INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS E SEGURANÇA INTERNA

O "falso" anonimato da *Blockchain*:

Como rastrear o circuito do dinheiro para a concretização probatória e descoberta da verdade

Gonçalo Alexandre da Piedade de Oliveira

Dissertação de Mestrado em Ciências Policiais

Área de especialização em Criminologia e Investigação Criminal

Orientação científica:

Prof. Doutor José Fontes

Academia Militar - Instituto Universitário Militar

Professor Lourenço Pimentel

Instituto Superior de Ciências Policiais e Segurança Interna

Outubro,2023

Dedicatória

A toda a minha família

Agradecimentos

À minha família que durante o processo educativo foi essencial na minha evolução como homem e, por isso, este último ofício é vosso.

Epígrafe

“O que for, quando for, é que será o que é.”

-Alberto Caeiro

Resumo

A presente dissertação surge no âmbito do curso de mestrado em Ciências Policiais, área de especialização em Criminologia e Investigação Criminal do Instituto Superior de Ciências Policiais e Segurança Interna.

O falso anonimato da *blockchain* permitiu que durante os seus primeiros anos de vida fosse um lugar perfeito para o agente do crime transferir e guardar os seus capitais em carteiras digitais. No entanto, nesta dissertação abordamos de que forma esta tecnologia não é totalmente anónima. Para isso, são introduzidos conceitos como a *blockchain*, criptomoedas e de que forma são usados pelos agentes do crime. Porém, as suas características também permitem ao investigador rastrear o circuito do dinheiro para a concretização probatória e descoberta da verdade.

Desta forma, realizamos um estudo de caso, onde aleatoriamente escolhemos uma carteira suspeita e tentamos rastrear até a podermos identificar, para isso utilizamos o software Graphsense.

Posto isto, analisámos formas possíveis que a Investigação Criminal tem para a repressão criminal desta natureza, entendemos também as suas limitações e discutimos possíveis políticas de combate ao cibercrime.

Palavras-chave: *Blockchain*. Criptomoedas. Investigação Criminal. Graphsense. Cibercrime.

Abstract

This dissertation comes within the scope of the Master's course in Police Sciences, specialization in Criminology and Criminal Investigation, of the Higher Institute of Police Sciences and Internal Security

The false anonymity of the *blockchain* allowed the criminals to transfer and store their assets in digital wallets during its early years, making it a perfect haven for such activities. However, in this dissertation, we will discuss how this technology is not entirely anonymous. To do this, we introduce concepts such as *blockchain*, cryptocurrencies, and how they are used by criminals. Nevertheless, their characteristics also enable investigators to trace the money trail for probative purposes and the discovery of the truth.

In this manner, we conducted a case study in which we randomly selected a suspicious wallet and attempted to trace it until we could identify it, using the software Graphsense.

Furthermore, we analyzed possible methods that Criminal Investigation has to combat crimes of this nature, understood their limitations, and discussed potential policies to combat cybercrime.

Keywords: *Blockchain*. Cryptocurrency. Criminal Investigation. Graphsense. Cybercrime.

Índice

Índice de Figuras

Abreviaturas

API – *Application Programming Interface*

BCH – *Bitcoin Cash*

BTC – *Bitcoin*

CRP – Constituição da República Portuguesa

DLT– *Distributed ledger Tecnology*

ETH – *Ethereum*

FATF – *Financial Action Task Force*

IC – Investigação Criminal

KYC – *Know Your Costumer*

LOIC – Lei da Organização da Investigação Criminal

LTC – *Litecoin*

OPC – Órgãos de Polícia Criminal

WGDC – Working *Group on Darknet and Cryptocurrencies*

Introdução

A presente dissertação surge no âmbito do curso de Mestrado em Ciências Policiais, na especialização de Criminologia e Investigação Criminal, no Instituto Superior de Ciências Policiais e Segurança Interna, com o tema "O "falso" anonimato da *Blockchain*: Como rastrear o circuito do dinheiro para a concretização probatória e descoberta da verdade", sob a orientação científica do Professor Doutor José Fontes e Professor Lourenço Pimentel.

Introduzida ao público a partir da criptomoeda *Bitcoin*, a *blockchain* é uma tecnologia digital emergente que pode ser descrita como um livro-razão público onde as transações são guardadas numa cadeia de blocos (Zheng et al., 2018), infelizmente apesar da potencialidade desta tecnologia a sua utilização nos seus primórdios focou--se no sistema financeiro (Tapscott & Tapscott, 2016).

A *blockchain*, como vai ser explicado mais à frente, é uma tecnologia que tem por base três principais características: a sua descentralização, distribuição e transparência. (Nakamoto, 2008). A partir de 2008, data da sua criação, esta nova moeda foi então utilizada pelos agentes do crime como uma forma de fazer transações fora do sistema tradicional, criando assim um mercado gigante de transações que não eram seguidas por parte das instituições internacionais e nacionais (FBI, 2014). O público em geral parece não entender o conceito de anonimato em relação à *bitcoin*, as criptomoedas são entendidas como ativos completamente anónimos.

O "falso" anonimato da *blockchain* é um termo usado para descrever que, as transações na *blockchain* não são completamente anônimas. A verdade é que, embora as transações na *blockchain* sejam pseudónimas, elas podem ser rastreadas e vinculadas a indivíduos por vários métodos.

Considerando a natureza pública e transparente da *blockchain* seria mais indicador descrever este serviço como pseudónimo do que anónimo. Um maior entendimento desta diferença seria um bom passo para a evolução desta tecnologia e a sua regularização (Balaskas & Franqueira, 2018).

A invenção das criptomoedas adicionou uma nova dimensão no processo de transações, pois estas criptomoedas são criadas por organizações não-governamentais e são transacionadas numa network digital sem qualquer tipo de intermediário, como bancos.

Dessa forma a *bitcoin* no seu início serviu como facilitador financeiro de todo o tipo de crimes como, branqueamento de capitais, fraude, tráfico de estupefacientes, cibercrime. Ou seja, nos seus primeiros anos era realmente um setor que não regulado. Até que os governos e as organizações internacionais como a Interpol se dedicaram a realizar investigações criminais de criptomoedas com o objetivo de identificar todas as partes ilícitas que participavam (Andriole, 2020), e é neste último ponto que esta investigação se vai centrar.A *bitcoin* tem uma elevada associação com o cibercrime devido á sua popularidade no mercado negro. A sua falsa anonimidade e a falta de jurisdição criam uma oportunidade para os criminosos.

Esta tese de mestrado tem como objetivo explorar o conceito de "falso" anonimato na tecnologia *blockchain* e como pode ser usado para rastrear o circuito do dinheiro, para a concretização probatória e descoberta da verdade, a conceptualização é importante para que o *mito* de que a *bitcoin* é completamente anónima acabe, e com isso exista um maior entendimento por parte da sociedade em geral do seu verdadeiro poder. O estudo analisa os vários métodos usados para rastrear transações na *blockchain* e identifica os desafios e limitações associados aos mesmos. A investigação também avalia a eficácia das ferramentas forenses existentes na *blockchain* e irá propor novas técnicas para rastrear o circuito do dinheiro

É identificado o porquê de os agentes do crime usarem as criptomoedas para fazer as transações, de que forma são usadas para transferir os ganhos ilícitos e por fim de que forma é que os OPC podem operar com o intuito de identificar os portadores das

carteiras. Este tipo de investigação demonstra ser demasiado complicado para os OPC e dessa forma internacionalmente estão a ser criados iniciativas com o setor privado. Tendo como objetivo a construção de soluções que consigam rastrear e fazer uma análise inteligente (Wainright, 2016), é dessa forma que introduzimos uma solução para facilitar o estudo de caso que iremos realizar, o GraphSense.

É com esta ferramenta que analisámos uma carteira com atividades suspeitas dentro da *blockchain* com o intuito de conseguir identificar qual a verdadeira identidade do indivíduo que a controla, sendo o mundo digital um lugar sem fronteiras para a conclusão de uma análise destas é necessária a implementação de mecanismos de colaboração internacional.

Posto isso, no primeiro capítulo desta tese abordamos o método, a *blockchain*, criptomoedas e como a investigação criminal liga todos estes conceitos. No segundo capítulo, introduzimos as ferramentas de analise da *blockchain* e fazemos a escolha de qual utilizar no estudo de caso. Seguidamente introduzimos também limites da investigação criminal na *blockchain* como as medidas de *Know you costumer* e o *mixers*. No terceiro capítulo é feita a analise da utilização criminal das criptomoedas, desde a sua tipificação a exemplos práticos. No quarto capítulo fazemos o estudo de caso e no quinto analisamos os resultados e abordamos a importância de mecanismo de colaboração internacional na luta do cibercrime.

I. Enquadramento Concetual

1. Método

O século XXI é um século de inovação em todos os campos, desde a medicina até ao setor financeiro. Desta forma, todos os setores foram influenciados pela principal alteração que se deu no início do século, a criação do mundo digital. É neste "mundo" que esta investigação se vai centrar.

Posto isto, esta investigação tem como objetivo entender o "falso" anonimato da *blockchain*. Para responder a esta pergunta é necessário conceptualizar vários termos centrais neste mundo. A *Blockchain*, criptomoedas e de que forma estes conceitos se ligam com a investigação criminal.

O objetivo desta investigação é utilizar o *GraphSense* para analisar uma carteira de *bitcoin* encontrada aleatoriamente no site *bitcoinabuse.com* e identificar o seu dono. Este site tem como objetivo manter a *blockchain* segura, dessa forma, é possível reportar carteiras digitais para alertar possíveis vítimas e ajudar a suportar quem já foi vítima.

A primeira etapa será recolher dados relevantes do site *bitcoinabuse.com* sobre o endereço da carteira, data e hora da transação suspeita, valor da transação e outros detalhes pertinentes.

Com o *GraphSense*, será possível rastrear as transações que entraram e saíram da carteira de *bitcoin*, analisar padrões de gastos, identificar endereços de carteiras relacionados e muito mais. A análise também inclui a identificação de outras carteiras de *bitcoin* que estejam conectadas à carteira em questão, bem como a identificação de outros indivíduos ou entidades que possam estar envolvidos nas atividades suspeitas.

Por fim, serão tiradas conclusões sobre a identidade da carteira de *bitcoin* em questão e sobre as atividades suspeitas associadas á mesma. Serão feitas recomendações para evitar atividades criminosas envolvendo criptomoedas no futuro.

Concluindo, esta investigação responde a quais são as principais limitações e desafios dos OPC em rastrear o circuito de dinheiro na *blockchain*, que tipo de programas e software usam e como funciona, e de que forma são utilizados na investigação criminal, sendo que, na sua génese entende-se o que é o "falso" anonimato da *Blockchain*.

2. A Blockchain e as suas inovações

Segundo Evan McFarland a *Blockchain* não passa de uma "fancy database", apesar de ser referido normalmente como algo muito mais do que isso, é apenas isso. No entanto, para perceber o porquê de uma base de dados iniciar um movimento global que já definiu a segunda década do século XXI e é considerada a "quarta revolução industrial" (Schwab, 2016) vamos conceptualizar.

A ideia da *Blockchain* foi primeiro introduzida e conceptualizada por Stuart Haber e Scott Stornetta (1990), sendo que, foi com a publicação do *whitepaper* da *Bitcoin* pelo seu criador anónimo Satoshi Nakamoto (2008) que ficou mais conhecida. No seu significado mais amplo, a *blockchain* é um tipo de livro razão distribuído (Distributed ledger technology). O significado de distribuído é a descentralização dos arquivos de informação que são controlados pelos participantes, sendo que, têm os mesmos direitos e controlo. Este tipo de vantagem permite que os participantes da *blockchain* possam partilhar, sincronizar e reportar todas as transações *peer-to-peer* sem a ajuda de terceiros. (Natarajan, Krause & Gradstein, 2017).

A grande diferença entre a *blockchain* e outro tipo de DLTs é o uso de criptografia e métodos algorítmicos com o objetivo de permanentemente estar a verificar a estrutura e a veracidade dos dados em forma de blocos que se ligam em cadeia (Natarajan et al., 2017), daí o nome *blockchain*.

Esta tecnologia então permite a gestão de dados de transação de uma forma descentralizada numa network de computadores por todo o mundo num sistema *open-source*. Qualquer alteração do software na *Blockchain* deve ser algo de um processo de consenso porque ninguém tem a autoridade total para tomar essa decisão (Glaser &

Bezzenberger, 2015). O sistema é transparente, pois todas as transações são guardadas no livro razão online onde todos podem ver e analisar, e é neste ponto que a nossa investigação se vai centrar. Sendo que, a descentralização e a criptografia da *blockchain* impedem qualquer tipo de alteração dos dados. (Abdulhakeem & Hu, 2021).

A descentralização e transparência oferecem várias vantagens, como a redução do potencial de fraude, um maior controlo e a minimização da necessidade de intermediários., é dessa forma que a evolução desta tecnologia vai alterar a forma como o Sistema financeiro mundial funciona, enfraquecendo o Sistema financeiro tradicional, que é ainda a maneira mais utilizada para fraude fiscal e branqueamento de capitais ilegais (IOCTA,2021).

No entanto, é importante entender que a tecnologia por detrás da *bitcoin* não tem esse objetivo, o crime, nem a maior parte dos seus utilizadores que procuram a anonimidade no mundo moderno da vigilância universal. (Greeshma,2015)

3. As criptomoedas e a sua utilidade

O Sistema financeiro tradicional define criptomoedas como dinheiro digital não regulado por nenhuma entidade estatal ou pelo Banco Central, que é gerado e armazenado eletronicamente, podendo ser utilizado como meio de pagamento (BCE,2022).

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.

No entanto, existem vários tipos de moedas digitais, sendo que, as criptomoedas apresentam-se sendo uma moeda descentralizada, com base na tecnologia *blockchain*,

esta tecnologia então oferece a possibilidade de não existir intermediários mesmo garantindo a segurança de todos os intervenientes. (Prybila et al., 2020)

Contudo, o valor das criptomoedas é apenas um compromisso feito por uma entidade privada, sem existir qualquer regulação por parte de uma entidade pública que possa proteger os seus utilizadores, como acontece com moedas oficiais (Carlos Carvalho et al., 2021).

Para definir criptomoedas iremos utilizar a *bitcoin* como modelo, devido á sua preponderância no mercado, desta forma a *bitcoin* segundo o seu criador Satoshi Nakamoto é uma alternativa às lacunas criadas pelas instituições financeiras (Nakamoto,2008), desta forma existem algumas vantagens que iremos referir para descrevermos este tipo de tecnologia da melhor forma, para entender o porquê de ser tão atrativo para o mundo criminoso.

A inflação acontece quando existe a necessidade de criar mais dinheiro a circular, no entanto, esta necessidade cria a inflação que diminui o valor da moeda, no entanto, o protocolo da *bitcoin* tem um limite de 21 milhões de moedas, ou seja, é impossível criar mais *bitcoin* prevenindo assim a inflação.

O facto de a moeda ser autossustentável, quer isto dizer, que a *bitcoin* ao ser transacionada e guardado por hardware, os registos de transações estarão sempre corretos e atualizados, mantendo a integridade da moeda e do registo (Nakamoto,2008).

É importante estabelecer a descentralização da *bitcoin* é uma das mais importantes virtudes desta tecnologia, a decentralização ajuda a manter o monopólio da moeda livre e sem restrições, para que nenhuma organização ou ninguém consiga controlar e determinar o seu valor, o que mantem o seu valor estável e seguro.

Ao ser *peer-to-peer* a *bitcoin* elimina a necessidade de uma terceira entidade a regular cada transação como VISA, posto isto, as transações tornam-se bastante mais fáceis e baratas, criando assim transações sem fronteiras praticamente instantâneas e com um custo-benefício melhor (Laskshete,2022).

4. Investigação Criminal

A lei não define a Investigação Criminal, isto de um ponto de vista metodológico e epistemológico, posto isto, não existem procedimentos ou estratégias que são adotadas pelo investigador, mas caracteriza-se como um conjunto de diligências (Braz, 2013).

No artigo 9.º, alínea b) da Constituição da República Portuguesa (CRP) é estabelecido como a fundamental tarefa do estado "garantir os direitos e liberdades fundamentais e o respeito pelos princípios do Estado de direito democrático", para isto, no número 1 do seu artigo 272.º, "a polícia tem por funções defender a legalidade democrática e garantir a segurança interna e os direitos dos cidadãos".

Deste modo, na Lei de Organização de Investigação Criminal (Lei n.º 49/2008, de 27 de agosto), no seu artigo 10.º, define a IC como um "conjunto de diligências que, nos termos da lei processual penal, visam averiguar a existência de um crime, determinar os seus agentes e a sua responsabilidade, descobrir e recolher as provas, no âmbito do processo". Dessa forma explicamos num sentido jurídico-penal que o crime corresponde a uma conduta por ação ou omissão, típica, ilícita, culposa e punível.

Segundo Oliveira (2004) a IC é uma atividade que está inserida nas medidas que um Estado desenvolve para que a criminalidade e o crime possam ser reprimidos.

A investigação criminal não visa a formulação de causas explicativas e etiológicas da criminalidade em geral ou a categorização de crimes. Esta, apenas procura explicar e demonstrar concreta e objetivamente um determinado crime, para que, possa ser exercido o Direito e a realização da Justiça (Braz, 2013,).

No âmbito desta investigação é necessário entender que fazer a IC no mundo digital é diferente por isso é necessária cautela, porque se a tecnologia facilita a investigação criminal também pode acompanhar violações aos direitos fundamentais, como o a privacidade, que é um direito fundamental para a vivência com dignidade e segurança.

II. Ferramentas de análise da Blockchain

Recentemente, temos observado o aumento da procura de ferramentas de análise da *blockchain* tanto na indústria como na academia, seja para analisar transações de cripto ativos seja para garantir que as regulações estão em conformidade. A verdade é que os OPC necessitam de novas ferramentas e técnicas para conseguir rastrear os fluxos de dinheiro.

Além disso, é importante referir que existe já população que utiliza as moedas virtuais como forma de pagamento convencional, ou seja, este fluxo de dinheiro também é possível observar com estas ferramentas e tentar perceber de que forma o dinheiro é utilizado, entende-se de que forma a população olha para a moeda, como um investimento ou um substituto das moedas convencionais.

As mais valias da análise da *blockchain* são imensas, podem responder a questões como quanto tempo a moeda fica em média nas carteiras, e quantas transações é que cada carteira realiza, estes indicadores e económicos são importantes, no entanto, esta investigação vai se focar na efetividade destas ferramentas para a Investigação Criminal.

Neste momento existem duas principais opções. De um lado, observamos serviços comerciais que oferecem a análise de carteiras de cripto ativos e transações por interfaces e APIs. Desta forma é possível obter melhores resultados com o cliente sem os custos de serviços serem elevados conseguido fazer a ligação com corretoras com as *tags* de atribuição.

Do outro lado, existem, também, programas gratuitos que oferecem acesso a transações na *blockchain* com uma capacidade de demonstrar gráficos de ligação entre transações, como vamos observar de seguida.

Blockchain Explorer é uma das mais reconhecidas ferramentas de análise da *blockchain*. Tem várias características como a facilidade de navegar no seu site, consegue rastrear transações individuais, apresentando gráficos e estatísticas. Permite também identificar as transações colocando um nome, ou *tag*, para mais tarde ser mais fácil a sua

identificação. Tem um sistema que se foca em duas componentes principais. Primeiramente, cria um índice de transações e endereços em relação às carteiras pretendidas, bem como é capaz de demonstrar informações como estatísticas e informações relacionadas com o endereço e por fim na *Blockchain Explorer* é possível pesquisar transações, endereços ou blocos de transações, apurar quais as transações ou blocos mais recentes e observar algumas informações, como o preço médio de cada *Bitcoin* e o volume de transações. (Blockchain.com, 2023)

Em segundo lugar introduz-se a *BlockSci*, que é uma plataforma de software de *open-source* para análise de *blockchain*. Segundo a sua descrição utiliza uma base de dados analítica na memória, o que a torna entre 15 a 600x mais rápida do que as ferramentas existentes. Como principais características oferece a capacidade de interagir com várias *blockchains* como *Litecoin, Namecoin e Xcash*, assim sendo, também oferece uma biblioteca de ferramentas analíticas e de visualização úteis para observar as transações. Estas ferramentas mostraram ter alguns problemas e dessa forma nesta investigação foi utilizado uma terceira opção a *Graphsense.*

1. Graphsense

Criado pelo *Austrian Institute of Technology* e suportado pelo projeto KIRAS KRYPTOMONITOR, *Graphsense* é uma plataforma analítica de cripto ativos com ênfase em soberania total de dados, transparência algorítmica e escalabilidade, é uma ferramenta *open source* e gratuita, suporta as maiores criptomoedas do momento como *Bitcoin* (BTC), *Bitcoin Cash* (BCH), *Litecoin* (LTC) e *Ethereum* (ETH).

A mais-valia da utilização desta ferramenta é a sua capacidade interligação entre *blockchain*s e corretoras diferentes. Oferece um painel básico, que facilita a investigação a utilizadores não profissionais, a diferença entre esta ferramenta e as mencionadas anteriormente é a capacidade de ter acesso a elementos estruturais e ligação direta a carteiras e gráficos de identidade, ou seja, tem a capacidade de identificar atores que interagem entre si ao longo das transferências de cripto ativos.

Com este tipo de software é possível fazer uma pesquisa intensiva de carteiras digitais, observar transações entre carteiras, inspecionar mega data e encontrar caminhos digitais que se conectem automaticamente.

Para o interesse da investigação criminal este tipo de ferramentas tem um importante valor forense, sendo que, pode ser utilizada pelo investigador para obter prova digital forense. Já foi utilizada em investigações realizadas pela Europol, tendo dessa forma a capacidade de preservar extrair e analisar a prova, para que mais tarde seja utilizada em tribunal.

Para a realização do estudo de caso foi pedido acesso a ferramenta por uma API, embora seja uma ferramenta gratuita a sua utilização necessita de um poder computacional muito elevado, dessa forma foi nos concedido uma chave pelos seus criadores para que pudéssemos utilizar na *cloud.*

2. Os seus desafios

Anteriormente foi introduzido de que forma estas ferramentas ajudam os OPC e de que forma operam, no entanto, existem ainda muitos desafios que impedem investigador de identificar dono das carteiras.

A problemática da identificação num sistema descentralizado é central (Balaskas, Franqueira, 2018), quer isto dizer o quê, enquanto no sistema financeiro tradicional o OPC pode em caso de suspeita suspender uma conta num banco, isso não é possível na *blockchain*. Para isso, o investigador tem de esperar que essa carteira faça a ligação com uma corretora (serviço centralizado), para que OPC entre em contacto com essa corretora, para pedir a identificação dessa carteira. Sendo que, isto pode não ajudar o investigador, pois é ainda necessário entender que tipo de medidas e regulações a corretora está a impor.

Anteriormente foi introduzido a necessidade de poder computacional necessário para utilizar este tipo de ferramentas, ou seja, o investimento inicial para que um programa destes seja utilizado numa sede de investigação criminal é muito elevado criando assim algumas dificuldades numa maior adoção desta solução. Durante o nosso estudo de caso foi nos concedido uma API, mas apenas teríamos

acesso a 1000 pedidos por hora, o que se mostrou ser suficiente, mas numa investigação mais elaborada não seria.

Outro dos principais desafios é a possível utilização de criptomoedas que tem como objetivo manter a privacidade dos seus utilizadores como Monero e Zcash (Zhang, 2023), sendo que para dificultar ainda mais o trabalho foram criados *Mixers* que vai ser abordado mais a frente.

A utilização de diferente criptomoedas presenta também um desafio, como observámos anteriormente existem ferramentas de análise que não conseguem fazer a ligação entre *blockchain*s o que adiciona outra camada de complexidade na monotorização das transações.

3. Know your Costumer

A conformidade regulatória é criada e essencial para impedir a corrupção (Ferreira,2018), dessa forma, as medidas Know your Costumer são um conjunto de procedimentos utilizados por instituições financeiras para verificar a identidade dos seus clientes (Bilali,2012).

As medidas têm como objetivo garantir a conformidade regulatória, prevenir atividade ilícitas, branqueamento de capitais ou financiar terrorismo. Desta forma, os utilizadores são obrigados e enviar informações pessoais como documentos de identificação válidos, comprovativo de morada, ou até fontes de rendimentos num padrão mais complexo (Ferreira,2018).

Estas medidas objetivam conhecer melhor os seus clientes e estabelecer uma base de confiança e cumprir as obrigações regulatórias para que a segurança e integridade do sistema financeiros sejam garantidos (Chen,2023).

Estas medidas de conformidade regulatória promovem o exercício de atividades económicas éticas, transparentes e de acordo com as leis nacionais (Siqueira e Francischetto, 2020)

Como foi dito anteriormente, a pouca vida deste setor é uma *chamada* para os agentes do crime, dessa forma é importante, também, entender que as medidas aplicadas pelas diferentes corretoras indicam a sua forma de lidar com o risco de oferecerem uma plataforma para o branqueamento de capitais e fraude, como se pode observar com a Bitlatzo.com.

Para fazer o registo na Bitzlato.com as medidas KYC são o fornecimento de uma cópia digital do documento de identificação oficial e uma foto do rosto para que o utilizador que se esteja a registar seja o mesmo do documento de identificação.

Sendo que a comparação com o KYC da Huobi.com é necessário também um documento de identificação oficial, para que não seja uma pessoa politicamente exposta ou esteja sujeito a sanções internacionais, mas a grande diferença é no comprovativo de endereço, que coloca um nível maior nível de segurança para garantir a veracidade do utilizador e dos seus dados. No entanto, é sempre possível que a Huobi solicite mais informações adicionais, dependendo dos requisitos e política internas.

Posto isto, este tipo de ferramentas são essências para os OPC conseguirem realizar o seu trabalho, mitigando assim os riscos de fraude e usurpação de identidade. Esta conformidade regulatória que tem de ser exercida pelas corretoras de criptomoedas, sendo que, é a única forma de retirar o anonimato da *blockchain*.

4. O que é um Mixer

A transparência e a anonimidade da *blockchain* criam um mercado de transações totalmente aberto ao público, desta forma, o mercado ilegal criou maneiras de contornar estas características para esconder a identidade de quem o utiliza, os *mixers* (Biryukov et al., 2019).

Um *mixer* é uma ferramenta que tem como objetivo manter o máximo de anonimidade do dono da carteira de cripto, ou seja, o seu trabalho é que a ligação entre o comprador e o vendedor não seja direta (Shojaeinasab et al., 2023). Desta forma a

compra feita à carteira A não vai diretamente para a carteira B, é enviada para a carteira C, o *mixer*, que por um preço envia o dinheiro para mais carteiras para que o rastro seja perdido antes de enviar para a carteira B.

Existem vários tipos de *Mixers* tradicionais e modernos (*ibid*) ou seja, escondem transações de forma mais complicada, passando por centenas de carteiras ao longo de meses, sendo então completamente perdido o rastro do dinheiro, impossibilitando assim muitas vezes os OPC de rastrearem o dinheiro se não tiverem a carteira B identificada.

A problemática principal com este tipo de ferramenta é que não é ilegal, no entanto, tanto a União Europeia como os Estados Unidos da América já tomaram medidas judiciais contra os mais conhecidos *mixers* devido a todas as suas aplicações ilegais, tenhamos este exemplo

> "*users to send bitcoins to recipients in a manner designed to conceal and obfuscate the source of the bitcoins. This process allows . . . customers engaged in unlawful activities to launder their proceeds by concealing the nature, source, and location of their 'dirty' bitcoin."*

Este foi o depoimento contra um dos primeiros *mixers* a ser perseguido judicialmente pelos EUA (Chen,2021).

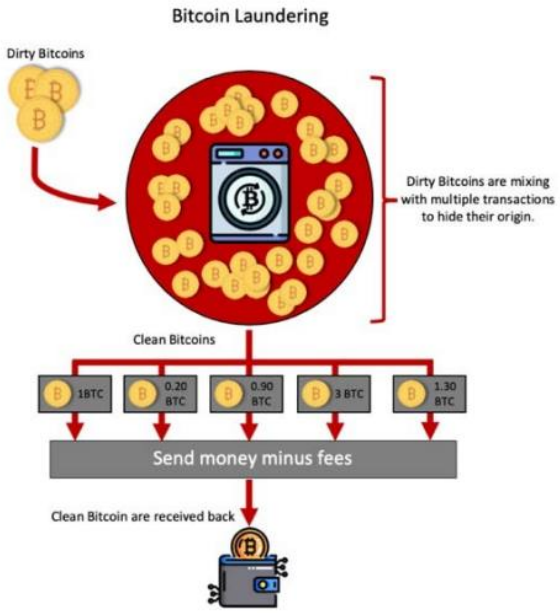

Figura - "como funciona um *mixer*" Interpol

III. O uso criminal de criptomoedas

A escala do uso ilícito de criptomoedas é difícil de estimar, no entanto, é possível realizar uma análise com a informação produzida de investigações realizadas por organizações europeias sobre os serviços e usos ilegal das criptomoedas. Segundo relatórios realizados pelo setor privado apenas 0,34% das transações são ilícitas (Chainalyis,2021).

No entanto, existem estudos que justificam que 23% das transações podem ser ligadas a atividades ilícitas (Foley et al.,2019). Ao analisarmos ambos, entendemos que as metodologias utilizadas são bastante diferentes, no relatório é entendido que o aumento do uso legitimo das criptomoedas aumentou enquanto o ilegítimo diminuiu, sendo que, o estudo é enviesado começando pelo seu título "*Sex, Drugs, and Bitcoin: How much illegal activity is financed through cryptocurrencies*?" e acabando na pequena análise que é realizada ao pequeno mercado de compra e venda de bens ilícitos com criptomoedas.

A criação das criptomoedas teve como principal objetivo uma alternativa à moeda fiduciária e ao sistema financeiro tradicional, criou uma independência às instituições centrais e dessa forma imunidade a qualquer intervenção na privacidade dos seus utilizadores.

Já foram introduzidas as principais características das criptomoedas e o porquê de terem ganho tanta popularidade desde a sua criação, no entanto, agora vamos entender de que forma essas características são utilizadas como uma mais-valia para o agente do crime.

O foco na privacidade abriu portas a transações sem controlo, criando assim um instrumento auxiliar na prática de crimes, este quase-anonimato dificulta a identificação dos suspeitos.

Em segundo plano, observamos a descentralização da tecnologia, no sistema tradicional o foco regulatório atinge as entidades intermediárias, estas têm o trabalho de identificação e proibição de atividade suspeitas prevenindo assim a prática de crimes com o auxílio dos seus serviços. Na *blockchain* esta regulação não é possível, sendo que, a regulação torna-se mais difícil devido à natureza internacional das criptomoedas, esta falta de coerência legislativa permite aos agentes do crime atuar em ordenamentos que não tenham adotado medidas eficientes na prevenção destes fenómenos.

Como já foi referido anteriormente a *blockchain* tem um falso anonimato e dessa forma este tipo de tecnologia é associada a crimes como fraude e tráfico de estupefacientes, sendo que, serve como meio de pagamento desses serviços tanto de forma online como offline.

O branqueamento de capitais, no entanto, é a principal atividade criminosa associada com o uso ilegal do criptomoedas. O aumento da popularidade e adoção de criptomoedas levou ao aumento, também, deste tipo de fraudes (IOCTA,2023).

Na compra e venda de bens ilícitos, é importante entender que mesmo que seja dos crimes que mais aumentou em 2021 existe muito mais compra e venda de produtos ilegais com *FIAT* do que com criptomoedas, este valor está a aumentar (Chainalyis,2021).

Segundo a *Chainalysis* e o seu relatório *The 2022 Crypto Crime Report* a atividade criminal relacionada com criptomoedas em 2021 teve um maior aumento, sendo que, foram proibidas legalmente mais de 14 biliões de dólares em transações, o que comparado com 2020 foram apenas 7,8 biliões (*Chainalysis*,2022). A questão que esta investigação pretende responder também é, qual é o papel das criptomoedas nestas atividades?

1. Branqueamento de capitais

O Branqueamento de capitais consiste na dissuasão da origem das vantagens que provêm de um ilícito anterior, posto isso, tem tido várias faces. O nome advém da expressão inglesa *Money laundering*, isto porque *Al Capone* utilizava o negócio de lavandarias para lavar os seus ganhos ilícitos no início do século XX.

Esta prática que se interliga diretamente com a criminalidade económico-financeira organizada passou de imediato a ser conectada com a *bitcoin*, pois, o agente do crime entendeu que seria uma maneira de passar ao lado do sistema financeiro tradicional.

Para que se observe branqueamento de capital o ganho ilício é necessário passar por três fases. A colocação (ou *placement*), isto descreve a colocação dos bens de origem ilícita no sistema financeiro. Seguidamente é a fase de circulação (ou *layers*), é aqui que o agente do crime faz várias transferências para que o rastro do dinheiro seja perdido. Por último, observamos a fase de integração (*Integration*), onde os bens já "branqueados" entram de novo no sistema financeiro (Teixeira,2022).

Segundo a Europol com a digitalização da economia os processos de branqueamento de capitais estão a ser redefinidos, ofuscando-os. O uso de criptomoedas elimina praticamente a fase de colocação pois os ganhos já estão a circular num sistema financeiro legal.

Corretoras têm um papel muito importante na materialização deste crime, pois facilitam a troca entre moeda fiduciária e critpomoedas. Durante a colocação são abertas várias contas em corretoras que não têm um KYC desenvolvido, e por isso são utilizados documentos falsos. Despois de fazer a troca entre moedas o agente do crime realiza mais trocas, mas desta vez entre diferentes criptomoedas, é aqui que os fundos circulam pela *blockchain*, utilizam *mixers*, e podem ser perdidos. Depois a integração já está feita e o agente do crime decide manter a criptomoeda ou levantar em moeda fiduciária (Europol,2023b).

2. *Ransomware*

Um ransomware é um sequestro de dados feito por criptografia, usa como refém os arquivos pessoais ou o próprio computador, o resgate é cobrado por criptomoedas que quando o pagamento é feito o computador fica desbloqueado.

O medo que as vítimas têm que a sua informação privilegiada seja partilhada, podendo assim criar danos reputacionais e monetários, presenteia uma capacidade a este tipo de crime de ser bastante lucrativo e dessa forma tenha tido um aumento exponencial com as criptomoedas (IOCTA,2020).

Segundo estudos da *Chainalysis* existem dois tipos de ataques *Ransomware*. O primeiro é feito por parte de grupos de Crime organizado, são realizados em grande escala e atacam um grande número de organizações, sendo que, pedem um resgate mais baixo para que o mesmo seja pago. Por outro lado, existe, também, ataques que são organizados de uma forma muito maior, tenhamos, por exemplo, o ataque *WannaCry*. Durante este ataque duzentos mil computadores foram afetados em mais de cento e cinquenta países causando prejuízos na ordem dos 4 biliões de dólares. É importante referir que quando os ataques são feitos nesta escala o objetivo não é o dinheiro, mas sim o caos. (*Chainalysis*,2020a).

Estes ataques incluem grandes níveis de encriptação para conseguir roubar informação sensível que ao tornar-se pública pode causar grandes danos e dessa forma as organizações criminosas garantem o seu pagamento (Patil,2021).

3. *Malware*

Malware é um nome que se dá a vários tipos de ataques que são realizados por programas maliciosas de software. Os criminosos conseguem realizar vários tipos de ataques, como espiar, destruição de informação e recursos, interromper serviços etc… Este ataque tem uma abordagem chamada *spray-and-pray*, ou seja, são enviados milhares de emails para usuários com o objetivo de roubar poucas quantias em grande escala. (Chainalyisis,2022).

Tenhamos o exemplo do ataque *Clippers*, um ataque malicioso que intervêm numa transação de criptomoeda, que durante a mesma troca a carteira que é suposto receber o dinheiro é alterada pela do atacante, dessa forma, o pagamento da criptomoeda acaba na carteira do agente do crime invés da suposta carteira (*Chainalysis* team,2022).

4. Ponzi Scheme

Um esquema *ponzi* é um esquema tradicional de investimento financeiro, a sua principal característica é a promessa de grandes retornos, sendo que, não existe qualquer fonte de receita. Os retornos que são pagos, normalmente, são pagos pelo investimento de outras vítimas no esquema (Wang et al., 2023), mais vulgarmente conhecido como um esquema de pirâmide.

Devido às características da *blockchain* este tipo de fraude é bastante popular e por isso em 2019 foi o seu maior ano, conseguido causar um prejuízo de 4,3 biliões de dólares nas suas vítimas (*Chainalysis*, 2020a). O pouco conhecimento e o *boom* das criptomoedas foram a principal causa deste elevado número, desde então, os utilizadores têm tido mais cuidado com este tipo de fraude.

O projeto PlusToken teve início em abril de 2018 e prometeu aos seus investidores grandes retornos no seu investimento. A maior parte das vítimas foram investidores da China e Coreia do Sul. Em junho de 2019 foi publicado no site oficial a seguinte mensagem:" *Sorry, we have run",* foi esta a última mensagem oficial dos criadores do projeto.

Desde então que foram seguidas mais de 800.000 *ethereum* e 45,000 *bitcoin* com o objetivo de deter os criminosos. A análise forense permitiu entender que foram levantadas 10,000 ETH e 25,000 BTCs, sendo que, estas moedas digitais foram levantadas por 8,700 carteiras de cripto criando assim um prejuízo superior a 3 biliões de dólares. (*Chainalysis*, 2020b)

É desta forma que as criptomoedas foram integradas nas fraudes financeiras, e infelizmente ainda são vistas apenas como fraudes para o grande público. No entanto, a *Security Exchange Commission* publicou pontos a ter em atenção para não haver mais uma vítima. Estas linhas apontam para ter cuidado quando os investimentos oferecem grandes retornos e pouco risco, retornos muito consistentes, investimentos não registados, estratégias de investimento difíceis de entender, e encorajamento a não levantar o investimento, mas sim reinvestir (Securities and Exchange Commission, 2013).

IV. Estudo de Caso

Primeiramente, como já foi introduzido anteriormente é necessário encontrar uma carteira, posto isso, vamos utilizar o site *bitcoin*abuse.com, e escolher uma carteira de *bitcoin* aleatória. "1F5RH8dTtzyznsPENTkUzrG62BuhbQsXLG", foi a carteira escolhida e foi reportada 56 vezes por ser uma fraude de criptomoedas.

Figura 1- ***carteira suspeita***

O passo seguinte é a introdução da carteira no *Graphsense (Figura 2)*, ao introduzir a carteira é nos dada uma panóplia de informações sobre a mesma desde a quantidade de transações que foram realizadas pela mesma, neste caso, foram realizadas 33 transações, sendo que recebeu 30 e enviou apenas duas. O que facilita a investigação, pois entende-se que o criminoso está a tentar esconder o rastro do dinheiro pela *blockchain*, mas não da melhor forma, 15,440 euros que a carteira tinha, envia 14,041 para uma carteira que passa a ser agora a que iremos seguir (Figura 3) (1KDhVnuJ47Gzkj4QpubGfwrvSM5AKocnBf).

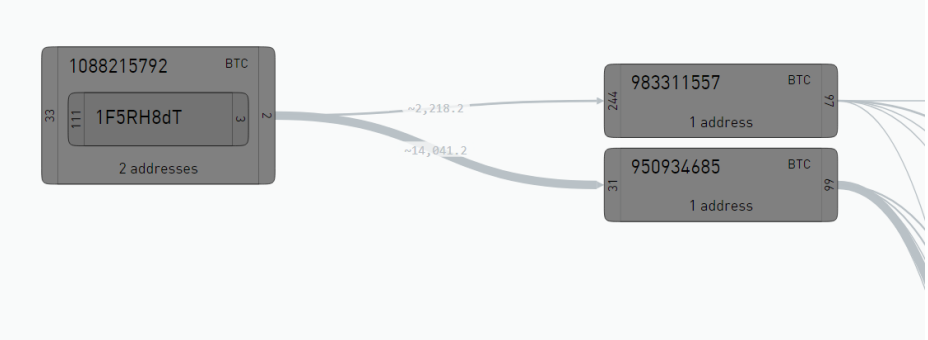

Figura 2 – ***transações feitas pela carteira suspeita***

É nesta carteira que o criminoso comete o erro de se conectar com uma corretora pela primeira vez, para provavelmente trocar a *bitcoin* por moeda fiduciária, como o euro ou dólar é neste momento que o anonimato da *blockchain* termina, pois, a carteira é conectada a uma conta numa corretora (carteira destacada a laranja, na Figura 4), neste caso, na Bitzlato.com, que iremos falar mais à frente como sendo uma corretora muito utilizada para branqueamento de capitais.

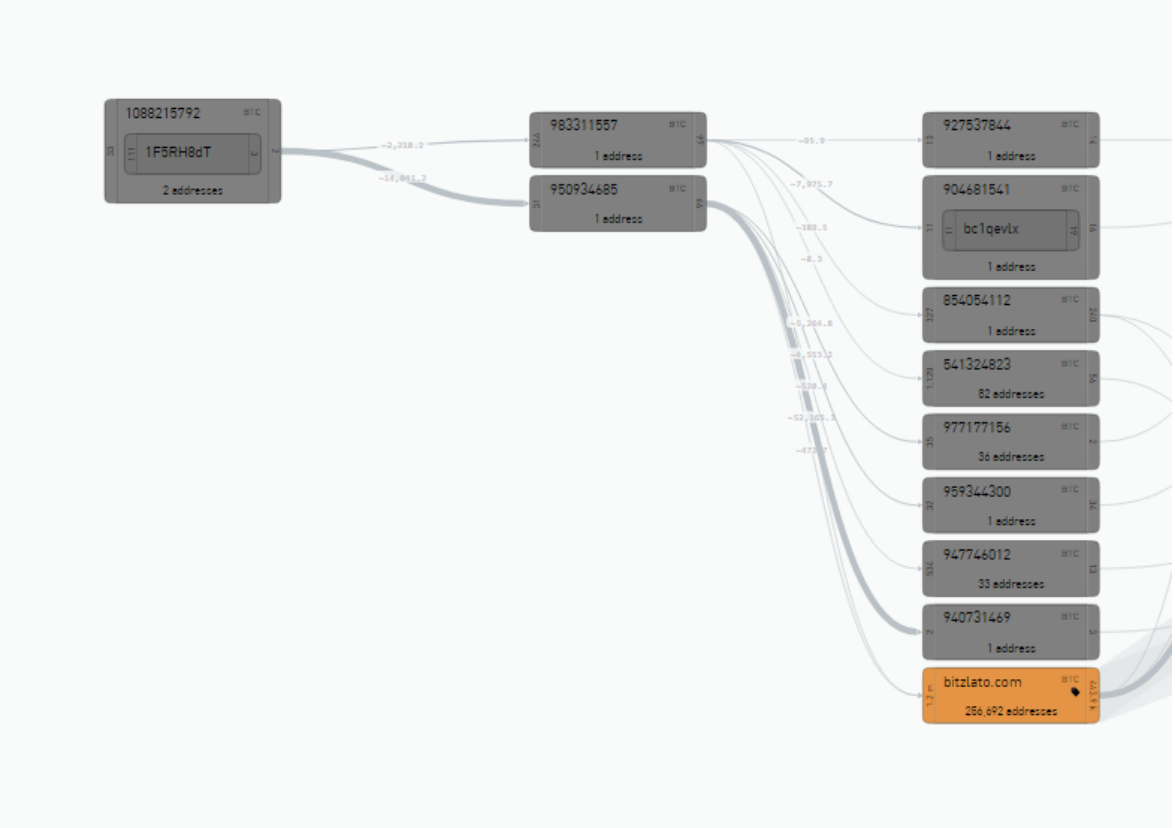

Figura 3- primeira vez que é feita a ligação com uma corretora

Posto isto, a nossa investigação em relação aquela carteira pode não identificar ninguém, no entanto, existe a capacidade de desenvolvermos mais a nossa investigação, com o objetivo de perceber se o suspeito liga a sua carteira a outra corretora onde o KYC seja mais elaborado e dessa forma poder detê-lo.

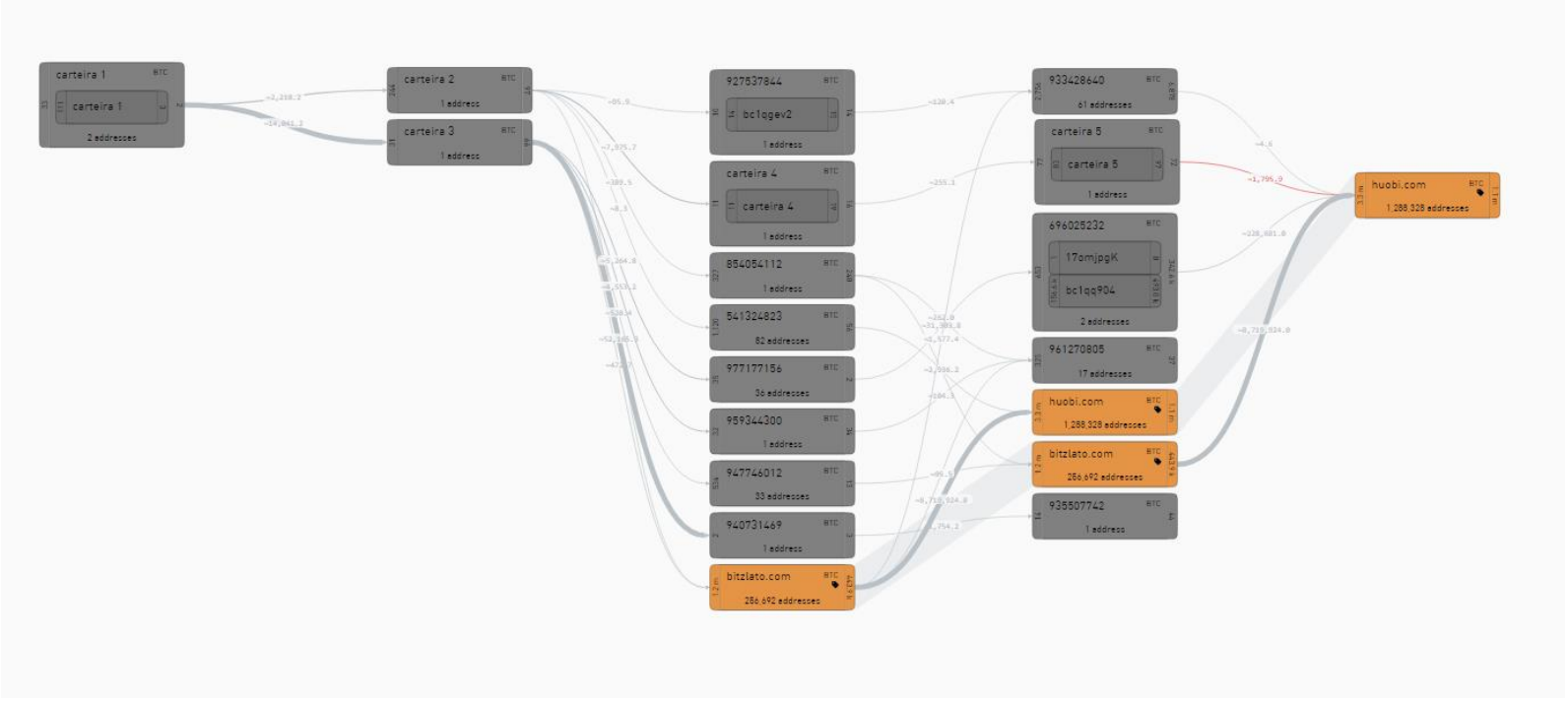

Figura 4- ligação entra carteira 5 e corretora *Huobi.com*

Address	bc1q777jy7jnh9nkfmfvk698vlent4uc6n3cs6kfea
Currency	BTC
Tags	0
Transactions	238 ↓ 122 ↑ 116
Receiving addresses	97
Sending addresses	83
First usage	09/20/2021 04:57 PM (2 years ago)
Last usage	06/02/2022 02:48 PM (last year)
Activity period	8 months 11 days 9 hours
Total received	136,805.6 EUR
Final balance	0.0 EUR

Figura 5- Informações sobre carteira 5

Observamos que a carteira 5 também faz a ligação com uma corretora, no entanto, esta corretora é a Huobi.com que é mais fidedigna do que a anterior. Como podemos observar pela informação dada pelo software a carteira digital teve ativa durante oito meses onze dias e nove horas entre 2021 e 2022. Durante esse tempo recebeu 136,805,6 euros, sendo que, de momento não tem dinheiro.

Posto isto conseguimos fazer o rastreio do dinheiro desde a nossa primeira carteira suspeita (carteira 1) até á carteira 5, o agente do crime fez cinco transferência. O rastro do dinheiro é o seguinte.

- Carteira 1 - envia 2,218,2 euros para a carteira 2
- Carteira 2- envia 7,975,7 para a carteira 4
- Carteira 4- envia 255,1 para a carteira 5
- Carteira 5- envia 1,795,9 para a corretora *Huobi.com*

É então neste momento que o principal trabalho do investigador acaba, esta informação é então chamada aos oficiais da corretora que devido à suspeita de transações ilegais por parte daquela carteira vão colaborar com os OPC e fornecer as informações pessoais da conta a qual a carteira está ligada.

V. Análise e discussão dos Resultados

O resultado obtido da realização do estudo de caso foi positivo. Foi possível observar vários métodos utilizados e entender tendências por parte dos agentes do crime.

Primeiro e segundo o site de onde foi aleatoriamente escolhida a primeira carteira a ser investigada entendemos que esta carteira foi reportada por fraude de criptomoedas, que como já estudamos é um dos principais cibercrimes que utiliza a criptomoeda como processo. É reportado como um "*This is a cryptocurrency giveaway scam*", normalmente funciona da seguinte forma. O agente faz publicidade de uma oferta de criptomoeda, normalmente *bitcoin*, a vítima faz o *log in* no site para receber a *bitcoin*. No entanto, para conseguir levantar a quantia oferecida é necessário investir dinheiro. Normalmente este investimento é mais pequeno que a quantia oferecida e dessa forma a vítima é tentada a enviar o dinheiro. Para além do dinheiro que a vítima perde, durante o registo é também pedido várias informações pessoais que agora estão na posse dos agentes do crime.

Não temos a certeza de que este é o crime pela qual esta carteira foi reportada, no entanto, pelos valores que são transferidos e análise realizadas existe a probabilidade de ser.

Depois de percebermos a possível fonte dos bens ilícitos que estamos a rastrear e ao colocar a carteira na ferramenta de auditoria, temos um trabalho bastante facilitado pois é automático, esta característica é bastante importante pois a não automatização deste processo tornaria impossível o rastreio de cartearias na *blockchain*, e dessa forma entendemos a importância da ferramenta para a investigação criminal. Neste caso não foi usado um *mixer*, o que facilitou o processo.

O único pedido que fazemos ao software é para encontrar ligações entre a carteira digital e corretoras. Neste caso, e talvez por incompetência do agente do crime a ligação é praticamente direta havendo apenas 2 transferências até o envio de dinheiro para a corretora *Bitzlato.com (Fig.4)* que iremos falar mais a frente.

Dada as características da corretora foi necessário continuar a investigação para que fosse possível fazer a identificação. Felizmente, seguindo mais uma transação o agente do crime faz a ligação com uma corretora considerada fidedigna a *Huobi.com.* Esta carteira transacionou 136.850.6 euros em apenas oito meses (Fig.6). Podemos observar que durante as transações nem sempre todo o dinheiro é transferido para as mesmas carteiras, por exemplo, a carteira 2 envia 7.975.7 para a carteira 4, mas a carteira 4 apenas envia 255,1 para a carteira 5. Esta discrepância entre valores é justificada por servir como pagamento a toda a infraestrutura do crime. Desde o website da fraude a toda a publicidade inerente ao mesmo, pagar a trabalho humano e outros custos do crime.

Se esta investigação fosse realizada por um OPC não acabaria aqui, pois iria ser feita a comunicação com a corretora para que fossem disponibilizadas informações sobre a conta a qual esta carteira está conectada, neste caso acaba aqui.

Consequentemente e dependendo do nível da infraestrutura desta rede criminosa poderiam ser expectáveis vários resultados. A conta estaria aberta com documentos falsos ou até poderiam estar a usar uma mula para conseguirem levantar o capital roubado. Não é garantido que esta investigação fosse identificar um suspeito, mas poderia servir para obter mais informação e tendências de fraude em oferta de criptomoedas online.

1. Investigação Bitzlato

Uma corretora de criptomoedas é uma plataforma online que tem como função a compra e venda de ativos digitais, também oferecem serviços similares ao sistema tradicional onde cobram taxas e comissões por transação (Alekseenko,2023).Segundo a Forbes, em 2022 existiam 600 corretoras em todo o mundo (Paz,2022), com um total de 52,1 biliões de dólares transacionados, sendo que, as maiores dez em novembro de 2022, três estão situadas em paraísos fiscais como as ilhas Caimão e Seicheles, desta forma é importante promover cooperação internacional para que estes mercados sejam

regulados com o intuito de tornar a troca de ativos descentralizados mais segura (Alekseenko,2023).

Durante a realização desta investigação a corretora Bitzlato.com foi investigada pelas autoridades Francesas e Americanas com a ajuda da Europol, no âmbito de suspeitas de facilitação de branqueamento de capitais. Consequentemente, as autoridades desmantelaram assim toda a infraestrutura digital do serviço que tinha base em França e interrogaram os principais membros da administração da plataforma (Bitzlato: senior management arrested, Europol).

A operação também envolveu autoridades judiciais da Bélgica, Chipre, Portugal, Espanha e Países Baixos.

Segundo o artigo publicado pela Europol metade das transações ligadas á corretora estavam ligadas a atividades criminais. É estimado que a corretora tenha recebido um total de 2.1 biliões de Euros.

Os resultados da Operação foram a detenção de 5 indivíduos para além do Diretor, a desativação da infraestrutura digital do serviço, apreensões de mais de 18 milhões em criptomoedas, veículos e equipamento eletrónico e o congelamento de mais de cem contas num total de 50 milhões de euros.

Este tipo de operações demonstram a importância de organizações de justiça supranacionais e coordenação internacional dos OPC.

2. Mecanismos de colaboração internacional

Segundo a última publicação da Europol os seus valores são o serviço, integridade, responsabilidade, iniciativa, parceria e diversidade. Com estes valores são o principal mecanismo de colaboração internacional relacionado com investigação internacional e partilha de informação, estamos então, numa era onde a segurança interna estende-se muito para além fronteiras, a Lei nº53/2008(Lei da Segurança Interna) é um diploma que promove esta mesma cooperação, sendo que, o seu asr.4.º

refere que, no , no âmbito de compromissos internacionais, «as forças e os serviços de segurança [FSS] podem atuar fora do [território nacional], em cooperação com […] organizações internacionais».

Com ao rápido crescimento da era digital, o cibercrime e a branqueamento de capitais tornaram-se um problema global. A criação de criptomoedas criou formas de enviar e receber dinheiro, colocando assim, desafios únicos para os OPC nacionais e internacionais. Para combater efetivamente este tipo de cibercrime e lavagem e dinheiro é importante criação de mecanismos de colaboração internacional. (IOCTA,2023)

O alcance macro deste mecanismo permite a partilha de informações, partilha de meios e conhecimentos, partilha no âmbito da cooperação operacional, partilha de experiência e modelos de policiamento, ações de formação conjuntas exercícios transfronteiriços, grupos de trabalho, redes de cooperação especializadas no domínio técnico e tático, entra outras.

Estes tipos de mecanismos são essenciais para o combate ao crime na internet pois não se limitam a jurisdições individuais e utilizam este espaço sem fronteiras de forma mais livre.

A descentralização das criptomoedas complica ainda mais a investigação e a acusação dos suspeitos, as limitações das fronteiras em relação a este tipo de crime oferece a este submundo do crime uma vantagem para quem os comete, as diferentes jurisdições, regulações e limites de recursos são algumas das lacunas que os mecanismos de colaboração internacional objetivam erradicar.

Estes mecanismos consistem na partilha de informação e partilhar as investigações individuais para que o trabalho em parcerias seja mais fácil e oferece resultados melhores. Tenhamos por exemplo o INTERPOL *Working Group on Darknet and Cryptocurrencies* que é uma plataforma onde as mais recentes técnicas de investigação são partilhadas pelos países membros, estas técnicas podem ser desenvolvidas pelo setor privado e pela Academia. (*Combatting Cyber-enabled financial crimes in the era of virtual asset and darknet servisse providers, INTERPOL*).

Existe por outro lado o *Interpol Global Complex for Innovation* que se foca no cibercrime e serve como plataforma de cooperação para todos os OPC, por último existe o *The Financial Action Task Force*, é uma organização supranacional que se dedica ao combate de lavagem de dinheiro e financiamento de terrorismo, cria um standard e tem um impacto importantíssimo na regularização de criptomoedas e ativos digitais (FATF,2012-2023).

Concluindo, os mecanismos de cooperação global fornecem então uma estrutura para os países trabalharem em conjunto, partilhar recursos e combinar os poderes para combater o cibercrime.

A *bitcoin* tem uma elevada associação com o cibercrime devido á sua popularidade no mercado negro. A sua falsa anonimidade e a falta de jurisdição fazem criam uma oportunidade para os criminosos. No entanto, é importante entender que a tecnologia por detrás da *bitcoin* não tem esse objetivo, o crime, nem a maior parte dos seus utilizadores que procuram a anonimidade no mundo moderno da vigilância universal. (Greeshma,2015)

Considerações Finais

Para entender o papel da criptomoedas e da *blockchain* na investigação criminal é importante entender as características que as tornam tão atraentes para as atividades ilícitas.

A *blockchain* tem por base três fatores principais, a sua transparência que permite observar todas as transações nela realizadas, segurança que é garantida pela criptografia e por último a descentralização onde impossibilita o controlo da rede por apenas uma entidade. É neste último ponto e mais importante que o agente do crime tem interesse. Esta caraterística dá vida também às critpomoedas.

É entendido a forma como o agente do crime utiliza esta nova moeda para fugir ao olho dos OPC, e a forma como a sua tecnologia é utilizada para o crime, desde servir como pagamento para os *Ransomware, malware* ou observamos a realização de esquemas fraudulentos mais elaborados como *Ponzi Schemes.*

Desta forma é importante impor a diferenciação dos crimes, pois é a convergência entre crime financeiro e cibercrime, um é a obtenção de benefícios financeiros ilegalmente, sendo que, crimes relativos a critpoativos são cibercrime pelo uso da *blockchain* como tecnologia de base. Embora o mercado das criptomoedas esteja a ficar cada vez maior, o seu fluxo de dinheiro ilegal está a diminuir, isto é possível devido a políticas criminais e sociais.

Estas políticas baseiam-se na tentativa de cultivar a sociedade no que realmente é a *Blockchain* e as criptomoedas, o seu verdadeiro valor e como podem ser uma mais-valia para todos os setores da sociedade moderna, conseguimos entender que esta tecnologia não apenas facilita o crime, mas é utilizada para tal. A *bitcoin* passa a ser então uma das formas de fazer a compra e venda de bens ilícitos desde a sua criação, isto porque o seu sistema não é controlado por qualquer organização governamental,

no entanto, com a evolução destas tecnologias a investigação criminal também teve de se aprimorar criando assim, ferramentas de auditoria da *blockchain*.

Estas ferramentas provam ser umas das principais formas de análise da blockchain, e a sua adoção e aprimoramento vão mostrar-se centrais na Investigação Criminal. Durante esta investigação foram analisadas várias destas ferramentas, sendo que a considerada mais adequada foi a Graphsense.

Esta ferramenta foca-se na auditoria de *blockchain* conseguindo analisar transações entre BTC, LTC, BCH e ETH. É importante referir que este *software* é utilizado por instituições de segurança supranacionais como a Europol para a realização de investigações como a desta dissertação.

Curiosamente, a carteira que foi aleatoriamente investigada levou-nos a uma corretora que durante esta dissertação foi alvo de uma investigação conjunta por parte das autoridades de sete países diferentes, incluindo Portugal com o auxílio da Europol e consequentemente encerrada. Esta decisão foi tomada pelas suspeitas da facilitarem a lavagem de dinheiro, sendo que, mais de 2,1 biliões de dólares foram transacionados pela corretora durante a sua atividade.

Durante o nosso estudo de caso foi nos possível fazer a auditoria de várias carteiras levando-nos a uma carteira que foi conectada a uma corretora fidedigna *Huobi.com*, ou seja, a probabilidade de ser identificada devido a melhores medidas de KYC é maior, dando assim a possibilidade provar o falso anonimato da *blockchain*.

No entanto, quando se lida com crimes no ciberespaço é importante entender que não estão apenas reduzidos a uma jurisdição e por isso é necessário trabalho conjunto de organizações de segurança e mais importantes organizações supranacionais como a Europol e Interpol para que sejam feitas as ligações e partilhas de informações necessárias como foi observado na investigação à corretora *Bitzlato.com*.

O *modus operandi* do criminoso neste crime envolve abusar das características da internet, um espaço sem fronteiras e dessa forma várias jurisdições, para batalhar esta

problemática é necessário estabelecer parcerias para aumentar o conhecimento e eficácia no combate nacional e internacional de cibercrimes como a FATF e WGDC

O investimento nacional no desenvolvimento de ferramentas de auditoria da *blockchain* também é essencial, foi possível entender que todos os softwares que foram introduzidos nesta dissertação eram privados, ou seja, se os OPC os quiserem utilizar é necessária a compra de licenças que podem ser muito caras. Dessa foram, é necessário a criação de projetos de investigação que criem ferramentas destas para os nossos OPC.

Globalmente é necessário que a investigação criminal se foque na prevenção, detenção e políticas de resposta para a problemática da *blockchain* e das criptomoedas, entendemos que esta vertente do cibercrime veio para ficar e é importante que haja foco no seu combate.

As limitações sentidas nesta investigação centram-se na capacidade de prosseguir com o estudo de caso, ou seja, o trabalho do investigador em relação á procura da prova está feito, agora é necessário que haja contacto entre a corretora e o investigador para que possa ser realizada a identificação da carteira digital, só depois dessa diligência é que o estudo estaria concluído.

Podemos descrever que existem também ferramentas de auditoria com melhores capacidades de rastreio de carteiras digitais às quais não temos acesso, sendo que, os principais métodos utilizados pelos OPC nacionais como internacionais nem sempre são públicos, posto isso, esta falta de informação é uma limitação, no entanto, com o exemplo dado e conceptualizado os conceitos necessários percebemos que a *blockchain* não é verdadeiramente anónima.

Originando a quarta revolução industrial a blockchain vai continuar a ser utilizada pelo agente do crime, sendo que, a partir de agora também contra ele.

Referências

A. Balaskas and V. N. L. Franqueira, "Analytical Tools for *Blockchain*: Review, Taxonomy and Open Challenges," *2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)* 10.1109/CyberSecPODS.2018.8560672.

A. Biryukov and S. Tikhomirov, "Deanonymization and Linkability of Cryptocurrency Transactions Based on Network Analysis," *2019 IEEE European Symposium on Security and Privacy (EuroS&P)*, Stockholm, Sweden, 2019, pp. 172-184,

Abdulhakeem, S. and Hu, Q. (2021) Powered by *Blockchain* Technology, DeFi (Decentralized Finance) Strives to Increase Financial Inclusion of the Unbanked by Reshaping the World Financial System. *Modern Economy*, **12**, 1-16. doi:

Alekseenko, Aleksandr P.2023. Model Framework for Consumer Protection and Crypto-Exchanges Regulation.Journal of Risk and Financial Management 16: 305.

Andriole, S. J. (2020). *Blockchain*, Cryptocurrency, and Cybersecurity. IT Professional, IT Prof., 22(1)

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

Bilali, Genci. Know your costumer – or not. University of Toledo Law Review 319, 2012.

Bitzlato: senior management arrested | Europol.” *Europol*, 23 January 2023,

Braz, J. (2013). Investigação Criminal - A organização, o método e a prova: Os Desafios da Nova Criminalidade (3. Ed. ed.). Almedina.

Braz, J. (2013). Investigação Criminal - A organização, o método e a prova: Os Desafios da Nova Criminalidade (3. Ed. ed.). Almedina.

Chainalysis (2021), The 2021 Crypto Crime report.

Chainalysis team. (2022, January 19). Meet the Malware Families Helping Hackers Steal and Mine Millions in Cryptocurrency [Blog post]. https://blog.*Chainalysis*.com/reports/2022-crypto-crime-report-preview-malware/

Chainalysis. (2020a). Cryptocurrency Typologies: Our Guide to Who's Who on the *Blockchain*. https://go.*Chainalysis*.com/2020-typologiesreport.html

Chainalysis. (2020b). The 2020 State of crypto crime. Everything you need to know about darknet markets, exchange hacks, money laundering and more.

Chainalysis. (2022). The 2022 Crypto Crime Report. Original data and research into cryptocurrency-based crime.

Chen, J. (n.d.). *Know Your Client (KYC): What It Means, Compliance Requirements*. Investopedia.

Decentralized Finance (DeFi) - What impact will it have on cryptoasset forensics?", 5th INTERPOL Working Group on Dark Web and Virtual Assets, September 2022, Online.

Di Francesco Maesa, D., & Mori, P. (2020). *Blockchain* 3.0 applications survey. Journal of Parallel and Distributed Computing, 138(0), 99–114. https://doi.org/10.1016/j.jpdc.2019.12.019

Eduardo C., Pires C., Artioli M., Oliveira G. (2021). Cryptocurrencies: technology, initiatives of banks and central banks, and regulatory challenges, 30 (2). https://doi.org/10.1590/1982-3533.2021v30n2art08

European Central Bank (2022). Euro Digital. https://www.ecb.europa.eu/paym/digital_euro/html/index.pt.html

Europol (2023), Internet Organised Crime Threat Assessment (IOCTA) 2023, Publications Office of the European Union,

Europol. (2022). Cryptocurrencies: Tracing the Evolution of Criminal Finances. Europol Spotlight Report series,

Europol. (2023b). The Other Side of the Coin - Analysis of Financial and Economic Crime,

FATF (2012-2023), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, www.fatf-gafi.org/recommendations.html

FBI (2014). Manhattan U.S. Attorney Announces the Indictment of Ross Ulbricht, the Creator and Owner of the Silk Road Website. Federal Bureau of Investigation. [online] https://www.justice.gov/usao-sdny/pr/manhattan-us-attorneyannounces-indictment-ross-ulbricht-creator-and-owner-silk-road [Acesso: 09/09/19]

Ferreira, Fábia Duarte. A prática do compliance como um instrumento empresarial anticorrupção para preservação das empresas. Revista de Direito Bancário e do Mercado de Capitais, vol. 81/2018, p. 161 – 178, jul./sep. 2018.

Glaser, F., & Bezzenberger, L. (2015). Beyond Cryptocurrencies—A Taxonomy of Decentralized Consensus Systems. In 23rd European Conference on Information Systems. Atlanta, GA: Association for Information Systems.

GraphSense. (2021, November 30). *Graphsense*: February 1, 2022 https://graphsense.info/

Greeshma, K. V. (2015), Crypto Currencies and Cybercrime, International Journal of Engineering and TechnicalResearch, https://www.ijert.org/research/crypto-currencies

Haber, S., & Stornetta, W. S. (1990). How to time-stamp a digital document. In Conference on the Theory and Application of Cryptography. Springer.

Ilbiz, E.; Kaunert, C. Sharing Economy for Tackling Crypto-Laundering: The Europol Associated ‘Global Conference on Criminal Finances and Cryptocurrencies’. Sustainability 2022, 14, 6618. https://doi.org/10.3390/ su14116618

Interpol. (2020) Combatting Cyber-enabled Financial Crimes in the era of Virtual Asset and Darknet Service Providers

L. Pawczuk, J. Holdowsky, R. Massey (2019, May 06) Deloitte's 2019 *Blockchain* Survey. Retrieved from https://www2.deloitte.com/ie/en/pages/technology/articles/Global_*Blockchain*_sur vey.html

Lakshete, B. (2022). *Recent trends in Humanities, Commerce and Management* (1st ed., Vol. Crypto Currency: A Secured and Safety way of dealing Business Transactions).

Mataković, Ivana. (2022). Crypto-Assets Illicit Activities: Theoretical Approach with Empirical Review. 17.

Nakamoto, S. (2008) *Bitcoin*: A peer-to-peer electronic cash system [White paper] https://*bitcoin*.org/*bitcoin*.pdf

Natarajan, H., Krause, S., & Gradstein, H. (2017). Distributed Ledger Technology and *Blockchain*. In FinTech note (Issue 1). World Bank Group. https://doi.org/10.1596/29053

Patil, Y. (2021, June 9). DarkSide Ransomware [Blog post].

Paz, Javier. 2022. The Best Global Crypto Exchanges. Forbes. March 16.

Poongodi, M., Sharma, A., Vijayakumar, V., Bhardwaj, V., Sharma, A. P., Iqbal, R., & Kumar, R. (2020). Prediction of the price of Ethereum *blockchain* cryptocurrency in an industrial finance system. COMPUTERS & ELECTRICAL ENGINEERING, 81.

Prybila, C., Schulte, S., Hochreiner, C., & Weber, I. (2020). Runtime verification for business processes utilizing the *Bitcoin blockchain*. Future Generation Computer Systems, 107, 816-831.

S. Foley, J. Karlsen and T. Putnis (2019), Sex, Drugs, and *Bitcoin*: How much illegal activity is financed through cryptocurrencies?

Schwab, K. (2016). The Fourth Industrial Revolution, World Economic Forum.

Securities and Exchange Commission. (2013). Ponzi Schemes Using Virtual Currencies.

T. Zhang, "Privacy Evaluation of *Blockchain* Based Privacy Cryptocurrencies: A Comparative Analysis of Dash, Monero, Verge, Zcash and Grin," in *IEEE Transactions on Sustainable Computing*, 10.1109/TSUSC.2023.3303180.

Tapscott, D., & Tapscott, A. (2016). The Impact of the *Blockchain* Goes Beyond Financial Services. Harvard Business Review, 7.

Teixeira, João Pedro da Cunha. (2022). *Branqueamento e criptomoedas: uma análise das novas entidades obrigadas do sistema preventivo* [Tese de Mestrado, Universidade Católica Portuguesa].

Wainright, R. The 'Uberisation' of International Police Work. 2016

Wang, Lei & Cheng, Hao & Zheng, Zibin & Yang, Aijun & Xu, Ming. (2023). Temporal Transaction Information-aware Ponzi Scheme Detection for Ethereum Smart Contracts. Engineering Applications of Artificial Intelligence. 126. 107022. 10.1016/j.engappai.2023.107022.

Y. Wu, A. Luo and D. Xu, "Forensic Analysis of *Bitcoin* Transactions," 2019 IEEE International Conference on Intelligence and Security Informatics (ISI), 2019, pp. 167-169, 10.1109/ISI.2019.8823498.

Zhao, K.; Dong, G.; Bian, D. Detection of Illegal Transactions of Cryptocurrency Based on Mutual Information. Electronics 2023, 12,1542. https://doi.org/10.3390/ electronics12071542-

Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). *Blockchain* challenges and opportunities: a survey. International Journal of Web and Grid Services, 14(4), 352–375.

Legislação:

Constituição da República Portuguesa;

Código Penal;

Código de Processo Penal;

Lei de Segurança Interna.

Lei da Organização da Investigação Criminal

Modelo da lombada

(dissertação de mestrado)

O “ falso “ anonimato da blockchain
Gonçalo Alexandre da Piedade de Oliveira
2023