# (BARTOLETTI et al., 2021)

We define scam as any unlawful behaviour of one or more persons who intentionally deceive people to obtain something illegal or unfair. More specifically, in a crypto scam, fraudsters exploit one the peculiar features of blockchain technologies, i.e. the availability of crypto-assets that can be anonymously (or pseudonymously) exchanged for fiat currencies.

A) PONZI SCHEMES

Ponzi schemes are scams that advertise themselves as highyield investment programmes (HYIPs) [14], [15]. They typically lure users with the promise of high profits in return for their investments by paying high levels of interest (see e.g. Figure 1). In practice, Ponzi schemes only pay users with the funds invested by new users, and therefore implode as soon as new investors stop joining. As a result, most investors in Ponzi schemes just lose their money.

B) MALWARE

The alleged untraceability of cryptocurrencies has been extensively exploited by malware developers. There are two types of malware closely related to cryptocurrencies:

1. Ransomware: After infecting the victim’s device, this kind of malware encrypts the data on the device, and locks it until the user pays a ransom (usually in Bitcoin). Figure 2 shows a screenshot of a device infected by Wannacry, along with the instructions to pay the ransom.

Crypto loggers This kind of malware tries to steal information about the victim’s accounts on crypto services (like, e.g., wallets). In particular, crypto loggers try to obtain the private key needed to transfer crypto-assets from the victim’s account to the fraudster’s. They often work as a transparent interface while the user is surfing the web, or is searching for password files

C) FAKE CRYPTO SERVICES

In the cryptocurrency ecosystem, there are multiple services to simplify their use and management. They include exchange services, wallets and mixers. However, numerous criminals develop these types of services in the form of fraud, as described below.

1. **Fake exchange** Fake exchange frauds deceive users by offering incredibly competitive market prices for purchasing cryptocurrencies. Indeed, they trick users with quick and easy access to some cheap currency. Figure 3 shows a fake exchange service at paybillsbitcoin.com, mirrored from BtcToPal.com.
2. **Fake wallet** Wallet services allow users to manage, send and receive cryptocurrencies. In this scenario, users can run into wallet scams characterised by various types of fraudulent behaviour. For example, some wallets steal the entire amount indiscriminately, while others take a small percentage of the daily deposit. Finally, others withdraw when the deposit exceeds a certain threshold.
3. **Fake mixing** Transactions in blockchain systems (e.g. Bitcoin) are linked together, so it is possible to inspect cryptocurrency movements between addresses. However, mixing services make it possible to erase the links between initial and final addresses, randomise the number of transactions, add delays to transactions, and use other extraneous addresses. On the other hand, fake mixers receive the money and steal it without sending it to the client. Figure 1 was a website of a fake mixer called ’’BitcoinMixer’’, online up to December 30, 2020. Several users sent money to this fake mixer and never received it back, as reported on BitcoinTalk. Moreover, a BitcoinTalk topic shows a list of fake mixers
4. **Fake mining pool** Cryptocurrencies based on the Proof Of Work (POW) mechanism require a computational effort to create blocks. Therefore, users who create blocks, called miners, receive a reward. This type of scam asks users to participate by investing money to buy mining hardware. Despite what the scam promised, the money invested is not used to buy new hardware but rather to pay interest to previously registered users.
5. **Fake donation** Usually, donors make donations to projects or people for good. Fraudsters exploit people’s virtue, creating fake donation campaigns, and instead of giving the money as a donation, they steal the money and disappear

Andryukhin [43] reviewed and classified the prominent frauds that occurred in blockchains, how the fraudsters implemented them, and how to mitigate scams. While analysing social engineering attacks, the authors found ’’Clone’’, a clone website to create IOTA wallet keys, and estimated that USD 4 million worth of MIOTA tokens had been stolen.

Holub and O’Connor [7] tracked a Bitcoin phishing campaign called ’’Coinhoarder’’ for over six months. The campaign theft USD 10 million by launching typosquatting domains containing clones of crypto exchange websites. For example, they find ’’block-chain.info’’ and ’’blockchian.info/wallet’’.

D) ADVANCE-FEE SCAMS

According to the FBI [49], ‘‘An advance fee scheme occurs when the victim pays money to someone in anticipation of receiving something of greater value—such as a loan, contract, investment, or gift—and then receives little or nothing in return.’’ In an advance-fee scam, scammers typically contact the victim via e-mail or social media using a fake e-mail address or social media account. They promise the victim a significant amount of money in exchange for a small upfront payment that scammers claim will use to obtain a substantial sum as a reward. If the victim makes the payment, the scammer either disappears or adds several additional charges that the victim has to pay. Recently, several of these scams campaigns have taken place on Twitter, using well-known personalities such as Elon Musk, as shown in Figure 6 example

E. BLACKMAIL

In blackmail scams, fraudsters usually claim to have hacked the victim’s device, and installed a key logger, or recorded the victim with the webcam. The mail typically asks for a ransom in Bitcoin to delete the material, threatening that they will otherwise sell it, or publish on social networks. Figure 7 shows an actual example of blackmail that the scammer sent to a potential victim. More advanced fraudsters tailor personalised emails to victims, by exploiting databases of emails and hacked passwords

F. FAKE ICO

An Initial Coin Offering (ICO) is a way for blockchainrelated currencies to raise funds before their official launch similar in many ways to Initial Public Offerings for shares. Fake ICO scams apply the same strategy by luring users into buying fake coins. Typically, a cryptocurrency company releases a predetermined number of coins on the open market in the same way that shares are issued when a company goes public. Many ICOs are legitimate cryptocurrencies that have the potential to make an investor as much money as any other stock [53]. Fake cryptocurrencies advertise themselves with peculiar features that others do not have via brand new websites. To try to mitigate this problem, the SEC launched a parody website in 2018 that mocks ICO [54], along with a fake eight-page white paper, fake celebrity endorsements, and a fake team working on the ICO. According to a study realised by Satis Group in 2018, approximately 80% of ICOs conducted in 2017 were scams, with no actual product to offer [55]. Moreover, in 2017, ICO gained USD 1.6 billion, of which USD 150 million belongs to fake ones [43].

To cite some examples of Fake ICO scams [53], [55], Pincoin was launched in 2018 and raised USD 660 million. PlexCoin in 2017 raised USD 8.5 million, while Bitconnect in 2016, reached a market cap of over USD 2.6 billion. OneCoin is perhaps the most famous. It was launched in 2014 as a mined cryptocurrency even though it was a Ponzi scheme. The FBI discovered it raised to USD 4 billion in income. Savedroid was funded in 2015 and raised USD 50 million until 2018. At the time of writing, it is still listed on exchanges. Finally, AriseCoin was an ICO attempt by a fake bank named AriseBank. The SEC stopped it in January 2018.

G. MONEY LAUNDERING Money laundering consists of making large amounts of money obtained from illegal activities appear to come from legitimate sources. It consists of three stages: placement, layering and integration. In the first stage, dirty money is introduced into the legitimate financial system. Then, the money is moved several times to create confusion, moving through numerous accounts. Finally, it is integrated into the financial system through further transactions until the process is completed. The main problem associated with this criminal activity is to make the proceeds legal without arousing the suspicion of law enforcement.

A. RECOMMENDATION #1.

IMPROVE SCAM REPORTING SYSTEMS As we have noted in Section III, the existing public data sources on crypto scams are heterogeneous, and not completely reliable. This hampers the development of effective scam detection and classification tools, for which it would be crucial to have a uniform and reliable dataset of scam. To overcome these issues, our recommendation is to construct a scam reporting system which is comprehensive (i.e., it allows users to report scams of any type, targeted to any blockchain), with a uniform taxonomy of scams (like, e.g., the one we have proposed in Section II) and moderated, so to reduce the amount of spurious or incorrect data. Further, this system should guide users towards the correct self-classification of scams, e.g. by providing an interactive questionnaire, and by showing scam templates of the various types.

B. RECOMMENDATION #2. DEVELOP A BROWSER EXTENSION TO WARN AGAINST SCAMS A success factor of cryptocurrency scams, besides users’ greediness, is that non-technical users often find it difficult to distinguish fraudulent websites from legit ones. Accordingly, we recommend the implementation of a browser extension which inspects websites, alerts users when it detects potential scams, and advises users what to do if they have already been scammed. Similarly, the browser extension could alert users when they try to send money to blockchain addresses related to scams, or when they read blackmails. Our toolchain can be the basis for developing such a browser extension.

# (SILVEIRA, 2020)

Esse – o anonimato – é um termo importante, pois sua história se justifica pela origem anárquica virtual defendida pelas chypherpunks,6 e mais: é a principal preocupação penal sobre potenciais crimes sem identificação do titular dos valores manipulados

Foi somente depois de alguns anos de sua criação que se deu a primeira operação, que ocorreu no dia 22 de maio de 2010. Naquela oportunidade, em um grupo de debate eletrônico denominado bitcointalk, um indivíduo chamado Lazlo Hanyecz ofereceu 10.000 bitcoins para quem lhe entregasse duas pizzas em sua casa, na Flórida, Estados Unidos. Note-se que a cotação da bitcoin, à época, era de 0,003 dólares para cada bitcoin, o que implicava em que estava ele a oferecer cerca de 30 dólares pelas pizzas.8 A proposta foi aceita por um indivíduo inglês, que pagou 25 dólares e recebeu o pagamento, hoje, no valor de mais de 70 milhões de dólares. Esse dia ficou conhecido como o Bitcoin Pizza Day.

Explica-se: a principal característica da bitcoin, ou de algumas das criptomoedas, é o caráter de anonimato. Elas, no mais das vezes, portam-se como uma espécie de título ao portador virtual, e, com isso, inúmeras condutas criminosas seriam possíveis. Foi assim que elas, em seu berço, já foram vistas como meio para prática delitiva, como foi o caso do famoso caso da Silk Road.14 Tratando-se quase de um mercado eletrônico das drogas, tinha-se nas criptomoedas a modalidade de pagamento ideal. Por outro lado, as mesmas criptomoedas, em si, já foram vistas como moeda falsa, como modalidade de pirâmide financeira ou, ainda, como cenário ideal para prática de crimes vários. Pois bem, é esse o ponto aqui tratado. Versa-se sobre a possibilidade de compreensão geracional sobre as criptomoedas.

Em termos econômicos, é comum ouvir dizer, por exemplo, que as criptomoedas ou criptoativos (que tem na bitcoin seu exemplo maior, uma vez que ela domina mais de 70% do mercado mundial) nada mais são do que uma pirâmide financeira. Warren Buffet, um dos maiores especuladores na Bolsa de Valores, já mencionou essa ideia.

Com lucros significativos nos últimos anos, acabou-se por constatar uma série de indivíduos ou companhias que prometem ganhos extraordinários, fazendo-se eventualmente valer, mesmo, de personalidades para suas publicidades. A mídia, no entanto, retrata incontáveis casos, particularmente no Brasil, onde houve abuso da boa-fé das pessoas em negociação de criptomoedas. E isso se externaliza na nítida preocupação de diversos projetos de lei que visam, hoje, criminalizar as chamadas pirâmides nesse formato.

Trata-se da mais profunda questão atinente ao Direito Penal Econômico moderno, que vem a englobar não somente as variações de lavagem de dinheiro, mas, também, relativas, no Brasil, à evasão de divisas e à sonegação fiscal. Em suma, a terceira geração diz respeito ao que aqui se denomina trilema penal econômico.

4.1 Evasão de divisas

Inicialmente, ao referir-se sobre a questão da evasão de divisas, é mencionado no art. 22, parágrafo único da Lei 7.492/1986 (LGL\1986\17), ser crime quem, a qualquer título, promove, sem autorização legal, a saída de moeda ou divisa para o exterior, ou nele mantiver depósitos não declarados à repartição federal competente.

a simples aquisição de criptomoedas não autoriza esse entendimento, pois não existe deslocamento espacial do dinheiro, senão a utilização simultânea de uma dimensão paralela de trabalho, vale dizer, dimensão real, dimensão virtual. O outro ponto, no entanto, seria o caso de potenciais arbitragens de criptomoedas, as quais poderiam gerar mais dúvidas

Por arbitragens desse teor, tem-se a ideia de se poder comprar criptomoedas de uma Exchange que apresente uma cotação mais baixa e vender a outra que esteja pagando mais,26 e isso pode se dar mesmo em países diversos. Ocorre que, como não existe um controle de Bancos Centrais, isso se dá em termos mundiais, podendo haver um tráfego internacional e automático de valores, os quais, se efetivados, poderiam implicar em dúvida sobre evasão.

4.2 Sonegação fiscal

A sonegação fiscal, prevista no art. 1º, da Lei 8.137/1990 (LGL\1990\43), também é um problema potencial a ser imaginado pela terceira geração. A Receita Federal brasileira, por exemplo, exige, consoante seu regulamento geral, que os detentores de moedas virtuais as declarem nas respectivas declarações anuais das pessoas físicas. Assim, uma omissão em tais declarações poderia, em tese, implicar crime de sonegação fiscal, consoante o art. 1º da Lei 8.137/1990 (LGL\1990\43). As dificuldades, no entanto, diriam respeito ao fato de sua propriedade ainda ser anônima, e, portanto, de prova extremamente difícil para as respectivas autoridades.

**Dessa forma, como já se mencionou, seriam de se imaginar possíveis problemas, para além do Direito Penal em sentido fechado, como pensar em alguém que adquire bitcoin com desconhecimento do cônjuge, visando uma eventual proteção patrimonial em caso de futura separação.29 Nesse caso, poderia ser considerada a existência de um crime de sonegação fiscal ou apropriação indébita, que estariam, a seu modo, a gerar figura criminosa apta para a consubstanciação, também, do crime de lavagem de ativos.**

4.3 Lavagem de capitais

Em termos sintéticos, tem-se que a lavagem de dinheiro, portanto, consiste, em essência, em disfarçar a origem ilegal de ativos provenientes de crime, com a finalidade última de dar-lhes aparência legítima. Em apertada síntese, ter-se-ia que o propósito de tal processo dizer respeito à criação de uma áurea de legalidade em torno do objeto inicial do crime.31 Em verdade, a questão fundamental a ser levada em conta diz respeito a como se pode constatar semelhante conversão. Por inegável influência estrangeira, nota-se, de fato, uma confusão entre o que objetivamente se constata como manobras de disfarce, como, também, o contexto subjetivo a ser levado em conta.32 Assim, é de se ter que, no caso concreto, existe evidente possibilidade de imputação segundo uma leitura ampliada do crime de lavagem de dinheiro. Desde uma perspectiva racional, por certo esse entendimento poderia não fazer sentido.33 Entretanto, é de se recordar que o instituto da lavagem de capitais porta-se, muitas vezes, como uma norma de reforço a perspectivas outras, no caso, de política criminal de (certo) controle no trânsito de moedas. Isso foi teoricamente ultimado com as previsões da Instrução Normativa 1.888/2019 (LGL\2019\3478).

De modo geral, a doutrina define as muitas possibilidades de fases da lavagem,34 sendo, na maioria das vezes, seguida a definição do Grupo de Ação Financeira Internacional (GAFI), segundo a qual poderiam ser vistas as fases de ocultação, de transformação, mascaramento ou dissimulação do capital, e de integração, vale dizer, de introdução dos valores na economia formal.35

A primeira diria respeito à

colocação do dinheiro no sistema econômico. Objetivando ocultar sua origem, o criminoso procura movimentar o dinheiro em países com regras mais permissivas e naqueles que possuem um sistema financeiro liberal. A colocação se efetua por meio de depósitos, compra de instrumentos negociáveis ou compra de bens.

Já a segunda, versando sobre a ocultação,

consiste em dificultar o rastreamento contábil dos recursos ilícitos. O objetivo é quebrar a cadeia de evidências ante a possibilidade da realização de investigações sobre a origem do dinheiro. Os criminosos buscam movimentá-lo de forma eletrônica, transferindo os ativos para contas anônimas – preferencialmente, em países amparados por lei de sigilo bancário – ou realizando depósitos em contas abertas em nome de ‘laranjas’ ou utilizando empresas fictícias ou de fachada

dar-se-ia a integração, onde

os ativos são incorporados formalmente ao sistema econômico. As organizações criminosas buscam investir em empreendimentos que facilitem suas atividades – podendo tais sociedades prestarem serviços entre si. Uma vez formada a cadeia, torna-se cada vez mais fácil legitimar o dinheiro ilegal

5. LAVAGEM DE DINHEIRO E CRIPTOMOEDAS: NOVAS POSSIBILIDADE DE INCIDÊNCIA

Para além de questões tradicionais e basilares, no entanto, existe hoje uma real preocupação sobre como a lavagem de dinheiro pode assumir um papel de destaque em relação à temática das criptomoedas.

A discussão, fundamentalmente, gira em torno das possibilidades de aquisição de criptoativos com dinheiro de origem ilícita; operado por pessoa diversa do autor do crime antecedente; quando isso é feito para obstaculizar a origem do próprio bem; se o espaço virtual anônimo já seria evidência de crime; ou, mesmo, se existe posterior ajuste em declarações de posse de criptoativos, ou, mesmo, retificações em imposto de renda visando tornar lícito dinheiro de origem ilícita.

não se pode dizer que as criptomoedas são inerentemente criminosas. São, pois, um meio, mas não um fim criminoso, e isso precisa ser evidenciado.

# (ESTELLITA, 2020)

O exame de manifestações oficiais de vários organismos internacionais sobre o tema, publicadas até o começo de 20184 – FATF,Autoridade Bancária Europeia (Europäischen Bankenaufsicht – EBA), Banco Central Europeu e União Europeia –, evidencia que os catalisadores para a lavagem que acompanham as moedas virtuais são a descentralização, a transnacionalidade livre de obstáculos, as possibilidades de anonimato e a possibilidade de transição do mundo virtual para o mundo real viabilizada pelas exchanges. 5 Esses catalisadores são por ela agrupados em três características com especial relevância para o tema da lavagem de dinheiro: a) descentralização; b) pseudoanonimidade; c) globalidade

Quanto à descentralização, na falta de uma instância gerenciadora central, não há um agente que possa examinar operações suspeitas e reportá-las. Esse papel, relativamente ao tráfego de dinheiro eletrônico, é desempenhado por bancos. Isso inexiste no sistema da BTC. Desse modo, a descentralização, que é uma vantagem operacional, acaba sendo uma desvantagem sob o ponto de vista da administração da justiça. Em caso de investigação, a única instância à qual se pode recorrer é representada pelos intermediários,as exchanges, que fazem a conexão entre o sistema do BTC e o mundo real econômico o. E não se deve olvidar que nem todos os usuários de BTC necessitam de um intermediário para negociar a moeda, que pode ser comercializada diretamente entre (os próprios) usuários, no que se denomina P2P (GRZYWOTZ, 2019, p. 98)

Quanto à pseudoanonimidade e ao contrário do que se pode pensar, as operações com BTC não são um meio de pagamento anônimo, mas garantem um grau de privacidade que é relevante em termos de persecução penal da lavagem de capitais. Ao abrir uma “conta”, a pessoa não tem de se identificar e basta o acesso à internet e a um cliente de BTC para gerar um par de chaves e ter acesso a transações.Ademais, uma mesma pessoa pode ter diversos endereços de BTCs, o que agrega mais anonimidade às transações. Porém, o fluxo de transações é todo registrado no blockchain, 6 o que dá uma transparência relevante quanto a todo o histórico de transações com os BTCs.A atribuição de identidade aos endereços de BTCs só pode ser feita por um terceiro (uma exchange, por exemplo), já que o código não contém ou comporta os dados pessoais do titular do endereço (GRZYWOTZ, 2019, p. 99-100). É isso que explica que os atuais esforços de regulação do setor, sob o ponto de vista da prevenção de lavagem, dirijam-se especialmente às exchanges, exigindo que tomem medidas de identificação dos usuários (Know Your Customer – KYC).

Por fim,a globalidade se caracteriza pelo fato de que as transações podem ser realizadas globalmente sem nenhum obstáculo; para isso, de novo, é suficiente o acesso à internet e a um cliente de BTC. Isso também vale para a troca de BTC por moedas estatais, que pode ser feita por intermediários ou mesmo por pessoas privadas.Todas essas transações são realizadas sem instâncias de controle, o que torna esse ambiente propício para aqueles que pretendem lavar dinheiro, nas tradicionais fases da lavagem de dinheiro: colocação, dissimulação ou transformação e integração (GRZYWOTZ, 2019, p. 100)

Na fase da colocação, pode-se pensar na inserção de valores patrimoniais no sistema de BTC, ou seja, a obtenção de BTCs com valores provenientes da prática de crime anterior. Isso pode ser feito por meio da aquisição em exchanges; em caixas automáticos de compra de BTCs com valores em espécie; em plataformas que conectam usuários para transações diretas; por meio da venda direta de bens obtidos com a prática de crimes e do recebimento do pagamento diretamente em BTC; pela aquisição direta de BTCs com o produto de crime, quando, por exemplo, a venda de drogas é remunerada em BTCs; ou pela transferência de BTCs de um para outro endereço de BTC (GRZYWOTZ, 2019, p. 101-103)

A dissimulação pode ser diferenciada em simples e complexa. A simples se dá ante a possibilidade de que uma mesma pessoa possa gerar infinitas chaves públicas, mudando o endereço dos BTCs sem que o usuário perca o controle sobre eles. Também se pode usar os endereços de BTCs de terceiros ou mesmo de agentes financeiros. Em qualquer desses casos, porém, o caminho e o rastro das transações serão facilmente identificáveis, dada a transparência do blockchain. A identidade dos usuários, ou seja, dos titulares dos endereços de BTC, contudo, não é passível de conhecimento a partir dos dados do sistema (GRZYWOTZ, 2019, p. 104). É essa combinação entre alta rastreabilidade e não identificação do titular do endereço que permite falar em pseudoanonimidade, e não em uma anonimidade total.

As formas mais complexas de dissimulação ou transformação envolvem os chamados mixing-services (serviços de mistura ou mescla), cuja função é justamente apagar o rastro das BTCs dentro do blockchain, ou seja, romper com a transparência inerente ao sistema. O mixing pode ser feito já por meio de serviços de carteiras (web-wallets), nos quais o controle sobre a chave privada não fica com o usuário, mas com o prestador de serviço.Tal qual em um banco, que gere os valores depositados pelos clientes, os quais, consequentemente, têm contra ele apenas uma pretensão de pagamento das cédulas depositadas, e não diretamente, direito a esta ou àquela cédula,assim funcionam esses serviços de web-wallet. Os BTCs custodiados por esses provedores de serviços não necessariamente serão os mesmos que serão pagos ao usuário. Por isso, as web-wallets podem ser usadas para fazer o mixing.A diferença no caso do uso de web-wallets é que há uma espécie de autoridade central (o provedor do serviço) que tem acesso a todas as informações quanto às transações e que poderá, se o desejar ou se for a isso obrigada, implementar medidas de identificação de cada usuário (KYC), o que diminuirá o grau de anonimidade, permitindo, ainda, a implementação de medidas de supervisão antilavagem (GRZYWOTZ, 2019, p. 104-105). Entre nós, a INRFB n. 1888/2019 passou a exigir a identificação dos usuários de exchanges de criptoativos, todavia a regulação tem fins tributários e não de prevenção à lavagem

Há, ainda, serviços de mixing especializados, cuja função é criar uma camada a mais de encobrimento entre o remetente e o receptor de BTCs. Cada usuário remete uma quantidade de moedas virtuais para o mixer e designa um ou mais endereços (geralmente novos) nos quais quer receber a mesma quantia, descontado o preço cobrado pelo serviço de mescla.As moedas, para falar de modo metafórico, são jogadas em uma “piscina” com as moedas de outros usuários, misturadas e, então,remetidas para os endereços designados pelo usuário.A remessa pode, ainda, ser fracionada em diversas pequenas transações, 8 usando diversos provedores de mixing em operações sucessivas. Pesquisas mostram que esses serviços têm o potencial de tornar impossível o rastreamento das moedas, além de implicarem riscos aos próprios usuários, como o de furto ou mesmo de desvio ou perda dos valores pelo encerramento ou bloqueio do serviço (GRZYWOTZ, 2019, p. 106-107)

A integração pode ser feita pela troca de BTCs por moedas estatais por meio de exchanges de criptoativos ou pela aquisição direta de bens e produtos. Em países com controle sobre as exchanges, isso pode levar à descoberta da transação. Entretanto, como uma das características da BTC é justamente a globalidade, pode-se facilmente optar pela execução dessa transação em países com medidas de controle antilavagem menos rigorosas (GRZYWOTZ, 2019, p. 109)

Diferentemente do que acontece com depósitos bancários, as transações com BTCs são rastreáveis até a primeira transação incriminada, de forma que sempre será possível determinar a parcela criminosa, o que viabiliza a aplicação do critério da contaminação parcial (GRZYWOTZ, 2019, p. 252).

No sistema BTC, também seria viável determinar um limite mínimo para a contaminação, medida que evitaria o bloqueio do tráfego econômico e financeiro pela contaminação de grande parte dos valores nele utilizados. Isso evidencia como uma possível aplicação da tecnologia de blockchain aos depósitos bancários traria para a moeda legal as vantagens dessa tecnologia: a rastreabilidade até a primeira transação com valores ilegais, a aplicação da contaminação parcial e, consequentemente, o afastamento da perspectiva de bloqueio significativo ou total do tráfego econômico por uma contaminação ampla e generalizada