não estariam estes últimos expressamente individualizados.

Dito isto, os autores defendem uma leitura mais restrita do conceito, interpretando-o à luz do seu sentido económico segundo o qual um "meio de troca" não será utilizado para o seu próprio consumo mas antes como um mero intermediário que auxilia a aquisição de produtos e serviços (Cancelli, 2020, p. 15; Covolo, 2019, p. 13; Haffke et al., 2020, p. 135).

Ora, alguns ativos virtuais têm utilidade própria para além da sua troca por produtos ou serviços, tais como fins de investimento, denominados *investment tokens* ou *security tokens*[12], bem como os *utility tokens*[13].

Estes não poderão ser enquadrados na perspetiva restrita do conceito de "meio de troca" devido ao valor próprio de consumo de quem os adquire. Então, caso adotemos a doutrina restritiva, o legislador, apesar de afirmar a sua intenção de abranger todas as utilizações potenciais das moedas virtuais, não o fará, deixando de fora do conceito de moedas virtuais a transação deste tipo de ativos.

Outros autores como ROBBY HOUBEN e ALEXANDER SNYERS não adotam a doutrina restritiva do conceito de "meio de troca" e fazem uma análise positiva da definição do artigo 3.º da Diretiva.

Segundo estes, caso um ativo não possua a finalidade de "meio de troca" (no seu sentido mais amplo), a utilidade deste tipo de ativos no crime de branqueamento será inexistente, isto porque o crime de branqueamento através de criptomoedas implicaria sempre a transação das moedas por qualquer bem, produto ou serviço (Houben & Snyers, 2018, p. 74).

4.2. As novas entidades obrigadas da Diretiva

Uma segunda questão de importante análise é a extensão da lista de entidades obrigadas da Diretiva. Para incluir as criptomoedas neste regime preventivo, o legislador apontou para as plataformas mais basilares no que toca à transação e armazenamento das criptomoedas.

[12] Os *investment tokens* ou *security tokens* são ativos virtuais que permitem aos detentores de o direito de participar dos retornos futuros através de pagamentos fixos ou a dividendos, podendo também exercer direitos de voto ou de participação (De Filippi & Wright, 2018, p. 101; Haffke et al., 2020, p. 127).

[13] Os *utility tokens* são emitidos para financiar o desenvolvimento de novas criptomoedas e podem ser usados posteriormente pelos detentores para adquirir bens ou serviços do emissor da moeda (Capraro, 2021, p. 27).

A entidade com mais relevância apontada pelo legislador são os mercados de câmbio entre moedas virtuais e moedas fiduciárias, presente no artigo 1.º, n.º 1, c). Segundo DAVID SILVA RAMALHO e NUNO IGREJA MATOS, estes são os principais pontos de acesso ao mercado de criptomoedas e, por isso, apresentam maior exposição dos agentes do crime de branqueamento (Ramalho & Matos, 2020, p. 100).

Quanto aos mercados de câmbio, a sua inclusão restringiu-se aos que permitem a troca de moedas fiduciárias e moedas virtuais, ficando de fora os mercados de câmbio exclusivamente de moedas virtuais, as *crypto-to-crypto exchanges*.

A doutrina é uniforme quanto à prejudicialidade da ausência destes últimos na lista das entidades obrigadas do regime de prevenção de branqueamento. Excluídos tais mercados do escopo regulatório, não se encontram delimitados pelas imposições da Diretiva.

Consequentemente, as transações de criptomoedas entre si não terão constrangimentos uma vez ultrapassado o "ponto de acesso" das moedas fiduciárias para as moedas virtuais, o que deixa um amplo espaço de atuação sem escrutínio num dos principais meios de branqueamento, as transações entre criptomoedas (Cancelli, 2020, p. 15; Capraro, 2021, p. 28; Covolo, 2019, pp. 14 e 15; Haffke et al., 2020, pp. 134 e 135; Houben & Snyers, 2018, p. 77; Ramalho & Matos, 2020, pp. 100 e 101; Soana, 2021, p. 6 a 8).

Para além dos mercados de câmbio, o artigo 1.º, n.º 1, c) da Diretiva inclui nas entidades obrigadas os prestadores de serviços de custódia de carteiras, cuja definição vem expressa no artigo 1.º, n.º 2, d).

A inclusão destas entidades no âmbito da Diretiva pode mitigar a ausência dos mercados de câmbio exclusivamente de moedas virtuais. De facto, a maioria destes mercados, para além da sua função primordial de facilitar a troca direta de criptomoedas entre os utilizadores, também guardam e administram as suas chaves criptográficas para facilitar a transação das moedas virtuais sem que os mesmos as tenham de introduzir a cada transação (Haffke et al., 2020, p. 135).

Não obstante, a definição não abrange todos os tipos de prestadores de carteiras digitais a que os utilizadores podem ter acesso, regulando apenas os serviços de custódia de carteiras e deixando de fora qualquer prestador de serviço de carteiras digitais sem custódia (os *noncustodial wallet providers*), ou seja, aqueles prestadores de serviços de carteiras *hardware* e *software* que providenciem os meios ao utilizador de guardar as suas

chaves criptográficas por si ao invés de as salvaguardar em seu nome (Houben & Snyers, 2018, p. 78).

Nesta senda, a ausência deste tipo de prestadores de serviços de carteiras sem custódia leva a que os utilizadores destes serviços não sejam objeto das exigências de identificação e controlo impostos pela Diretiva, abrindo portas para o acesso ao mercado de moedas virtuais de modo completamente anónimo.

Ademais, caso um mercado de câmbio entre moedas virtuais queira escapar às imposições da Diretiva, bastar-lhe-á exigir ao utilizador a introdução destas chaves a cada transação ao invés de as administrar em seu nome.

Por estes motivos, alguns autores entendem que a não aplicação das medidas preventivas aos outros prestadores de carteiras representa uma outra falha no sistema preventivo (Cancelli, 2020, p. 16; Haffke et al., 2020, pp. 135 e 136; Soana, 2021, pp. 6 e 7).

O catálogo de novas entidades abrangidas no sistema europeu de prevenção de branqueamento limitou-se aos mercados de câmbio entre moedas virtuais e moedas fiduciárias e os prestadores de serviços de custódia de carteiras.

Paralelamente, não foram incluídos neste contexto as restantes entidades relevantes no sistema das criptomoedas, como é o caso dos utilizadores, os *miners* ou a própria atividade de mineração, os prestadores de serviços de mistura, os criadores da criptomoeda e as entidades encarregues da distribuição inicial da criptomoeda.

4.3. O sistema de prevenção nacional: a Lei n.º 83/2017 e alteração da Lei n.º 58/2020

A Lei n.º 83/2017, de 18 de agosto transpôs a quarta Diretiva relativa à prevenção de branqueamento. Para tal, instituiu um regime de prevenção idêntico ao redigido pelo legislador europeu em 2015, isto é, baseado na imposição de deveres de diligência quanto à clientela, controlo das transações, entre outros (Machado, 2017, p. 73).

O legislador nacional dividiu os deveres em gerais, os quais todas as entidades obrigadas devem seguir; e os específicos, desenhados para apenas certas entidades. Veja-se, para tal, os artigos 11.º e seguintes da Lei. Quanto às entidades obrigadas, estas estão listadas nos artigos 3.º a 7.º da Lei. O incumprimento destes deveres levará à aplicação do regime sancionatório da Lei, composto por ilícitos criminais e contraordenacionais presentes nos artigos 157.º e seguintes.

No contexto da prevenção da utilização de criptomoedas para o branqueamento, cabe analisar as alterações ditadas pela Lei quanto ao conceito de moedas virtuais e às novas entidades obrigadas.

O artigo 5.º da Lei aditou a alínea ll) no qual se define ativo virtual como

> uma representação digital de valor que não esteja necessariamente ligada a uma moeda legalmente estabelecida e que não possua o estatuto jurídico de moeda fiduciária, mas que é aceite por pessoas singulares ou coletivas como meio de troca ou de investimento e que pode ser transferida, armazenada e comercializada por via eletrónica.

A definição adotada pelo legislador nacional diverge daquela presente no artigo 1.º, n.º 2, al. d) da quinta Diretiva quanto às moedas virtuais. Quanto ao desvio semântico entre "moeda virtual" e "ativo virtual", o mesmo não parece ter relevância, devendo a questão centrar-se na análise do seu conceito, sejam eles denominados moedas virtuais, ativos virtuais ou até criptomoedas.

Por um lado, o legislador nacional não excluiu do conceito de ativos virtuais os emitidos ou garantidos por um banco central ou autoridade pública. Significa isto que, contrariamente à Diretiva, ficam incluídas nesta definição as criptomoedas estatais, isto é, emitidas pelo Estado, como é o caso da criptomoeda Petro emitida pelo governo venezuelano e as futuras criptomoedas chinesas e sul-coreanas, caso venham a ser emitidas (Zapotochny, 2021).

Por outro, o legislador nacional adicionou ao requisito da aceitação como "meio de troca" a utilidade de "meio de investimento". Quanto a isto, tal inclusão permite englobar na definição alguns dos ativos virtuais que foram excluídos da definição da Diretiva como é o caso dos *investment tokens*. Ainda assim, a discriminação de certas utilidades como requisito causa um entrave desnecessário à inclusão de todos os tipos de criptomoedas independentemente das suas funções, objetivo expressamente assumido na Diretiva.

A dicotomia entre o sistema preventivo nacional e europeu acentua-se expressivamente nas entidades obrigadas cujo leque vem agora substancialmente mais alargado. Para tal, a Lei não escreve uma lista de entidades que devem ser obrigadas aos deveres, ao invés foca-se em identificar as atividades que quando praticadas por uma entidade levam a que esta caia no escopo do regime preventivo.

Foram então incluídos os serviços de troca entre ativos virtuais e moedas fiduciárias, assim como os de troca entre moedas virtuais entre si, ambos previstos na alínea mm), i) e ii) aditada pela Lei.

Podemos, desde já, concluir que o legislador nacional não se bastou com a inclusão dos pontos de acesso entre o mercado de criptomoedas e o mercado tradicional,

regulando também as entidades que atuam exclusivamente dentro das transferências de ativos virtuais entre si, neste caso, as *crypto-to-crypto exchanges*.

No que diz respeito às carteiras virtuais, a Lei também recorreu a um método mais extenso do que a da Diretiva, indo para além dos prestadores de serviços de custódia de carteiras. Lê-se na alínea mm), iv): "serviços de guarda ou guarda e administração de ativos virtuais ou de instrumentos que permitam controlar, deter, armazenar ou transferir esses ativos, incluindo chaves criptográficas privadas."

A expressão "serviços de guarda ou guarda e administração de ativos virtuais (…), incluindo chaves criptográficas privadas" é idónea a englobar os prestadores de serviços de custódia de carteiras, uma vez que a guarda das chaves criptográficas é de facto a principal função deste tipo de prestadores de serviços.

Apesar de não especificar se esta guarda é feita em nome de terceiros (os utilizadores), deve entender-se através da letra da lei que a guarda destes ativos é feita pelo prestador de serviços e não pelo próprio utilizador.

Quanto aos "instrumentos que permitam controlar, deter, armazenar ou transferir esses ativos", o preceito remete para a detenção própria do utilizador através dos meios providenciados por este tipo de prestadores de carteiras, logo, engloba os prestadores de carteiras sem custódia.

Não havendo qualquer referência à vertente virtual ou física deste tipo de serviços, devemos entender que nestes "instrumentos" incluem-se as carteiras *software* e as carteiras *hardware*.

Deste modo, a Lei parece incluir todos os tipos de prestadores de carteiras digitais: os prestadores de carteiras *software* e *hardware* e os serviços de custódia de carteiras.

Por fim, na alínea mm), iii) são ainda abarcados os serviços de transferência de criptomoedas entre endereços ou carteiras digitais. Esta definição abrange os prestadores de serviços de mistura que, após recolherem as criptomoedas do utilizador, procedem à transferência das criptomoedas com outras e do produto final da mistura para um endereço destinatário.

5. Análise crítica da atual abordagem e das futuras alterações

5.1 Proibição das criptomoedas: um caminho a considerar?

Os riscos que a utilização das criptomoedas comporta na integridade do sistema económico-financeiro devido à volatilidade do valor e o aproveitamento destes ativos

para fins ilícitos levanta inevitavelmente a questão sobre se deveria ou não ser adotada uma abordagem proibitiva perante esta nova realidade.

KAI JIA e FALIN ZHANG distinguem três principais respostas no espectro legislativo: a perspetiva liberal, adotado pelos Estados Unidos da América; a proibição total, seguida pela Rússia; e o "entusiasmo prudente", presente na China (Jia & Zhang, 2018, p. 89).

O modelo proibitivo das criptomoedas que hoje vemos ser aplicado em países como a Rússia, Vietnam, Equador e Bolívia pode apresentar algumas vantagens quanto à repressão dos riscos das criptomoedas.

A proibição total desta nova realidade resultaria num maior entrave aos mercados de venda de produtos ilegais online, na frustração da utilização destes instrumentos crimes como branqueamento, financiamento de terrorismo ou crimes de evasão fiscal e também na proteção do consumidor face aos riscos de flutuação do valor dos ativos virtuais e dos possíveis ataques informáticos.

Não obstante, este modelo implicaria necessariamente a obstrução à inovação tecnológica que os ativos virtuais e a sua tecnologia subjacente representam (Jia & Zhang, 2018, p. 99). Tal reação proibitiva seria incompatível tanto de um ponto de vista teórico, no que toca a princípios basilares constitucionais e do Direito Penal, como de um ponto de vista prático face à realidade evolutiva da sociedade.

Segundo TAIPA DE CARVALHO, o desenvolvimento das sociedades complexas atuais, que trouxe consigo novas formas de criminalidade, não poderá justificar a reação excessivamente repressiva por parte do Direito Penal que incida sobre a dignidade humana, ou seja, não justificará a desaplicação do Direito Penal como *ultima ratio*, violaria o princípio da indispensabilidade da restrição constitucionalmente consagrado no artigo 18.º, n.º 2 CRP (Taipa de Carvalho, 2016, p. 55; Vaz et al., 2015, p. 246).

A proibição destas novas tecnologias implicaria uma intervenção manifestamente excessiva num fenómeno evolutivo natural da sociedade a que o Direito deve acompanhar e não dificultar, tendo sempre em consideração que a resposta penal perante os seus riscos poderá ser alcançada através de outros modelos menos agressivos perante o fenómeno.

No ponto de vista prático, a proibição implicaria também o não aproveitamento da tecnologia. Os ativos virtuais podem trazer vantagens ao sistema financeiro tradicional, tais como a diminuição do custo de emissão e circulação de moeda e o aumento da conveniência e transparência da economia, fatores que foram reconhecidos pelo Banco Popular da China (Jia & Zhang, 2018, p. 100).

Paralelamente, também a tecnologia subjacente, as *blockchains*, como novos sistemas de base de dados, podem apresentar vários usos nos campos mais diversos, tais como bases de dados dos cidadãos, votos digitais, dados armazenados em hospitais, armazenamento em nuvem e entre inúmeros outros (Gates, 2017, p. 36 a 39).

Restringir o maior campo de utilização das *blockchains*, as transações das criptomoedas, resultaria num obstáculo ao desenvolvimento desta tecnologia para meios de operação mais eficientes (tal como aconteceu com o sistema PoS).

Na perspetiva da prevenção de utilização de ativos virtuais para fins ilícitos, as perspetivas liberais e intermédias apresentam-se como mais proporcionais perante a colisão entre a evolução tecnológica e o risco da prática de crimes. Ambas as perspetivas permitem a utilização das criptomoedas, impondo deveres de prevenção de utilização das criptomoedas para fins ilícitos às entidades que auxiliam as transações[14].

5.2. O modelo europeu e a sua evolução

Apesar de haver acesso aos mercados de criptomoedas, qualquer intervenção estadual no seu ecossistema contrariará necessariamente a sua própria natureza, visto que estas surgiram nos ideais politico-liberais de transação de valores monetários sem a intervenção de instituições intermediárias públicas ou privadas que controlassem quer as transferências, quer a identidade de quem as executa.

Esta perspetiva marcada pelo choque entre as necessidades preventivas e a proteção da essência dos mercados virtuais constrangeu a atuação do legislador europeu aquando da introdução da 5ª Diretiva.

Por conseguinte, o receio de uma excessiva intervenção no ecossistema das criptomoedas e dos danos que tal pudesse causar na sua natureza e no desenvolvimento tecnológico limitou o legislador europeu na imposição de deveres de prevenção de branqueamento, que se bastou nas entidades que atuam como pontes entre os mercados de criptomoedas e os mercados fiduciários.

Sem descartar a importância da consideração das consequências dos excessos normativos, a prevenção da utilização de criptomoedas para efeitos de branqueamento através da imposição de deveres nestas entidades apenas seria eficiente se a própria existência do mercado das criptomoedas dependesse do mercado fiduciário tradicional,

[14] O modelo intermediário ou de "entusiasmo prudente" vai mais longe do que a abordagem liberal e restringe a interação entre o mercado de ativos virtuais e o mercado fiduciário tradicional, através da proibição de todas as instituições financeiras de realizar negócios relacionados com criptomoedas, assim como a proibição de instituições de pagamento de fornecer serviços a empresas que conduzam negócios de criptomoedas (Jia & Zhang, 2018, p. 101 a 103).

ou seja, se as vantagens sujeitas a branqueamento através de criptomoedas tivessem necessariamente de passar, a certo ponto, pelo mercado fiduciário (Soana, 2021, p. 3).

Nesta perceção, os instrumentos que permitem a troca entre as criptomoedas e as moedas fiduciárias teriam sempre a sua participação no esquema de branqueamento, seja numa fase de colocação, onde as vantagens são trocadas por ativos virtuais, seja numa fase de integração, onde as vantagens seriam devolvidas ao mercado financeiro tradicional.

Ora, tal perceção desenquadra-se com a realidade dos ativos virtuais e demonstra-se progressivamente mais irrealista perante a perspetiva de evolução futura do seu ecossistema. Cada vez mais utilizadores interagem com o mercado das criptomoedas e a sua aplicação na compra e venda de produtos e serviços é também gradualmente mais comum, o que leva a que esta realidade se autonomize do mercado fiduciário a um ritmo acelerado.

Um indivíduo poderá adquirir moedas virtuais através de uma transferência direta ou de uma *airdrop distribution*, podendo trocá-las por outras moedas ou comprar produtos e serviços a comerciantes que as aceitem como meio de pagamento, sem ter de passar pelos mercados de câmbio descritos na Diretiva.

Isto dito, a decisão de apenas incluir na lista de entidades obrigadas as *crypto-to-fiat exchanges* e os prestadores de serviços de custódia de carteiras virtuais, deixando de fora as *crypto-to-crypto exchanges* e os demais tipos de prestadores de carteiras virtuais leva a uma abordagem ineficiente no combate ao branqueamento.

Não obstante, uma intervenção legislativa no próprio ecossistema de transferências de criptomoedas entre si será estritamente necessária também na perspetiva de proteção do desenvolvimento da tecnologia subjacente.

Através de um sistema eficaz de prevenção da criminalidade económico-financeira, garante-se que as criptomoedas como fenómeno desvinculam-se da reputação negativa que o associa à prática de crimes e que cria hesitação na sua adoção como um novo meio alternativo ao sistema financeiro tradicional.

A recetividade positiva promoverá o aumento da sua utilização que, por sua vez, impulsionará o desenvolvimento da tecnologia de modo a poder ser aplicado em cada vez mais campos do quotidiano, sejam estes económicos (através das criptomoedas) ou outras diversas aplicações (através das *blockchain* aplicadas a outros fins).

5.3. A antecipação do legislador nacional

Comparando a Lei n.º 58/2020, de 31 de agosto com a Diretiva que esta transpôs, evidencia-se a inclusão mais extensa de entidades adotada no ordenamento nacional. Do ponto de vista de prevenção de branqueamento, esta é uma abordagem mais eficaz e, pelos motivos enunciados, preferível.

As falhas da Diretiva quanto às novas entidades obrigadas foram desde cedo reconhecidas pelo GAFI, que alterou em outubro de 2018 a sua Recomendação n.º 15 (relativa à prática do crime de branqueamento com as novas tecnologias) e a respetiva nota interpretativa, adicionando novos conceitos de "ativos virtuais" e "prestadores de serviços de criptoativos" (VASP), aos quais devem ser aplicados os deveres (FATF/GAFI, 2012, pp. 76 e 77).

Através destas alterações, o GAFI aprofundou o âmbito subjetivo da aplicação das medidas de prevenção de branqueamento, recomendando um alargamento das entidades às quais devem ser aplicadas tais medidas. A grande novidade centra-se nos prestadores de serviços de criptoativos: este novo conceito identifica as entidades obrigadas pela sua atividade prestada e não pela *ratione personae*. Este novo método demonstra-se mais apto a compreender novos modelos de negócio que possam surgir neste setor (Covolo, 2019, p. 17).

Integram-se neste novo conceito, para além das *crypto-to-fiat exchanges* e os serviços de custódia de carteiras, as *crypto-to-crypto exchanges*, os serviços de transferência de ativos virtuais, os serviços de carteiras virtuais e os serviços financeiros relacionados com as ICO (FATF/GAFI, 2019, pp. 13 e 14).

Estas alterações marcam o abandono da estratégia conservadora focalizada nos pontos de acesso ao mercado dos ativos virtuais e assume a necessidade de controlo dentro do ecossistema dos ativos virtuais, que permite a aplicação das medidas de prevenção a um leque de entidades substancialmente mais carregado (Soana, 2021, pp. 10 e 11).

Confrontado com estas novidades apresentadas pelo GAFI, organização que tem guiado o paradigma regulatório nesta matéria, inclusive o quadro legislativo europeu, o legislador nacional, que ainda não tinha transposto a 5ª Diretiva[15], viu-se na oportunidade de se antecipar ao legislador europeu.

[15] O prazo de transposição da 5ª Diretiva seria em janeiro de 2020.

Deste modo, e aproveitando o preceito normativo do artigo 5.º da 4.ª Diretiva (regime base alterado pela 5ª Diretiva) que permite aos Estados-Membros aplicar medidas mais restritivas, o legislador nacional transpôs a 5ª Diretiva, mas fê-lo seguindo a nova abordagem recomendada pelo GAFI e que certamente iria ser seguida posteriormente pelo legislador europeu.

É então percetível a coincidência entre a definição de "atividades com ativos virtuais" apresentada pelo legislador nacional no artigo 5.º da Lei n.º 58/2020 e o conceito de VASP desenvolvido pelo GAFI nestas alterações. A letra da Lei neste ponto resume-se a uma tradução literal da nova definição de VASP, diferenciado do que foi exposto na 5ª Diretiva.

Para além disso, esta antecipação à Diretiva não se bastou pela matéria de entidades obrigadas, também se verificou o mesmo fenómeno quanto à definição de criptoativos. Na mesma linha de pensamento, o legislador nacional passou a incluir, para além das criptomoedas aceites como meio de pagamento, as utilizadas como investimento. Ao contrário do regime da Diretiva, passam então a ser considerados os *investment tokens* ou *security tokens*.

Todavia, se é verdade que o legislador nacional aproveitou esta oportunidade para se antecipar ao regime europeu nestas vertentes, também é verdade que não o fez quanto à inclusão das atividades de lançamento das criptomoedas (as ICO) como recomendado pelo GAFI.

Tal exclusão nas atividades das VASP constitui uma falha no sistema preventivo, uma vez que a aquisição de um ativo virtual no seu lançamento é uma forma de adquirir criptomoedas sem ter de recorrer aos mercados de câmbio e, consequentemente, não estando sujeito a qualquer dever de diligência de clientela ou controlo de suspeitas de branqueamento aquando da aquisição (Forgang, 2019, p. 17 a 19; Houben & Snyers, 2018, p. 78).

5.4. A futura alteração do modelo europeu

Em julho de 2021, a Comissão Europeia apresentou um pacote de propostas de alterações legislativas relativamente ao atual sistema de prevenção de branqueamento. Neste, estão incluídas propostas de revogação da 4ª Diretiva e a sua substituição pela 6ª Diretiva e por um novo Regulamento, assim como a criação da Autoridade para o Combate ao Branqueamento de Capitais e ao Financiamento do Terrorismo, encarregue da supervisão da aplicação das obrigações impostas e de agilizar a cooperação entre UIFs nacionais (Financial Stability, Financial Services and Capital Markets Union, 2021).

Com estas alterações, o legislador europeu vem simplificar o conceito de criptoativos para que neste sejam abrangidos todo o tipo de moedas independentemente da sua utilidade, desde que possam ser transferidos ou armazenados.

Quanto às entidades obrigadas, o mesmo fenómeno verificou-se: o legislador consagrou o novo modelo das Recomendações nesta matéria, focando-se nas atividades prestadas para considerar ou não uma entidade como obrigada.

Passarão a ser entidades obrigadas todas as que sejam consideradas prestadoras de serviços de criptoativos, ou seja, os que prestem as atividades descritas no artigo 3.º, n.º 1, ponto (9) da Proposta de Regulamento COM/2020/593, sendo: custódia e administração de criptoativos por conta de terceiros, operação de uma plataforma de negociação de criptoativos (P2P), troca de criptoativos por moeda fiduciária com curso legal e por outros criptoativos, colocação de criptoativos (as ICO) e execução, receção e transmissão de ordens relativas a criptoativos em nome de terceiros.

Note-se que as alterações propostas levam a que o sistema de prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais deixe de ser regulado num único instrumento legislativo europeu, a Diretiva, e passe a ser enquadrado em dois elementos legislativos distintos: a 6ª Diretiva, vocacionada nas medidas a ser aplicadas pelos Estados-Membros (identificadas sucintamente no artigo 1.º da proposta de Diretiva); e a proposta de Regulamento, direcionada para as entidades obrigadas e os respetivos deveres de prevenção de branqueamento.

Caso a matéria de deveres das entidades obrigadas passe a ser ditada por Regulamento, não será necessária qualquer transposição para a lei nacional, inclusive a dada pela Lei n.º 83/2017 (alterada pela Lei n.º 58/2020), devido ao carácter geral e abstrato dos Regulamentos.

5.5. Mineração: o último passo

Em retrospetiva, a rápida evolução do sistema preventivo de branqueamento aplicado às criptomoedas tem-se como necessária para a própria eficácia e funcionamento do sistema. O modelo regulatório da 5ª Diretiva não se mostrou suficiente para acautelar os perigos do fenómeno das criptomoedas como designadamente a *pseudonimização* e a sua natureza intrinsecamente internacional.

A política mais intervencionista quanto ao âmbito subjetivo, ao incluir mais participantes do ecossistema das criptomoedas no leque das entidades obrigadas, deixa pouco espaço para que a interação com estas possa ser feita sem passar por métodos de verificação de identidade e monitorização de transações.

Tal modelo tem vindo a ser adotado através das alterações às Recomendações do GAFI em 2018, pela Lei n.º 58/2020 que alterou o modelo de prevenção de branqueamento nacional e transpôs a 5ª Diretiva e, por fim, pelas propostas de alterações do sistema preventivo a nível europeu.

Porém, o tema que não foi abordado em nenhuma destas novidades legislativas foi a atividade de mineração. Na perspetiva de autores como LARS HAFFKE, MATHIAS FROMBERGER e PATRICK ZIMMERMANN, a inclusão dos *miners* ou dos prestadores de ferramentas ou serviços de mineração seria desnecessária, uma vez que o branqueamento através da atividade de mineração não constitui um meio de atuação do crime de branqueamento suficientemente distinto dos restantes para a sua individualização no sistema preventivo (Haffke et al., 2020, p. 138).

Apesar de a mineração poder ser um dos muitos *modi operandi* do crime de branqueamento através da utilização de criptomoedas, a verdade é que também é um meio de aquisição de criptoativos, tal como uma ICO. A discussão não deve estar restrita na individualização dos modos de branqueamento, deve focar-se também nos modos de aquisição de ativos virtuais que podem levar posteriormente à prática do branqueamento.

Um potencial utilizador de criptomoedas pode adquiri-las através da atividade de mineração. Assim como numa ICO, as criptomoedas vão ser adquiridas sem passar por uma entidade que esteja obrigada a cumprir os requisitos de prevenção da Diretiva.

Este facto constitui um perigo de prática de branqueamento: um agente que queira dissimular a origem ilícita das suas vantagens pode adquirir com estes instrumentos (*hardware*) para exercer a atividade de mineração e obter a compensação em criptomoedas sem ter de ser sujeito a deveres de diligência de clientela.

No final, terá criptomoedas adquiridas aparentemente de modo legítimo, através da mineração, que poderá trocar por moeda fiduciária, por outras moedas virtuais ou por produtos e serviços. Esta prática também poderá ser exercida a nível coletivo, através dos *pools* de mineração, onde vários indivíduos trabalham cooperativamente para a mineração de moedas.

Posto isto, e acompanhando o entendimento de autores como ROBBY HOUBEN, ALEXANDER SYNERS, DAVID SILVA RAMALHO e NUNO IGREJA MATOS, entendo que a atividade de mineração deve constar no sistema preventivo de branqueamento (Houben & Snyers, 2018, pp. 76 e 77; Ramalho & Matos, 2020, pp. 102 e 103). Para tal, deve ser considerada a inclusão das entidades que se dedicam à

comercialização de *hardware* destinado à atividade de mineração nas atividades que definem as entidades obrigadas, as novas VASP.

6. Conclusão

A inclusão das criptomoedas no sistema de prevenção de branqueamento deu-se com o enquadramento de novas entidades essenciais à sua aquisição nesse sistema ditado pelas Diretivas e transposto pelos ordenamentos jurídicos nacionais dos Estados-Membros. Tais entidades terão agora de cumprir os deveres de prevenção de branqueamento que passam por identificação de clientela, controlo de transações e cooperação com as UIFs.

Esta novidade que surgiu com a 5ª Diretiva reconheceu o perigo da utilização das criptomoedas no crime de branqueamento e a necessidade de acautelar este novo meio de execução do crime.

Não obstante a importância de tal reconhecimento na prevenção do branqueamento moderno, as novidades introduzidas pela 5ª Diretiva não se revelaram suficientes para prevenir a utilização das criptomoedas para estes fins.

A integração dos pontos de acesso entre o mercado fiduciário e o ecossistema das criptomoedas não é, por si, apto a englobar todos os meios de acesso a estes ativos virtuais devido à gradual autonomização das criptomoedas do sistema financeiro tradicional.

Por conseguinte, a Diretiva não englobou todos os tipos de criptomoedas nem conseguiu implementar a aplicação dos deveres de controlo e diligência à totalidade de utilizadores que as adquirem, o que leva à falha do sistema preventivo.

Contrariamente, o mesmo sistema preventivo transposto pelo legislador nacional foi mais eficaz na matéria, incluindo outras entidades para além dos pontos de acesso entre estes dois mercados. Assim, ao seguir as recomendações mais recentes do GAFI, o legislador nacional estendeu tais deveres a outras entidades para além dos mercados de câmbio.

As propostas de alteração do sistema preventivo europeu salientam a urgência de modificação da abordagem tomada na 5ª Diretiva para uma mais incisiva no ecossistema das criptomoedas, nos moldes recomendados pelo GAFI e já adotados pelo legislador nacional.

Dado o volume que o crime de branqueamento tem vindo a revelar nas últimas décadas, em especial através destes novos instrumentos, entendo que as alterações

propostas não só são necessárias como também urgentes para a boa realização da prevenção do crime neste setor económico-financeiro.

Ainda assim, a ausência da atividade de mineração nesta matéria pode revelar-se uma falha visto que é tanto um meio de aquisição de criptomoedas como um meio idóneo a branquear valores monetários que fica fora do escopo do sistema.

Bibliografia

Albuquerque, P. P. de. (2021). *Comentário do Código Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem* (4ª Edição). Universidade Católica Editora.

A.V., V. (2018). ICO as Economic Security Threat. Possible Risks Analysis. Experience of Foreign States. *KnE Social Sciences*, *3*(2), 208. https://doi.org/10.18502/kss.v3i2.1544

Banco de Portugal. (2020). *Occasional Paper On Crypto-Assets*. https://www.bportugal.pt/sites/default/files/anexos/papers/op202004.pdf

Braguês, J. L. (2009). *O Processo de Branqueamento de Capitais*. Edições Húmus & OBEGEF. https://obegef.pt/wordpress/wp-content/uploads/2009/02/wp0021.pdf

Cancelli, L. (2020). *The Growing Crypto-assets Threat to Anti-money Laundering: How Institutions Are Coping with This Phenomenon*. 21.

Capraro, T. (2021). *The 5th Anti-Money Laundering Directive In The Light Of Virtual Currencies: The Exploitation Of The Decentralized System And Rising Legislative Challenges*. 39.

Chaum, D. (1983). Blind Signatures for Untraceable Payments. Em *Advances in Cryptology*. Springer.

Chaum, D. (1985). Security without identification: Transaction systems to make big brother obsolete. *Communications of the ACM*, *28*(10), 1030–1044. https://doi.org/10.1145/4372.4373

Choo, K.-K. R. (2013). New payment methods: A review of 2010–2012 FATF mutual evaluation reports. *Computers & Security*, *36*, 12–26. https://doi.org/10.1016/j.cose.2013.01.009

Choo, K.-K. R. (2015). Cryptocurrency and Virtual Currency. Em *Handbook of Digital Currency* (pp. 283–307). Elsevier. https://doi.org/10.1016/B978-0-12-802117-0.00015-1

CipherTrace Cryptocurrency Intelligence. (2018). *Cryptocurrency Anti-Money Laundering Report*. 22.

Commission Staff Working Document. (2017). *Accompanying the document Report from the Commission to the European Parliament and to the Council on the assessment of the risks of money laundeirng and terrorist financing affecting the internal market and relating to cross-border situations*. https://eur-lex.europa.eu/resource.html?uri=cellar:d4d7d30e-5a5a-11e7-954d-01aa75ed71a1.0001.02/DOC_1&format=PDF

Covolo, D. V. (2019). *The EU Response to Criminal Misuse of Cryptocurrencies: The young, already outdated 5th Anti-Money Laundering Directive*. 277.

de Barros, G. O. (2019). Cryptocurrencies: Advantages and Risks of Digital Money. *Gabinete de Estratégia e Estudos Do Ministério Da Economia*, *67*, 42.

De Filippi, P., & Wright, A. (2018). *Blockchain and the law: The rule of code*. Harvard University Press.

Duarte, J. M. D. (2002). *Branqueamento de Capitais: O Regime do D. L. 15/93, de 22 de Janeiro, e a Normativa Internacional*. Coimbra Editora.

European Central Bank. (2015). *Virtual currency schemes: A further analysis.* Publications Office. https://data.europa.eu/doi/10.2866/662172

FATF/GAFI. (2012). *The FATF Recommendations*. https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

FATF/GAFI. (2014). *Virtual currencies – Key Definitions and Potential AML/CFT Risks*. 17.

FATF/GAFI. (2018). *Professional Money Laundering*. https://www.fatf-gafi.org/media/fatf/documents/Professional-Money-Laundering.pdf

FATF/GAFI. (2019). *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*. https://www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html

FATF/GAFI. (2022, Janeiro 4). *Money Laundering*. https://www.fatf-gafi.org/faq/moneylaundering/#d.en.11223

Financial Stability, Financial Services and Capital Markets Union. (2021, Julho 20). *Anti-money laundering and countering the financing of terrorism legislative package*. https://ec.europa.eu/info/publications/210720-anti-money-laundering-countering-financing-terrorism_en

Forgang, G. (2019). *Money Laundering Through Cryptocurrencies*. 31.

Gates, M. (2017). *Blockchain: Ultimate guide to understanding blockchain, bitcoin, cryptocurrencies, smart contracts and the future of money.* CreateSpace Independent Publishing Platform.

Girasa, R. (2018). *Regulation of Cryptocurrencies and Blockchain Technologies*. Springer International Publishing. https://doi.org/10.1007/978-3-319-78509-7

Haffke, L., Fromberger, M., & Zimmermann, P. (2020). Cryptocurrencies and anti-money laundering: The shortcomings of the fifth AML Directive (EU) and how to address them. *Journal of Banking Regulation*. https://doi.org/10.1057/s41261-019-00101-4

Herting, A. (2020, Dezembro 29). *What Is a Stablecoin?* https://www.coindesk.com/learn/what-is-a-stablecoin/

Hiramoto, N., & Tsuchiya, Y. (2020). Measuring dark web marketplaces via Bitcoin transactions: From birth to independence. *Forensic Science International: Digital Investigation*, *35*, 301086. https://doi.org/10.1016/j.fsidi.2020.301086

Houben, D. R., & Snyers, A. (2018). *Cryptocurrencies and blockchain*.

Hudges, E. (1993). *A Cypherpunk's Manifesto*. https://www.activism.net/cypherpunk/manifesto.html

IMF Staff Discussion Note. (2016). *Virtual Currencies and Beyond: Initial Considerations*. https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf

Jia, K., & Zhang, F. (2018). Between liberalization and prohibition: Prudent enthusiasm and the governance of Bitcoin/blockchain technology. Em *Bitcoin and beyond: Cryptocurrencies, blockchains and global governance* (p. 207). Routledge, Taylor & Francis Group.

Kelly, J. (2017, Maio 18). *Bitcoin's murkier rivals line up to displace it as cybercriminals' favourite*. https://www.reuters.com/article/cyber-attackbitcoin/bitcoins-murkier-rivals-line-up-to-displace-it-as-cybercriminals-favouriteidUSL8N1II1MV

KYC-Chain. (2019, Abril 25). *The History Of Money Laundering*. https://kyc-chain.com/the-history-of-money-laundering/

Lee, S., Yoon, C., Kang, H., Kim, Y., Kim, Y., Han, D., Son, S., & Shin, S. (2019). Cybercriminal Minds: An investigative study of cryptocurrency abuses in the Dark Web. *Proceedings 2019 Network and Distributed System Security Symposium*. Network and Distributed System Security Symposium, San Diego, CA. https://doi.org/10.14722/ndss.2019.23055

Machado, M. da C. (2017). Problemas, paradoxos e principais deveres na prevenção do branqueamento de capitais. *Revista de Concorrência e Regulação*, *Ano 8, N.º 31*, 39–91.

Marsali, M. (2018, Abril 26). Crypto money-laundering: Will crypto help the money-launderers of the future? *The Economist.* https://www.economist.com/finance-and-economics/2018/04/26/crypto-money-laundering

Martucci, B. (2021, Maio 18). *What Is Cryptocurrency – How It Works, History & Bitcoin Alternatives*. https://www.moneycrashers.com/cryptocurrency-history-bitcoin-alternatives/

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. 9.

Ramalho, D. S., & Matos, N. I. (2020). Branqueamento e Bitcoin: Uma introdução. *Revista do Ministério Público*, 40.

Richards, K. (2021, Setembro). *Cryptography*. https://www.techtarget.com/searchsecurity/definition/cryptography

Soana, G. (2021). Regulating cryptocurrencies checkpoints: Fighting a trench war with cavalry? *Economic Notes*, *51*(1). https://doi.org/10.1111/ecno.12195

Taipa de Carvalho, A. (2016). *Direito Penal, Parte Geral—Questões Fundamentais, Teoria Geral do Crime* (3ª). Universidade Católica Editora.

Teichmann, F. M. J., & Falker, M.-C. (2020). Cryptocurrencies and financial crime: Solutions from Liechtenstein. *Journal of Money Laundering Control*, *ahead-of-print*(ahead-of-print). https://doi.org/10.1108/JMLC-05-2020-0060

Tziakouris, G. (2018). Cryptocurrencies—A Forensic Challenge or Opportunity for Law Enforcement? An INTERPOL Perspective. *IEEE Security & Privacy*, *16*(4), 92–94. https://doi.org/10.1109/MSP.2018.3111243

U. Breu, S., & G. Seitx, T. (2018). *Legislative Regulations to Prevent Terrorism and Organized Crime From Using Cryptocurrencies and Its Effect on the Economy and Society*. https://ssrn.com/abstract=3081911

Vaz, M. A., Santos Botelho, C., Carvalho, R., Folhadela, I., & Teresa Ribeiro, A. (2015). *Direito Constitucional: O Sistema Constitucional Português* (2ª). Universidade Católica Editora.

World Bank Group. (2017). *Distributed Ledger Technology (DLT) and Blockchain*. https://documents1.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf

Zapotochny, A. (2021, Fevereiro 18). *Government-issued cryptocurrencies: An overview*. https://blockgeeks.com/government-issued-cryptocurrencies-an-overview/