

**UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL  
FACULDADE DE CIÊNCIAS ECONÔMICAS  
DEPARTAMENTO DE ECONOMIA E RELAÇÕES INTERNACIONAIS**

**JEFERSON LEMOS JUNIOR**

**ANÁLISE DA RELAÇÃO ENTRE A UTILIZAÇÃO DE CRIPTOMOEDAS E O  
CRIME DE LAVAGEM DE DINHEIRO**

**Porto Alegre**

**2023**

**JEFERSON LEMOS JUNIOR**

**ANÁLISE DA RELAÇÃO ENTRE A UTILIZAÇÃO DE CRIPTOMOEDAS E O  
CRIME DE LAVAGEM DE DINHEIRO**

Trabalho de conclusão submetido ao Curso de Graduação em Ciências Econômicas da Faculdade de Ciências Econômicas da UFRGS, como requisito parcial para obtenção do título Bacharel em Economia.

Orientador: Prof. Dr. Maurício Andrade  
Weiss

**Porto Alegre**

**2023**

### CIP - Catalogação na Publicação

Lemos Junior, Jeferson  
ANÁLISE DA RELAÇÃO ENTRE A UTILIZAÇÃO DE  
CRIPTOMOEDAS E O CRIME DE LAVAGEM DE DINHEIRO /  
Jeferson Lemos Junior. -- 2023.  
68 f.  
Orientador: Mauricio Andrade Weiss.

Trabalho de conclusão de curso (Graduação) --  
Universidade Federal do Rio Grande do Sul, Faculdade  
de Ciências Econômicas, Curso de Ciências Econômicas,  
Porto Alegre, BR-RS, 2023.

1. Moeda. 2. Criptomoedas. 3. Bitcoin. 4. Lavagem  
de Dinheiro. I. Andrade Weiss, Mauricio, orient. II.  
Título.

**JEFERSON LEMOS JUNIOR**

**ANÁLISE DA RELAÇÃO ENTRE A UTILIZAÇÃO DE CRIPTOMOEDAS E O  
CRIME DE LAVAGEM DE DINHEIRO**

Trabalho de conclusão submetido ao Curso de Graduação em Ciências Econômicas da Faculdade de Ciências Econômicas da UFRGS, como requisito parcial para obtenção do título Bacharel em Economia.

Aprovada em: Porto Alegre, 5 de setembro de 2023.

**BANCA EXAMINADORA:**

---

Prof. Dr. Maurício Andrade Weiss – Orientador  
UFRGS

---

Prof. Dr. Carlos Eduardo Schonerwald da Silva  
UFRGS

---

Prof. Dr. Marcelo Milan  
UFRGS

## AGRADECIMENTOS

Gostaria de agradecer a todos que contribuíram para a realização deste trabalho de conclusão. Em primeiro lugar, expresso minha gratidão ao meu orientador Dr. Maurício Andrade Weiss, pela orientação, paciência e *insights* fornecidos ao longo deste processo. Seu apoio foi fundamental para o desenvolvimento deste trabalho.

Também gostaria de agradecer aos meus amigos e familiares que me apoiaram durante toda essa jornada acadêmica, pelo incentivo, encorajamento e compreensão nos momentos de dedicação e estudo intenso.

Finalmente, sou grato à Universidade, por oferecer a estrutura e recursos necessários para a realização deste trabalho e aos professores que tive contato durante o curso, que contribuíram com suas teorias e conhecimentos, fundamentais para embasar e enriquecer este trabalho.

Este projeto não teria sido concluído sem o apoio, incentivo e colaboração de todos mencionados acima.

Muito obrigado!

*“It takes 20 years to build a reputation and five minutes to ruin it. If you think about that, you’ll do things differently.”*

*(Warren Buffett)*

## RESUMO

Este trabalho propõe-se a avaliar as formas de utilização das denominadas criptomoedas no cometimento do crime de lavagem de dinheiro, originário de outras condutas criminosas. A metodologia adotada inclui uma revisão de pesquisa bibliográfica, análise de casos práticos e estudo das regulamentações vigentes. Dados fornecidos pela empresa Chainalysis também foram empregados para enriquecer o estudo. O intuito secundário do trabalho é explorar as características dos diversos tipos de moedas existentes ao longo da história, apresentando as suas semelhanças, diferenças e conceitos. Ainda, foi analisada a capacidade de evolução da moeda, suas variadas formas, surgimento e necessidades, destacando a ascensão das criptomoedas, mais especificamente, do Bitcoin. O trabalho observa como resultado não somente a ampla gama de oportunidades que as criptomoedas proporcionam nos cenários financeiro e tecnológico, mas também identifica uma tendência preocupante: a incidência de lavagem de dinheiro com criptomoedas. Embora em menor proporção quando comparada a outros métodos tradicionais, a sua utilização para esse propósito é uma realidade. Portanto, regulamentações são necessárias para combater as atividades dessa natureza.

**Palavras-chave:** Moeda. Criptomoedas. Bitcoin. Lavagem de Dinheiro.

## **ABSTRACT**

This work proposes to evaluate the ways of criminals using the so-called cryptocurrencies in the commitment of the crime of money laundering, originating from other criminal conducts. The methodology adopted includes a review through bibliographical research, analysis of practical cases and study of current regulations. Data provided by the company Chainalysis were also used to enrich the study. The secondary purpose of the work is to explore the characteristics of the different types of currencies existing throughout history, presenting their similarities, differences and concepts. Also, the currency's ability to evolve was analyzed, its various forms, emergence and needs, highlighting the rise of cryptocurrencies and, more specifically, Bitcoin. As a result, the work observes not only the wide range of opportunities that cryptocurrencies provide in the financial and technological dimensions, but also identifies a worrying trend: the incidence of money laundering with cryptocurrencies. Although to a lesser extent when compared to other traditional methods, its use for this purpose is a reality. Therefore, regulations are needed to combat activities of this nature.

**Keywords:** Currency. Cryptocurrencies. Bitcoin. Money laundry.

## LISTA DE FIGURAS

Figura 1 – Moeda de ouro do antigo reino da Lídia.....	20
Figura 2 – Florim holandês, a 1ª moeda cunhada no Brasil.....	21
Figura 3 – Real Português cunhado no Brasil.....	22
Figura 4 – Relatórios de Inteligência Financeira produzidos pelo COAF .....	45
Figura 5 – Ciclo da Lavagem de Dinheiro .....	46
Figura 6 – Total de criptomoedas utilizadas para lavagem de dinheiro, por ano.....	48
Figura 7 – Destino dos fundos que saem das carteiras ilícitas, por ano .....	49
Figura 8 – Destino dos fundos que saem das carteiras ilícitas, por atividades ilegais .....	50
Figura 9 – Criptomoedas recebidas pelos misturadores, por origem .....	52
Figura 10 – Fontes de criptomoedas ilícitas enviadas para misturadores, em 2022 .....	52
Figura 11 – Número de serviços de saídas para moeda fiduciária recebendo fundos ilícitos vs. Participação em fundos ilícitos recebidos pelas cinco principais <i>exchanges</i> .....	53
Figura 12 – Valor de criptomoeda ilícita recebida pelos endereços de depósito de serviços de saída para moeda fiduciária, por montante .....	54
Figura 13 – Participação ilícita no volume total de transações de criptomoedas, por ano .....	55

## LISTA DE ABREVIATURAS E SIGLAS

BCB	Banco Central do Brasil
CBECI	<i>Cambridge Bitcoin Electricity Consumption Index</i>
CEO	<i>Chief Executive Officer</i>
COAF	Conselho de Controle de Atividades Financeiras
CVM	Comissão de Valores Mobiliários
DEFI	<i>Decentralized Finance</i>
DLT	<i>Distributed Ledger Technology</i>
EUA	Estados Unidos da América
GAFI	Grupo de Ação Financeira
IN	Instrução Normativa
IPHAN	Instituto do Patrimônio Histórico e Artístico Nacional
OFAC	<i>Office of Foreign Assets Control</i>
ONU	Organização das Nações Unidas
P2P	<i>Peer-to-Peer</i>
RFB	Receita Federal do Brasil
RIF	Relatório de Inteligência Financeira
RPOW	<i>Reusable Proofs-of-Work</i>
SCIELO	<i>Scientific Electronic Library Online</i>
TWh	Terawatt-hora
UNODC	<i>United Nations Office on Drugs and Crime</i>

## SUMÁRIO

<b>1</b>	<b>INTRODUÇÃO</b> .....	<b>10</b>
<b>2</b>	<b>A MOEDA</b> .....	<b>13</b>
2.1	CONCEITOS, FUNÇÕES E CARACTERÍSTICAS DA MOEDA.....	13
<b>2.1.1</b>	<b>A visão de Keynes</b> .....	<b>15</b>
2.2	ORIGEM DA MOEDA.....	17
2.3	EVOLUÇÃO HISTÓRICA DA MOEDA.....	22
<b>2.3.1</b>	<b>Moeda-Mercadoria</b> .....	<b>23</b>
<b>2.3.2</b>	<b>Moeda Metálica</b> .....	<b>25</b>
<b>2.3.3</b>	<b>Moeda-Papel</b> .....	<b>25</b>
<b>2.3.4</b>	<b>Papel-Moeda</b> .....	<b>26</b>
<b>2.3.5</b>	<b>Moeda Bancária</b> .....	<b>27</b>
2.4	CONSIDERAÇÕES FINAIS DO CAPÍTULO.....	28
<b>3</b>	<b>CRIPTOMOEDAS</b> .....	<b>29</b>
3.1	SURGIMENTO DAS CRIPTOMOEDAS.....	29
3.2	PRIMEIRAS CRIPTOMOEDAS.....	31
3.3	SURGIMENTO DO BITCOIN.....	34
<b>3.3.1</b>	<b>Características do Bitcoin</b> .....	<b>36</b>
<b>3.3.2</b>	<b>Funcionamento e Estruturação do Bitcoin</b> .....	<b>37</b>
3.4	CONSIDERAÇÕES FINAIS DO CAPÍTULO.....	41
<b>4</b>	<b>LAVAGEM DE DINHEIRO</b> .....	<b>42</b>
4.1	ORIGEM E HISTÓRIA DA LAVAGEM DE DINHEIRO.....	42
4.2	CONCEITO DE LAVAGEM DE DINHEIRO.....	43
4.3	FASES DA LAVAGEM DE DINHEIRO.....	45
4.4	CONSIDERAÇÕES FINAIS DO CAPÍTULO.....	46
<b>5</b>	<b>ANÁLISE DA RELAÇÃO ENTRE A UTILIZAÇÃO DE CRIPTOMOEDAS E O CRIME DE LAVAGEM DE DINHEIRO</b> .....	<b>47</b>
5.1	CRIPTOMOEDAS COMO INSTRUMENTO NA LAVAGEM DE DINHEIRO.....	47
5.2	REGULAMENTAÇÃO DAS CRIPTOMOEDAS.....	56
5.3	CONSIDERAÇÕES FINAIS DO CAPÍTULO.....	59
<b>6</b>	<b>CONCLUSÃO</b> .....	<b>60</b>
	<b>REFERÊNCIAS</b> .....	<b>62</b>

## 1 INTRODUÇÃO

Desde a antiguidade, diversos tipos de bens já foram escolhidos pela sociedade para desempenhar o papel de dinheiro na economia. Com o aprimoramento das atividades comerciais e das trocas, as formas de dinheiro foram passando por um processo evolutivo significativo.

Mais recentemente, surgiram as criptomoedas. Dentre elas, o Bitcoin se destacou como pioneiro e líder. Lançado em 2008 por um indivíduo ou grupo sob o pseudônimo Satoshi Nakamoto, o Bitcoin introduziu uma rede descentralizada, baseada na criptografia e na tecnologia *blockchain*, pelas quais as transações eletrônicas seriam feitas de maneira segura, rápida e sem a necessidade de uma entidade central por trás (SICHEL; CALIXTO, 2018). Ademais, sua natureza pseudônima, oferta limitada e capacidade de realizar transações de forma direta e global, sem a necessidade de intermediários, conferiram-lhe notável reconhecimento e valorização.

Porém, a valorização do Bitcoin ao longo dos anos não se deu de forma contínua e desprovida de desafios. No início de 2013, o seu preço saiu de cerca de US\$ 13,00 para alcançar US\$ 19.000,00 no final de 2017 – ou seja, uma valorização superior a 146.000% no período. Passado 1 ano, em dezembro de 2018, o seu preço já havia recuado mais de 80%, para US\$ 4.000,00. Em 2021, o Bitcoin atingiu sua máxima histórica, próximo dos US\$ 68.000,00. Mas, em 2022, encerrou o ano próximo dos US\$ 16.000,00 (BITCOIN USD...,2023).

Assim, embora tenha testemunhado um crescimento notável, é inegável que essa trajetória ascendente foi acompanhada por considerável volatilidade e instabilidade. Essa volatilidade, apesar de ter proporcionado oportunidades de lucro especulativo para alguns, também gerou incertezas significativas, dificultando o Bitcoin e as criptomoedas de desempenhar efetivamente as funções de unidade de conta e reserva de valor.

Outro desafio que apareceu com o crescimento das criptomoedas foi a questão da lavagem de dinheiro. Devido à capacidade de realizar transações de forma relativamente anônima, o Bitcoin tem sido utilizado para atividades ilícitas. A falta de regulamentação uniforme em nível global e a dificuldade em rastrear transações em uma rede descentralizada tornaram-se preocupações em relação ao

uso indevido da criptomoeda para ocultar a origem de fundos provenientes de atividades ilegais.

Assim, a questão principal que o trabalho busca responder é: as criptomoedas estão relacionadas com o crime de lavagem de dinheiro? A justificativa para esse estudo ocorre em razão desses ativos terem crescido bastante em popularidade nos últimos anos e por conta de possuírem características e tecnologias próprias, diferenciando-se das moedas tradicionais.

O objetivo geral consiste em avaliar as formas de utilização das criptomoedas no cometimento do crime de lavagem de dinheiro a fim de verificar se esses ativos estão sendo empregados como ferramentas para a prática de crimes virtuais. Os objetivos específicos incluem: analisar os conceitos, funções e características da moeda, investigar as características técnicas das criptomoedas que podem facilitar ou dificultar a lavagem de dinheiro, avaliar as regulamentações e medidas de combate à lavagem de dinheiro, propor diretrizes ou recomendações para aprimorar a regulamentação e os mecanismos de prevenção à lavagem de dinheiro no contexto das criptomoedas e contribuir para a compreensão mais ampla dos riscos e benefícios das criptomoedas, fornecendo informações relevantes para formuladores de políticas, profissionais de segurança financeira e público em geral.

A hipótese principal é de as criptomoedas estão relacionadas com o crime de lavagem de dinheiro, muito em função de algumas características suas. A hipótese secundária é de que o caráter descentralizado e pseudônimo das criptomoedas faz delas um instrumento propício para que criminosos possam praticar crimes, já que os endereços são uma combinação alfanumérica e as transações não são validadas por nenhuma autoridade central.

A metodologia adotada inclui uma revisão abrangente por meio de pesquisa bibliográfica, análise de base de dados relevantes ao tema e estudo das regulamentações vigentes. Em relação ao material bibliográfico, foram analisados artigos acadêmicos, teses e dissertações. Esses materiais foram coletados de fontes diferentes, tais como: *Scientific Electronic Library Online (SciELO)* e Biblioteca Digital Brasileira de Teses e Dissertações. Uma vez reunidos, esses textos foram analisados e resumidos, de modo a organizar suas principais informações e uma pesquisa descritiva.

O trabalho divide-se em quatro capítulos após a introdução. No primeiro, busca-se revisar os conceitos e características da moeda, com destaque para a

visão de Keynes, além de lembrar o surgimento e os tipos de moeda ao longo da história. Em seguida, aborda-se sobre as criptomoedas, explorando sua história e propriedades, mas com maior ênfase no estudo do Bitcoin e seu funcionamento.

O terceiro capítulo destaca a origem, história e conceitos da lavagem de dinheiro. O propósito dele, assim como dos anteriores, é trazer uma base teórica que permita avaliar a relação entre as criptomoedas e o crime de lavagem de dinheiro – sendo a análise dessa relação o tema do quarto capítulo. Nesse último, são apresentados dados da Chainalysis, empresa de análise de *blockchain*, a fim de verificar os objetivos e hipóteses.

## 2 A MOEDA

A moeda desempenha um papel crucial nas atividades comerciais e financeiras da sociedade. Ao explorar os seus conceitos fundamentais e abordar as suas características e funções, dentro do contexto econômico, é possível compreender a sua origem e analisar como esse importante instrumento monetário tem evoluído ao longo da história e como suas diversas formas têm moldado o funcionamento dos sistemas econômicos em diferentes períodos.

Com o objetivo de entender as criptomoedas e contextualizar seu papel na história monetária, este capítulo tem como propósito revisar os conceitos, funções e características da moeda, com destaque para a literatura keynesiana, além de relembrar a sua origem e trajetória.

### 2.1 CONCEITOS, FUNÇÕES E CARACTERÍSTICAS DA MOEDA

De acordo com Galbraith (1983), moeda é aquilo que é comumente oferecido ou recebido pela compra ou venda de bens, serviços ou quaisquer outras coisas. O autor considera o significado descomplicado mesmo, pois qualquer tentativa de complicar o assunto seria uma maneira de disfarçar a simplicidade sobre ele.

Polanyi (2012) aponta que a moeda é somente um outro nome para uma mercadoria empregada na troca com maior frequência que qualquer outra, e que é, assim, obtida principalmente com o objetivo de facilitar o intercâmbio.

Hillbrecht (1999) complementa que a concepção de moeda para os economistas é aquilo que geralmente é aceito como meio de pagamento por bens e serviços e como pagamento ou liquidação de dívidas, além de também ser conhecida como meio de troca.

Ainda, como a moeda representa um poder de aquisição, desde o momento em que é recebida até o momento em que é dada em pagamento de outra transação, ela também se caracteriza como uma reserva de valor. (LOPES; ROSSETTI, 2005).

Essas visões estão muito associadas à moeda mercadoria. Levando isso em consideração, é possível destacar três principais funções da moeda:

- a) intermediária de trocas;
- b) unidade de conta;

- c) reserva de valor. (FROYEN, 2013; HILLBRECHT, 1999; LOPES; ROSSETTI, 2005).

De acordo com Hillbrecht (1999), a primeira função diz respeito à moeda ser um meio de pagamento normalmente aceito para liquidar transações de bens e serviços. Para Lopes e Rossetti (2005), essa é a função essencial da moeda, pois permitiu a superação da economia de escambo e a passagem à economia monetária. A função de unidade de conta, ou medida de valor, possibilita a mensuração de valor por meio do uso da moeda, trazendo um denominador comum na precificação de bens e serviços de uma economia. Segundo Lopes e Rossetti (2005), a utilização generalizada da moeda implica a criação de uma unidade-padrão de medida, à qual são convertidos os valores de todos os bens e serviços disponíveis.

A terceira função, de reserva de valor, permite que se possa poupar poder de compra da renda recebida no presente para efetuar gastos no futuro, ou seja, permite que se possa transferir consumo e gastos para o futuro. (HILLBRECHT, 1999). Sendo assim, a moeda pode funcionar como um estoque de riqueza, um modo de economizar e poupar para gastos futuros, funcionando como um ativo financeiro (FROYEN, 2013).

Segundo Lopes e Rossetti (2005), para cumprir tais funções, a moeda deve reunir as seguintes características:

- a) indestrutibilidade e inalterabilidade;
- b) homogeneidade;
- c) divisibilidade;
- d) transferibilidade;
- e) facilidade de manuseio e transporte.

De acordo com a primeira característica, a moeda precisa ser bastante resistente, de modo que não se desgaste ou se danifique, enquanto os agentes econômicos a utilizam para facilitar transações. A característica da homogeneidade está relacionada à padronização, em que duas unidades monetárias distintas, mas de igual valor, devem ser idênticas. A terceira característica, da divisibilidade, é necessária pois a moeda deve poder ser fracionada em múltiplos e submúltiplos, para que qualquer tipo de transação, de pequeno ou grande porte, possa ser realizada sem dificuldades (LOPES; ROSSETTI, 2005).

A transferibilidade é a característica que prevê a eficiência e a facilidade na transferência monetária de um detentor para outro. Por fim, a quinta característica da moeda, a facilidade de manuseio e transporte, informa que o manuseio e transporte da moeda não pode ser prejudicado na sua utilização, pois, no caso de ser dificultado, sua utilização será gradativamente descartada (LOPES; ROSSETTI, 2005).

Assim, quando uma moeda possui essas características físicas essenciais, pode-se dizer que ela está habilitada a desempenhar suas três funções monetárias de meio de troca, unidade de conta e reserva de valor (CARVALHO *et al.*, 2000).

### **2.1.1 A visão de Keynes**

Segundo Silva (1987), Keynes elabora uma taxonomia da moeda buscando ressaltar uma característica que se torna teoricamente fundamental para ele: a moeda enquanto unidade de conta, ou seja, que se pode apresentar uma lista de preços para compra e venda imediata expressos em moeda e também representa que a moeda serve como instrumento de reconhecimento de crédito e débito, isto é, possibilita o estabelecimento de contratos de compra e venda com pagamentos diferidos.

A existência desses contratos exige a presença de algum elemento que possa representar a continuidade do passado no futuro e que ligue esses dois momentos, de forma que os agentes possam reduzir as fronteiras da incerteza. Esse elemento é exatamente a moeda em sua função de unidade de conta (AMADO, 2000).

Para Keynes (1971), todas as outras funções da moeda derivam dessa função originária:

A Moeda, especialmente por ser o elemento em que os contratos e contratos de preços são cancelados, e na forma em que o estoque de poder de compra geral é mantido, deriva seu caráter de sua relação com a unidade de conta, uma vez que os débitos e preços têm que ser primeiro denominados na forma deste último. (KEYNES, 1971, p. 3).

Ao contrário da doutrina neoclássica, que concebe a moeda apenas como intermediário de trocas, para Keynes ela é um ativo e, assim, possui valor e, ao mesmo tempo liquidez absoluta, o que a faz uma alternativa de preservação de riqueza ao longo do tempo (DORNELAS; TERRA, 2021).

Para Keynes (1936), a moeda desempenhava diversos papéis essenciais na economia. Ele argumentava que a moeda era uma ponte entre o presente e o futuro, permitindo que os indivíduos e as empresas armazenassem poder de compra para uso posterior.

Segundo Dornelas e Terra (2021), as ideias de Keynes defendem que a economia é banhada pela incerteza decorrente, de um lado, da descentralização das decisões e, do outro, do futuro desconhecido. Nestas circunstâncias, a moeda, enquanto o ativo mais líquido, passa a ter importância fundamental como garantia contra esta incerteza.

Assim, a preferência pela liquidez pode crescer o suficiente para inibir a decisão de investimento. A incerteza que banha a economia afeta o investimento de duas maneiras: por um lado, por meio da determinação da taxa de juros; por outro, afetando a eficiência marginal do capital (DORNELAS; TERRA, 2021).

Em seu livro, Keynes (2005/1936) desenvolveu uma teoria sobre a demanda por moeda enfatizando a importância das taxas de juros. Essa teoria, que ficou conhecida como a Teoria da Preferência pela Liquidez, rompeu com a teoria clássica ao considerar que a demanda por moeda é afetada pelas expectativas sobre o comportamento da taxa de juros, enquanto o nível de emprego e outras variáveis do setor real da economia experimentam a influência de variações situadas no setor monetário.

Segundo Lopes e Rossetti (2005), Keynes incorporou na sua versão da demanda de moeda a incerteza acerca das variações futuras na taxa de juros. Para Keynes (1936) há três motivos por trás da demanda por moeda:

- a) motivo de transação;
- b) motivo de precaução;
- c) motivo de especulação.

O primeiro motivo pode ser subdividido em dois segmentos: motivo de renda e motivo de negócios. Quanto à renda, diz respeito à necessidade de manter moeda para efetuar pagamentos correntes de bens e serviços no dia a dia. Já, quanto à negócios, trata-se da conservação de recursos líquidos para assegurar o intervalo entre o momento em que começam as despesas com a produção e aquele em que se recebe o produto das vendas (KEYNES, 1936).

O motivo de precaução refere-se à preferência das pessoas por manter dinheiro como uma reserva para emergências ou situações imprevistas. Em tempos

de instabilidade econômica, os indivíduos tendem a aumentar a demanda por moeda como uma forma de segurança financeira, visto que ela é um ativo líquido e seguro para atravessar um futuro incerto e nebuloso (LOPES; ROSSETTI, 2005).

Diferente dos demais, o motivo de especulação é especificamente keynesiano. Ele faz referência à demanda por moeda como uma forma de manter poder de compra para aproveitar oportunidades futuras de investimento ou de obter benefícios financeiros. Conforme apontam Lopes e Rossetti (2005), sob uma expectativa generalizada de alta na taxa de juros ou de uma queda equivalente no preço dos títulos, no futuro, a retenção de saldos monetários para fins especulativos tende a se elevar; no caso contrário, a retenção de moeda devida a esse motivo tende a diminuir.

Portanto, a visão de Keynes destaca a importância fundamental da moeda na economia e seu papel no comportamento dos agentes econômicos. Sendo esta não apenas meio de troca e reserva de valor, mas também fator decisivo em períodos de incerteza econômica.

## 2.2 ORIGEM DA MOEDA

Esclarecido o conceito de moeda, suas funções e suas características, é mais fácil entender o motivo do seu surgimento. Hoje, é impossível imaginar uma economia desenvolvida com o comércio sendo realizado sem a utilização do dinheiro. Porém, nem sempre foi assim.

Segundo Fernandes (2018), o comércio teve início na antiguidade, quando as trocas eram feitas diretamente entre mercadorias ou serviços, sem a utilização de recurso monetário. Essa primeira etapa de troca era conhecida como escambo. Os primeiros agrupamentos humanos, em geral nômades, eram grupos que não conheciam a moeda e que precisavam ser autossuficientes e, portanto, recorriam a essa forma de troca para sobreviverem.

Com a fixação de grupos em determinadas áreas, o desenvolvimento da vida social e econômica e a evolução e complexidade do comércio, surgiu-se a moeda. Nesse contexto, ela emergiu como uma solução prática, atuando como um meio de facilitar as transações e superar as limitações do escambo. Sua aceitação generalizada proporcionou maior liquidez, permitindo que as pessoas acumulassem riqueza e estabelecessem relações comerciais mais complexas. A partir desse

momento, o conceito de moeda evoluiu continuamente, desempenhando um papel essencial na organização econômica e social das civilizações ao longo dos séculos.

Não existe um consenso a respeito do local e da data exata do surgimento da primeira forma de dinheiro. Para Harari (2016), por exemplo, a primeira forma de dinheiro conhecida na história foram os grãos de cevada sumérios e teriam surgido por volta de 3000 a.C. na Suméria. Outros autores, afirmam que, embora não se conheça o local e o momento histórico exato do seu surgimento, o dinheiro existe a pelo menos 4000 anos (MITCHELL; WRAY; WATTS, 2016).

Dalto *et al.* (2020), em linha com a Teoria Monetária Moderna, enxergam o dinheiro como uma unidade de conta criada pelo Estado. Segundo eles:

Cerca de cinco mil anos atrás, nos templos e palácios sumérios da Mesopotâmia, as autoridades públicas definiram as primeiras unidades de conta para contabilizar e calcular as obrigações (tributos) dos cidadãos para com as autoridades públicas. Desde então, essa é prerrogativa exercida por todos os estados modernos. Além de definir a unidade de conta na qual as dívidas a receber (tributos, taxas, contribuições e outras penalidades) são contabilizadas, o Estado emite a moeda (uma coisa, um instrumento físico ou virtual) que será aceita no pagamento dessas dívidas. (DALTO *et al.*, 2020, p. 20).

A Teoria Monetária Moderna define moeda como dívida. Portanto, o Estado determina o que é dinheiro ao escolher por qual meio receberá seus impostos. De acordo com Dalto *et al.* (2020):

[...] se a moeda de conta definida pelo Estado para pagar os tributos é uma unidade virtual ou tijolo (de barro ou de ouro) não é questão crucial. A imposição da dívida tributária pelo Governo criará uma demanda cativa pela moeda do Estado. Isto é, a necessidade de pagar tributos com uma determinada moeda estabelecida pelo Governo, fará as pessoas demandarem a moeda do Estado. (DALTO *et al.*, 2020, p. 44 e 45).

Dessa forma, “ao determinar esse padrão de conta de dívidas para consigo, o Estado garante que sua moeda, também emitida no mesmo padrão, será amplamente aceita por todos os membros da sociedade” (DALTO *et al.*, 2020).

A teoria cartalista, em contraposição à teoria ortodoxa – marcada pela visão de moeda como mercadoria – possui outra explicação para a origem da moeda. Conforme Carvalho (2017):

A explicação convencional sobre as origens da moeda foi desafiada pela escola heterodoxa, qual seja, a Teoria Cartalista da Moeda. De acordo com

esta abordagem, a essência da moeda não deve ser encontrada no seu papel como meio de trocas, mas sim na sua capacidade de medir o valor abstrato, tornando-se, assim, unidade de conta. Os cartalistas [...] discordam da visão metalista, pois entendem que as moedas não são originadas no setor privado, mas o resultado da ação dos Estados, que têm um papel central na determinação do valor da moeda. Diferentemente da visão metalista, eles propõem uma teoria não mercantil da moeda. (CARVALHO, 2017, p. 16).

Os cartalistas enfatizam a natureza política da moeda. Para eles, a moeda é, em sua essência, creditícia, e o Estado tem um papel fundamental na definição do instrumento que irá operar como moeda, assim como na delimitação do sistema monetário (GIROTTI, 2021).

De acordo com Knapp (1924), a moeda é uma criatura da lei e, portanto, uma teoria monetária deve lidar com a história jurídica. O material utilizado para a sua confecção não é o mais relevante, mas sim o ordenamento legal que regula o seu uso. Dessa maneira, a moeda metálica representa apenas uma das formas que os meios de pagamento assumiram ao longo da história.

Embora haja diferentes visões para o surgimento da moeda, sabe-se que a cunhagem de moedas metálicas, por exemplo, surgiu por volta de 800 a.C., na Lídia. Mas, tanto antes quanto depois do surgimento das moedas cunhadas em metal, muitas outras mercadorias, metálicas e não metálicas, foram usadas como moeda, até chegar na forma de dinheiro que se conhece hoje.

Entretanto, para deixar mais detalhado, o surgimento da moeda enquanto mercadoria, segundo Fernandes (2018), se deu nos primeiros humanos, em geral nômades, que viviam sob padrões bem simples de atividades econômicas. Estes grupos não conheceram a moeda e recorriam às atividades de trocas diretas em espécie, denominadas escambo.

Segundo Fernandes (2018), no escambo as trocas eram feitas por produto-produto ou serviço-serviço, de forma direta. Era um sistema aparentemente simples e eficiente, mas que apresentava inúmeras inconveniências, uma vez que o detentor de determinado produto deveria encontrar alguém que desejasse o mesmo e dispusesse de um produto que lhe interessasse.

Com o intuito de promover as trocas, Fernandes (2018) apontou que se fazia preciso encontrar algum bem que fosse aceito por todos de forma fácil. Nesse contexto, diversos objetos ou mercadorias foram utilizados como intermediários nas trocas, como tecido, arroz e conchas. Mas, foram os metais e, posteriormente a

moeda metálica, que se consagraram como o principal meio de troca das civilizações antigas.

Fernandes (2018) esclarece que:

Segundo historiadores, foi no quarto milênio a.C., quando se formaram as primeiras cidades na Mesopotâmia, que o homem passou a pensar em termos de objeto que ajudavam a traduzir valores. Antes disso, não havia concentração humana que justificasse essa ideia abstrata. Foi no Oriente Médio, lugar culturalmente mais rico da Antiguidade, que o dinheiro se difundiu, passando a existir como dinheiro de metal cerca de 2.500 a.C. A primeira grande revolução monetária ocorreu no século VII a.C., no reino da Lídia, onde hoje fica a Turquia. Lá foi inventada a moeda moderna, com todas as características básicas das atuais. Entre os anos 640 a.C. e 630 a.C., o homem chegou, finalmente, à cunhagem de moedas. (BRASIL, 2008, p. 6).

A Figura 1 ilustra a moeda de ouro cunhada no antigo reino da Lídia:

**Figura 1 – Moeda de ouro do antigo reino da Lídia**



Fonte: Fernandes (2018).

No Brasil, segundo Fernandes (2018), a primeira moeda a circular foi o Real Português, sendo popularmente substituído por Réis. Mas, devido à insuficiência de moedas nos dois primeiros séculos de colonização, séculos 16 e 17, o escambo foi muito usado em negociações entre nativos e europeus, com evidência para mercadorias como fumo, tecidos, açúcar e pau-brasil. Cabe destacar também a circulação das moedas espanholas, principalmente no período da União Ibérica.

Mesmo com o domínio português e espanhol na região, os primeiros a cunhar as moedas no Brasil foram os holandeses, nos anos de 1630 a 1654, durante o seu

domínio no nordeste brasileiro (FERNANDES, 2018). Estas moedas, conhecidas como Florins holandeses, tinham aparência quadradas e pequenas e eram feitas de ouro e prata. Elas surgiram em Pernambuco, em 1645, e foram direcionadas ao pagamento de fornecedores e de suas tropas. Segundo Fernandes (2018), elas tinham a marca da Companhia das Índias Ocidentais no anverso e, no reverso, a palavra Brasil.

A Figura 2 mostra o Florim holandês, sendo a primeira moeda cunhada no Brasil:

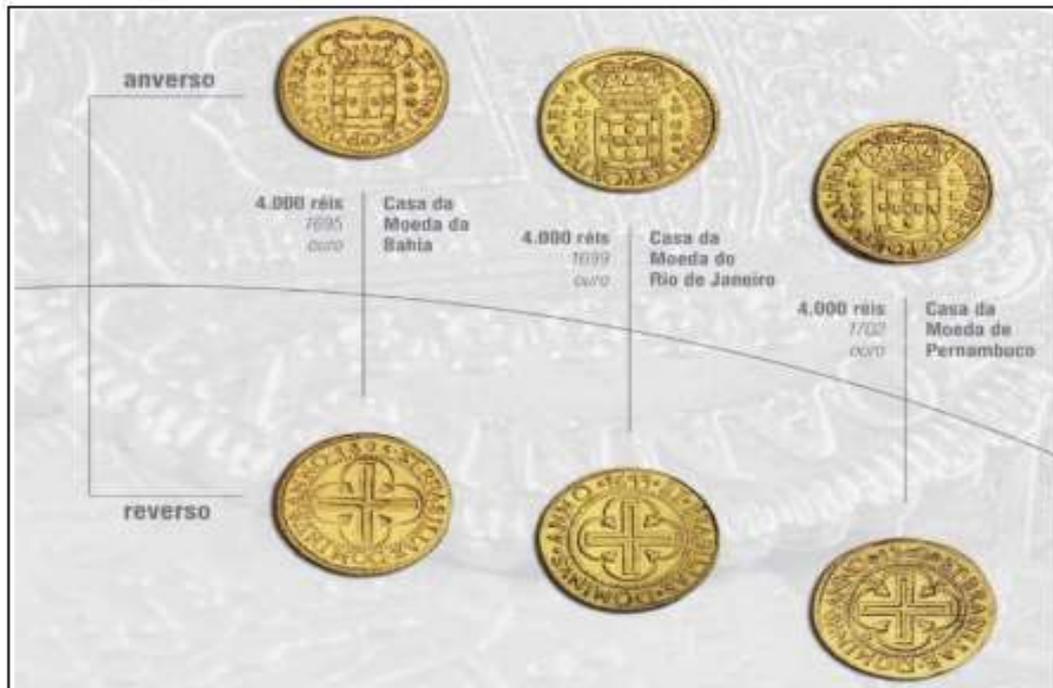
**Figura 2 – Florim holandês, a 1ª moeda cunhada no Brasil**



Fonte: Fernandes (2018).

Segundo Fernandes (2018), a partir do ano de 1695, o Real Português passou a ser cunhado no Brasil, como ilustra a Figura 3:

**Figura 3 – Real Português cunhado no Brasil**



Fonte: Fernandes (2018).

De acordo com Lopes e Rossetti (2005), com a crescente complexidade da vida em sociedade, o escambo precisou ceder lugar a processos indiretos de pagamentos que atribuíram valor às mercadorias e, assim, atenderam uma necessidade geral. Dessa forma, as operações de compra e venda tornaram-se distintas, passando a ser intermediadas principalmente por moedas, já que estas se tornaram um produto de aceitação geral. Portanto, a moeda tornou-se um meio facilitador das transações e desempenhou funções importantes para efetivar as trocas entre os agentes econômicos. Seu surgimento ampliou a divisão social do trabalho e facilitou crescimento da riqueza.

### 2.3 EVOLUÇÃO HISTÓRICA DA MOEDA

A evolução da moeda ao longo da história foi moldada pelas necessidades das sociedades em diferentes momentos. Desde suas origens no escambo até o desenvolvimento de moedas metálicas cunhadas e notas representativas, a moeda tem sido uma ferramenta essencial para facilitar as trocas econômicas.

Nos primórdios da civilização humana não havia moeda. As trocas ocorriam por meio do escambo, onde bens e serviços eram diretamente trocados entre os indivíduos. No entanto, essa forma de troca apresentava diversas dificuldades, como

a falta de divisibilidade dos bens, a dificuldade em avaliar o valor relativo entre diferentes mercadorias e a questão da coincidência de desejos. À medida que as comunidades humanas se desenvolviam e o comércio expandia, surgia a necessidade de encontrar uma solução mais prática para facilitar as trocas e as transações econômicas.

### **2.3.1 Moeda-Mercadoria**

As primeiras moedas, adotadas como resposta às limitações do escambo, foram mercadorias. Segundo Lopes e Rossetti (2005), para que pudessem ser aceitas sem restrições por todos os integrantes dos grupos envolvidos em trocas indiretas, essas deveriam ser suficientemente raras, para que tivessem valor de troca, e deveriam atender a uma necessidade comum e geral, para que tivessem valor de uso.

As moedas-mercadorias variavam amplamente de comunidade para comunidade e de época para época, sob influência dos usos e costumes dos grupos sociais em que circulavam. A Tabela 1 abaixo mostra as principais mercadorias utilizadas como moeda, em diferentes épocas e regiões.

Tabela 1: Principais moedas-mercadorias da história econômica.

Épocas e regiões	Principais moedas-mercadorias
<b>ANTIGÜIDADE</b>	
Egito	Cobre. Anéis de cobre, como subdivisão da unidade-peso.
Babilônia e Assíria	Cobre, prata e cevada.
Lídia	Peças metálicas cunhadas. Embora existam dúvidas históricas, os lídios (século XVII a.C.) teriam sido os primeiros povos a cunhar moedas, atestando seu peso e título.
Pérsia	Gado, sobretudo bovinos e ovinos.
Bretanha	Barras de ferro. Espadas de Ferro. Escravos.
Índia	Animais domésticos. Arroz. Metais (notadamente ouro e cobre).
China	Conchas, seda e metais. Instrumentos agrícolas. Cereais. Sal.
<b>IDADE MÉDIA</b>	
Ilhas Britânicas	Moedas de couro (precursoras das cédulas de papel). Gado. Ouro e prata em unidades-peso.
Alemanha	Gado (início da Idade Média). Cereais (notadamente aveia e centeio). Mel. Moedas cunhadas: <i>Solidus</i> , de ouro; e <i>denar</i> , de prata.
Islândia	Gado. Tecidos. Peixes secos (notadamente o bacalhau).
Noruega	Gado bovino. Escravos. Tecidos. Manteiga. Peles curtidas.
Rússia	Gado bovino. Peles de esquilo e de marta. Prata, em unidade-peso.
China	Arroz (com instrumento de troca e unidade de conta). Chá. Sal.
Japão	Peças de ferro, estanho e prata, com valores inter-relacionados. Anéis de cobre, cobertos com ouro e prata. Pérolas. Ágata. Arroz.
<b>IDADE MODERNA</b>	
Estados Unidos	Época colonial: fumo, cereais, carnes-secas, madeira e gado.
Austrália	Rum, trigo e carne (nos primórdios da colonização britânica).
Canadá	Peles e cereais.
França	Após a desvalorização dos <i>assignats</i> : metais preciosos e cereais.
Alemanha e Áustria	No Tirol: terra como denominador comum de valores; gado, como instrumento de troca.
Japão	Arroz. <i>Warrants</i> , emitidos por depósitos desse cereal, até o século XVIII foram usados como moeda.

Fonte: Lopes e Rossetti (2005).

Mesmo tendo chegado até a Idade Moderna, as moedas-mercadorias aos poucos foram sendo substituídas. A maior parte delas não preenchia as características essenciais que se exigia para o desempenho de suas funções. Conforme Paiva e Cunha (2008):

[...] a moeda mercadoria apresentava uma série de desvantagens, dentre as quais: não era durável, divisível, ou suficientemente escassa para ser percebida como portadora de valor intrínseco e, assim, ter uma aceitação universal. (PAIVA; CUNHA, 2008, p. 240).

Tudo isso somado tornava as transações comerciais difíceis e pouco práticas, comprometendo a sua aceitação geral.

### **2.3.2 Moeda Metálica**

Com a necessidade de formas mais desenvolvidas de moeda, os metais foram ganhando destaque. Sua durabilidade, maleabilidade e escassez relativa garantiram a posição das moedas metálicas como instrumentos universalmente utilizados nas sociedades pré-capitalistas (PAIVA; CUNHA, 2008). Suas características físicas, além de se aproximarem daquelas que se exigem dos instrumentos monetários, possibilitava o processo de cunhagem, essencial para a evolução da moeda. Através da cunhagem, as unidades da moeda são vinculadas a um agente emissor e produzidas de forma padronizada, garantindo sua aceitabilidade (ORRELL; CHLUPATÝ, 2016).

Os metais não preciosos foram os primeiros utilizados na confecção de moedas. No entanto, sua grande abundância comprometia algumas das funções básicas que a moeda deveria atender, em especial a de servir como reserva de valor (LOPES; ROSSETTI, 2005). Com a descoberta de novas jazidas e o aperfeiçoamento das técnicas de fundição, o valor desses metais ficou instável. A solução para este problema foi a adoção do ouro e da prata, metais suficientemente escassos que garantiam a estabilidade dos preços ao longo do tempo (LOPES; ROSSETTI, 2005).

Mesmo não sendo tão utilizados atualmente, os metais preciosos ainda mantêm sua relevância como valiosos recursos para preservação de valor, principalmente em períodos de instabilidade financeira.

### **2.3.3 Moeda-Papel**

Apesar de ter sido um avanço significativo em relação às moedas-mercadorias, o sistema monetário baseado nas moedas metálicas ainda possuía algumas limitações.

Com a multiplicação das trocas entre regiões e países diferentes, manifestaram-se alguns inconvenientes da moeda metálica como instrumento de pagamento. O transporte de metais a longas distâncias tornou-se relativamente difícil (em decorrência do peso) e sujeito a riscos (em decorrência de roubos). Pela precariedade das estradas e dos meios de transporte e, sobretudo, pelos riscos envolvidos no porte de metais preciosos desenvolveram-se esforços para a criação e a difusão de instrumentos monetários mais flexíveis que, ao mesmo tempo em que

contornassem os inconvenientes da moeda metálica, também facilitassem a efetivação de operações de crédito. Ademais, as relações comerciais só poderiam desenvolver-se se esse novo instrumento monetário passasse a ser aceito de forma ampla, ainda que tivesse a necessária contrapartida de lastro metálico integral. (LOPES; ROSSETTI, 2005, p. 32).

Após o Renascimento, os comerciantes, tendo em vista essas circunstâncias, passaram a recorrer a instituições que estavam equipadas para guardar, sob garantia, metais monetários e outros valores (LOPES; ROSSETTI, 2005). Essas instituições eram as chamadas casas de custódia e custodiavam ouro e prata em troca de certificados de depósitos, que passaram a circular em lugar dos metais monetários.

Com a circulação desses certificados, surgiu a chamada moeda-papel. De acordo com Paiva e Cunha (2008):

O lastro metálico da moeda papel costumava ser integral. Com o tempo as “casas de depósito”, os embriões dos bancos modernos, perceberam que o volume de depósitos de metais preciosos era normalmente superior ao volume de saques. Com isso passaram a emitir moeda-papel em quantidade superior ao lastro metálico que lhe dava origem. Ou seja, os depósitos de moedas-metálicas tornavam-se a fonte para a realização de empréstimos em moeda-papel. As rendas desses empréstimos eram apropriadas na forma de juros. (PAIVA; CUNHA, 2008, p. 240).

### **2.3.4 Papel-Moeda**

A popularização dos certificados de depósitos abriu campo para uma nova forma representativa de moeda, não integralmente lastreada. Segundo Lopes e Rossetti (2005), a experiência da custódia e da conversibilidade mostrou que o lastro metálico integral em relação aos certificados em circulação não era necessário para a operacionalização desse novo sistema monetário.

Como nem todos os detentores solicitavam simultaneamente a reconversão da moeda-papel em metais preciosos, o lastro total não se fazia necessário. Assim, as casas de custódia começaram a emitir certificados não lastreados, fazendo uso da confiança da sociedade. Essa emissão com lastro inferior a 100% ensejou a criação da moeda fiduciária, ou papel-moeda (LOPES; ROSSETTI, 2005).

Essa moeda, entretanto, também passou por transformações ao longo do tempo. Apesar de ter possuído lastro metálico parcial em suas fases iniciais, a partir de 1971, com o fim do lastro do dólar em ouro, todos os sistemas monetários

importantes para o mercado internacional passaram a operar puramente com base fiduciária. (LOPES; ROSSETTI, 2005).

### 2.3.5 Moeda Bancária

O avanço na tecnologia da informação através da revolução computacional começou a alterar as formas como as trocas se realizavam nas economias contemporâneas, dando origem a uma nova modalidade de moeda. (COSTA, 2020).

Assim, ao lado da moeda fiduciária desenvolveu-se a moeda bancária. Lopes e Rossetti (2005) explicam o surgimento dela conforme o parágrafo abaixo.

O desenvolvimento desta moeda ocorreu de forma acidental. Foi precipitado pela independência do poder decisório dos departamentos bancário e monetário do Banco da Inglaterra, no século XIX. A não-conscientização de que os depósitos bancários, movimentados por cheques, eram uma forma de moeda ajudou a expansão dos meios de pagamento, pelo efeito multiplicador desses depósitos. (LOPES; ROSSETTI, 2005, p. 33).

Atualmente, a moeda bancária representa uma parcela relevante, senão a maior, dos meios de pagamento em todos os países. Essa forma de moeda é criada pelos bancos comerciais e corresponde ao total de depósitos a vista e a prazo nesses estabelecimentos. Ela também é chamada de moeda invisível, pelo fato de não ter existência física, e de moeda escritural, por corresponder a lançamentos registrados nas contas correntes dos bancos (LOPES; ROSSETTI, 2005).

De acordo com Carvalho *et al.* (2000), os bancos comerciais criam moeda bancária conforme concedem crédito aos seus correntistas. E isso é feito apenas através de um registro contábil.

Quando um indivíduo toma um empréstimo junto a um banco, essa instituição realiza uma operação contábil de criação de depósito à vista. Para conceder um crédito no valor de 5.000 unidades monetárias (u.m.), o banco lança no lado do ativo do seu balancete “empréstimo no valor de 5.000 u.m.”. No lado passivo, lança “depósito à vista no valor de 5.000 u.m.”. (CARVALHO *et al.*, 2000, p. 6).

## 2.4 CONSIDERAÇÕES FINAIS DO CAPÍTULO

Ao final deste capítulo, fica evidente que a moeda transcende seu papel físico, refletindo a história e a complexidade das interações econômicas. O estudo histórico é indispensável para entender as readaptações da moeda, que acompanha a evolução do seu tempo (ABREU; COELHO, 2009). Nos últimos tempos, percebe-se a transição gradual da moeda além de sua forma física, à medida que a tecnologia e a sociedade mudam.

Mais recentemente, as criptomoedas apareceram como uma possível alternativa à moeda bancária, porém, com limitações quanto à sua capacidade de exercer as três funções principais da moeda. Em relação à função de meio de troca, embora as criptomoedas tenham sido apresentadas como uma opção digital para transações, a adoção generalizada para fins cotidianos permanece limitada. Em El Salvador, primeiro país a adotar o Bitcoin como moeda legal, somente 14% das empresas fizeram transações com essa criptomoeda, desde a sua introdução na economia, e 3% afirmaram que enxergavam algum valor comercial nela (KURMANAEV; AVELAR, 2022).

As flutuações frequentes nos preços das criptomoedas também desempenham um papel negativo. A incapacidade de manter um valor relativamente estável em comparação com outras moedas ou bens dificulta a avaliação e a comparação de preços, prejudicando sua utilidade como unidade de conta. Já a volatilidade elevada e a natureza especulativa das criptomoedas dificultam a sua adoção como reserva de valor.

### 3 CRIPTOMOEDAS

As criptomoedas representam um marco na evolução do sistema financeiro global, revolucionando a maneira como as transações são conduzidas. Com sua base tecnológica em *blockchain*, elas proporcionam segurança avançada, descentralização e eficiência. Por outro lado, apresentam sérios problemas, como a instabilidade nos preços, o alto consumo energético no processo de mineração e a facilitação para fraudes.

Nesse capítulo, estuda-se o surgimento e o conceito das criptomoedas, com foco na pioneira entre elas: o Bitcoin. Além do mais, explora-se os mecanismos e as tecnologias que possibilitam o funcionamento do sistema de criptomoedas, abordando desde o papel das redes de mineração até a utilização da criptografia, a fim de fornecer um conhecimento sólido sobre as inovações que as criptomoedas introduziram e como elas se inserem no cenário financeiro contemporâneo.

#### 3.1 SURGIMENTO DAS CRIPTOMOEDAS

O surgimento das criptomoedas representa uma inovação disruptiva no campo das finanças e da tecnologia. Também chamadas de moedas virtuais, elas emergiram em resposta a diversas questões e desafios enfrentados pelos sistemas monetários tradicionais. A crescente desconfiança em relação aos bancos e governos por parte de uma parcela de indivíduos, a necessidade de transações mais rápidas e baratas, bem como o desejo de maior privacidade nas transações, foram alguns dos fatores que levaram ao seu surgimento (ULRICH, 2014).

Testa (2022) define as criptomoedas como:

A moeda objeto do sistema de trocas econômicas em que não há a figura da autoridade central são as denominadas criptomoedas, que, basicamente, são moedas virtuais, conversíveis e descentralizadas, e que se caracterizam, adicionalmente, por serem protegidas por criptografia. (TESTA, 2022, p. 18).

Telles (2020) possui uma visão semelhante, destacada no trecho abaixo:

São chamadas de criptomoedas as 'moedas' que não possuem existência física, sendo criadas por computadores exclusivamente no espaço digital. Tais moedas são criadas de forma descentralizada, sem a intervenção ou

aval de qualquer governo ou autoridade monetária. Elas também não possuem garantia de conversão para moeda oficial, além de não serem lastreadas por ativo real de qualquer espécie e não possuem força obrigatória. (TELLES, 2020, p. 21).

De uma maneira geral, as criptomoedas possuem características inovadoras que as diferenciam dos sistemas monetários tradicionais. Em primeiro lugar, por não dependerem de um agente central, elas são enquadradas como descentralizadas (ULRICH, 2014). Além disso, suas transações são efetuadas a partir de uma carteira digital e, na maioria dos casos, registradas em um *blockchain*.

Segundo Crosby *et al.* (2016), a maior inovação tecnológica das criptomoedas é o uso da tecnologia *blockchain*, um sistema *peer-to-peer*<sup>1</sup> que funciona como uma espécie de registro público onde todas as transações são adicionadas. Oliveira (2022) define *blockchain* como:

A tecnologia *Blockchain* é um tipo de DLT (*Distributed Ledger Technology*), Tecnologia de Registro Distribuído. As DLT são um tipo de tecnologia de base de dados, utilizada para registrar transações. Funcionam de maneira descentralizada, com vários servidores físicos, onde o registro é efetuado de maneira partilhada e repetida entre todos os servidores. Este tipo de sistema parte do princípio que não existe confiança entre os utilizadores, como tal as transações são registadas com recurso a criptografia, e antes de serem publicadas no registro são verificadas por todos os servidores. (OLIVEIRA, 2022, p. 5).

Um sistema *blockchain*, para além de possuir estas características, conta ainda com alguns outros componentes que tornam a tecnologia algo disruptivo (TRELEAVEN; BROWN; YANG, 2017). A grande diferença entre esses sistemas e os restantes DLT é a sua arquitetura. Um sistema *blockchain*, tal como o nome indica, é construído como uma corrente de blocos, onde cada bloco está criptograficamente ligado ao seguinte. Esta construção torna este tipo de sistema virtualmente impossível de subverter, pois qualquer alteração realizada fica registada no sistema, e cria uma nova corrente de blocos. Outra característica que torna o sistema *blockchain* em tecnologia disruptiva é a descentralização de poder, visto que ele não depende de uma entidade central para tomar decisões (TRELEAVEN; BROWN; YANG, 2017).

---

<sup>1</sup> *Peer-to-Peer*, no contexto em questão, caracteriza um sistema em que os computadores conectados a ele formam os servidores, ou seja, não há uma entidade central, mas são os próprios usuários (pontos) da rede que se responsabilizam pela administração (NIFA, 2022).

Diferentemente das moedas tradicionais, as criptomoedas não possuem uma forma física, sendo de caráter puramente virtual. Baseadas em diferentes sistemas de criptografia, cada unidade das moedas é representada por uma sequência única de caracteres, constituída por uma chave pública (disponível para todos os usuários da rede) e uma chave privada (disponível apenas para o dono da carteira) (OLIVEIRA; TOTTI; NEY, 2014).

Essas características conferem maior segurança, transparência e autonomia nas transações, além de possibilitarem a realização de transferências globais de forma instantânea e com baixos custos.

### 3.2 PRIMEIRAS CRIPTOMOEDAS

Embora o Bitcoin tenha sido a primeira criptomoeda a vingar, algumas iniciativas de moeda virtual já haviam sido idealizadas antes do seu surgimento. Mesmo não dando certo, essas tentativas foram importantes, pois serviram como base e inspiração para a criação do Bitcoin.

Uma das primeiras tentativas de moeda virtual foi o *eCash*, de 1983. Seu criador, David Lee Chaum, é considerado um dos maiores criptógrafos do mundo. Overture (2017) afirma:

Um criptógrafo famoso da época chamado David Chaum desenvolveu um projeto chamado *ECash* em 1982 (e lançado em 1983), sendo implementado com as devidas patentes em 1990, através de uma empresa chamada DigiCash. Este projeto inclusive chegou a ser implementado no US Bank, Credit Suisse e no Deutsche Bank, mantendo grande parte da filosofia que atualmente as criptomoedas pregam, como o anonimato. A DigiCash faliu em 1998, graças ao crescimento do uso do cartão de crédito no *e-commerce*. Uma questão importante que merece ser mencionada sobre David Chaum é que ele também desenvolveu um método de votação em 1981, que hoje se assemelha muito a proposta de democracia de criptomoedas como o Decred. Hoje David Chaum é considerado o pai do anonimato na internet. (OVERTURE, 2017, p. 1).

David Chaum trabalhou muito em cima do conceito de anonimato de transações e o *eCash* foi uma das primeiras iniciativas que propôs a ideia de assinatura digital usando chave pública. Em 1983, através do seu artigo chamado "*Blind Signatures for Untraceable Payments*", ele apresentou ideias de como uma transação financeira poderia ser realizada apenas com base em assinatura digital para verificação de autenticidade.

Em 1996, um oncologista chamado Douglas Jackson e um advogado chamado Barry Downey criaram o *e-gold*, um sistema de pagamento eletrônico lastreado em ouro que pretendia ser uma alternativa aos meios de pagamento tradicionais, permitindo a transferência da propriedade de ouro entre seus membros através de uma carteira pública (OVERTURE, 2017).

Porém, por ser um dinheiro privado e centralizado, ele enfrentou uma série de desafios, como problemas de fraude e lavagem de dinheiro. Já que o sistema era anônimo, muitos criminosos começaram a usá-lo para movimentar recursos ilegalmente. Por conta disso, o governo americano acabou encerrando o projeto nos anos 2000 (OVERTURE, 2017).

Outra tentativa de moeda virtual foi proposta por Charles Cohen. Por volta de 1998, ele criou a *Beenz*, uma moeda completamente digital que possibilitava a compra de produtos e serviços na internet (OVERTURE, 2017). De acordo com Grant (2018), os clientes recebiam *Beenz* gastando dinheiro ou tempo em um *website*. Quando acumulados, elas se tornavam moedas, livres para serem compradas, vendidas ou negociadas como qualquer outra moeda.

Segundo Grant (2018), mesmo tendo arrecadado US\$ 86 milhões de grandes companhias de *Venture Capital*, como *Softbank*, *Apax Partners*, *Vivendi* e *Oracle*, a *Beenz* se viu em apuros com o surgimento de uma moeda concorrente, em 1999. Com uma campanha publicitária apresentada por Whoopi Goldberg, a chamada *Flooz* aumentou suas vendas de US\$ 3 milhões para US\$ 25 milhões entre 1999 e 2000 - o suficiente para desafiar *Beenz* pelo título de moeda digital (GRANT, 2018).

A ideia da *Flooz* era praticamente a mesma. Porém, o projeto ficou mais famoso por ter sido usado em esquemas de tráfico de informações de cartões de crédito e lavagem de dinheiro. Inclusive seu CEO, Robert Levitan, foi acusado de realizar compras fraudulentas com 19% de todos os cartões de crédito cadastrados na plataforma (OVERTURE, 2017).

No final dos anos 1990, surgiu uma nova iniciativa de moeda digital, conhecida como *B-money*. Ela foi proposta de forma teórica por Wei Dai na forma de um artigo, mas nunca chegou de fato a ser construída e testada. A ideia era permitir que pseudônimos digitais pudessem enviar e receber moeda em uma rede descentralizada e até mesmo fazer cumprir contratos entre si sem o envolvimento de terceiros (BUNTINX, 2016).

O projeto, ainda que não tenha sido posto em prática, propunha a utilização de um sistema similar ao *blockchain*, com a necessidade de processamento computacional e validação das transações, chegando a considerar a utilização do *Proof of Work*<sup>2</sup> para a mineração (BUNTINX, 2016). Por conta dessas ideias, o projeto foi referenciado no *whitepaper*<sup>3</sup> do Bitcoin, servindo como inspiração para a sua criação (OVERTURE, 2017).

Outro projeto surgido nos finais dos anos 1990, mais precisamente em 1998, foi o *Bitgold*. Com a pretensão de ser uma espécie de ouro digital, ele foi proposto pelo criptógrafo americano Nick Szabo. Segundo Overture (2017):

Nick Szabo, considerado o inventor da tecnologia dos *Smart Contracts*, iniciou seus trabalhos com o *Bitgold*, uma plataforma monetária descentralizada que foi considerada a precursora da arquitetura do Bitcoin. (OVERTURE, 2017, p. 1).

O *Bitgold* oferecia uma forma descentralizada e segura de transferência de valor, eliminando a necessidade de intermediários confiáveis para evitar o gasto duplo da moeda (BUNTINX, 2016). Além disso, proporcionava uma maneira de proteger as transações financeiras contra a interferência do governo. No entanto, apesar dessas vantagens, o projeto não chegou a ser implementado devido a dificuldades tecnológicas (CABRAL, 2023).

Em 2004, seis anos depois do *Bitgold* e quatro anos antes do Bitcoin, surgiu o RPOW – *Reusable Proofs-of-Work*. Segundo Overture (2017):

Em 2004, o criptógrafo Hal Finney desenvolveu um modelo reutilizável de *Proof of Work* baseado no trabalho do Adam Beck. Quando o projeto tomou forma de criptomoeda, foi dado o nome de RPOW, que combinado aos projetos do Adam Back e do Nick Szabo, deu origem a outras criptomoedas. (OVERTURE, 2017, p. 1).

O RPOW usava, como o próprio nome do projeto indica, a prova de trabalho para criar *tokens* digitais que poderiam ser usados como meio de pagamento. Assim, o processo de criação de *tokens* envolvia a resolução de um problema

---

<sup>2</sup> *Proof of Work* é um protocolo de consenso utilizado pela rede Bitcoin para validar e registrar as transações. Ele funciona através do uso de força computacional para resolver problemas matemáticos complexos (NOTÁRIO, 2023).

<sup>3</sup> *Whitepaper* é um documento que traz todas as informações relevantes sobre um ativo, descrevendo seus fundamentos e especificações (CARVALHO, 2021).

matemático e, posteriormente, o depósito desse saldo para o solucionador do cálculo (CABRAL, 2023).

Apesar de todo o esforço, Cabral (2023) afirma que, devido à complexidade do sistema, o projeto não conseguiu atrair um grande número de usuários e nem receber muito financiamento.

### 3.3 SURGIMENTO DO BITCOIN

Foi em 2008, ano da maior crise financeira desde a Crise de 1929, que surgiu o Bitcoin. Também conhecida como a Grande Recessão, a crise financeira de 2008 foi um dos eventos mais marcantes da história econômica mundial. Ela teve origem nos Estados Unidos, com a bolha imobiliária e o colapso do mercado de hipotecas de alto risco, conhecidos como *subprime*. Seu ápice foi atingido com a quebra do *Lehman Brothers*, um dos maiores bancos de investimento. Em setembro daquele ano, o banco declarou falência após uma série de más decisões e exposição excessiva aos ativos relacionados às hipotecas *subprime*, agravando ainda mais a instabilidade e desconfiança do mercado. O colapso sistêmico abalou a estabilidade do sistema financeiro global, resultando em uma recessão econômica de proporções internacionais e afetando milhões de pessoas ao redor do mundo.

Esse colapso financeiro serviu de catalisador para o surgimento e, conseqüente, popularização, de um novo paradigma econômico, dando origem às chamadas criptomoedas - um novo tipo de dinheiro completamente digital. (GUIMARÃES; AGUIAR, 2017).

He (2018) complementa que a crise financeira de 2008 e a desconfiança, tanto nos bancos com operações fraudulentas e com riscos que levaram ao colapso, quanto nos Bancos Centrais, que vieram a socorrer os bancos com fortes injeções de liquidez nos sistemas financeiros, fez com que nascessem movimentos de contestação ao sistema monetário tradicional.

Nesse ano em questão, a primeira criptomoeda foi apresentada ao mundo: tratava-se do Bitcoin. Ele surgiu como resposta à crise financeira mundial de 2008 e à maneira como os governos reagiram a ela. Também se opunha ao papel dos bancos e outros intermediários das transações financeiras, por estar assentado em uma tecnologia que possibilita o envio de recursos financeiros de parte a parte, sem

necessitar de um terceiro de confiança a quem se outorgue a função de zelar para evitar que o mesmo recurso seja gasto mais de uma vez. (BAL, 2015).

Com uma visão análoga, Ulrich (2014) expõe seu ponto de vista sobre alguns fatores que podem ter levado a criação do Bitcoin:

Ainda que possa ser considerada uma mera coincidência o fato de a moeda digital ter surgido em meio à maior crise financeira desde a Grande Depressão de 1930, não podemos deixar de notar o avanço do estado interventor, as medidas sem precedentes e arbitrárias das autoridades monetárias na primeira década do novo milênio e a constante perda de privacidade que cidadãos comuns vêm enfrentando em grande parte dos países desenvolvidos e emergentes. Esses fatores são certamente responsáveis por parte do ímpeto da criação do Bitcoin. (ULRICH, 2014, p. 35).

O Bitcoin foi introduzido através de um artigo intitulado "*Bitcoin: A Peer-to-Peer Electronic Cash System*", escrito por Satoshi Nakamoto – pseudônimo utilizado pelo criador ou (criadores) do Bitcoin – e postado em um fórum aberto na internet. Algumas invenções, como o *B-money* e o *HashCash*, serviram como referência para desenvolver esse sistema de dinheiro eletrônico descentralizado e sem a presença de uma autoridade central para a emissão de moeda ou para a liquidação e validação de transações (ANTONOPOULOS, 2016).

De uma maneira simples, Ulrich (2014) define o Bitcoin como:

Bitcoin é uma moeda digital, *peer-to-peer* (par a par ou, simplesmente, de ponto a ponto), de código aberto, que não depende de uma autoridade central. Entre muitas outras coisas, o que faz o bitcoin ser único é o fato de ele ser o primeiro sistema de pagamentos global totalmente descentralizado. Ainda que à primeira vista possa parecer complicado, os conceitos fundamentais não são difíceis de compreender. (ULRICH, 2014, p. 17.)

Ocorre que, logo no início, segundo Bertolucci (2022), o Bitcoin era conhecido somente por uma comunidade de *Cypherpunks* – grupo ativista que considerava a criptografia uma ferramenta fundamental para proteger a privacidade dos indivíduos. Mas, aos poucos, começou a ganhar o mundo por se tratar de uma forma de moeda totalmente nova e com características muito distintas do sistema monetário tradicional.

### 3.3.1 Características do Bitcoin

Segundo Ichioka e Coimbra (2018), a principal característica do Bitcoin é a sua descentralização e a sua ausência de forma física, pois não é controlada pelo Banco Central. Assim, ele opera em uma rede ausente de uma autoridade controladora e que, portanto, pode continuar ativa mesmo que haja perda de conexão com algumas das partes (CROSBY *et al*, 2016).

Ivaschenko (2016) destaca também o fato de não poder haver aumento da base monetária dado que no código base do Bitcoin foi estipulado uma oferta total de 21 milhões de unidades. Dessa forma, não há risco de inflação, como ocorre com as moedas fiduciárias.

Outra vantagem é o baixo custo de operação. Ulrich (2014) enfatiza os menores custos de transação, conforme o trecho abaixo:

Porque não há um terceiro intermediário, as transações de Bitcoin são substancialmente mais baratas e rápidas do que as feitas por redes de pagamentos tradicionais. E porque as transações são mais baratas, o Bitcoin faz com que micropagamentos e suas inovações sejam possíveis. (ULRICH, 2014, p. 23).

De acordo com Ivaschenko (2016), como a maior parte do processo de transação do Bitcoin envolve a matemática, as taxas de transação são mínimas, equivalendo a 0,1% do valor transacionado. Além disso, enquanto a abertura de conta em bancos é complicada e demorada, uma carteira de criptomoeda pode estar criada e disponível para uso, sem comissões e questionamentos, em até 5 minutos (IVASCHENKO, 2016).

Outra característica marcante no Bitcoin é o uso de pseudônimo, que permite, em certo grau, um anonimato relativo. Porém, as movimentações não são completamente anônimas em função da transparência da rede do Bitcoin, que registra todas as transações em uma espécie de livro-razão, conhecido como *Blockchain*. Ulrich (2014) afirma que:

Em realidade, qualquer e toda transação já efetuada na história da economia Bitcoin pode ser vista no *blockchain*. Enquanto as chaves públicas de todas as transações – também conhecidas como “endereços Bitcoin” – são registradas no *blockchain*, tais chaves não são vinculadas à identidade de ninguém. Porém, se a identidade de uma pessoa estivesse associada a uma chave pública, poderíamos vasculhar as transações no *blockchain* e facilmente ver todas as transações associadas a essa chave.

Dessa forma, ainda que Bitcoin seja bastante semelhante ao dinheiro vivo, em que as partes podem transacionar sem revelar suas identidades a um terceiro ou entre si, é também distinto do dinheiro vivo, pois todas as transações de e para um endereço Bitcoin qualquer podem ser rastreadas. Nesse sentido, Bitcoin não garante o anonimato, mas permite o uso de pseudônimo. (ULRICH, 2014, p. 21).

Além dessas características, que, na visão de alguns autores, se tratam de vantagens para os agentes econômicos em comparação com as moedas tradicionais, o Bitcoin trouxe consigo alguns elementos técnicos que sustentam o seu funcionamento. A análise deles é essencial para entender como essa criptomoeda existe e opera de maneira descentralizada e segura.

### **3.3.2 Funcionamento e Estruturação do Bitcoin**

O surgimento das moedas virtuais está muito relacionado com o desenvolvimento da computação. Durante muito tempo, uma das maiores dificuldades das criptomoedas era solucionar o problema do gasto duplo.

Ulrich (2014) explica esse conceito de maneira simplificada, conforme o trecho a seguir:

Até a invenção do Bitcoin, [...] as transações online sempre requereram um terceiro intermediário de confiança. Por exemplo, se Maria quisesse enviar 100 u.m. ao João por meio da internet, ela teria que depender de serviços de terceiros como PayPal ou Mastercard. Intermediários como o PayPal mantêm um registro dos saldos em conta dos clientes. Quando Maria envia 100 u.m ao João, o PayPal debita a quantia de sua conta, creditando-a na de João. Sem tais intermediários, um dinheiro digital poderia ser gasto duas vezes. Imagine que não haja intermediários com registros históricos, e que o dinheiro digital seja simplesmente um arquivo de computador, da mesma forma que documentos digitais são arquivos de computador. Maria poderia enviar ao João 100 u.m. simplesmente anexando o arquivo de dinheiro em uma mensagem. Mas assim como ocorre com um e-mail, enviar um arquivo como anexo não o remove do computador originador da mensagem eletrônica. Maria reteria a cópia do arquivo após tê-lo enviado anexado à mensagem. Dessa forma, ela poderia facilmente enviar as mesmas 100 u.m. ao Marcos. Em ciência da computação, isso é conhecido como o problema do "gasto duplo", e, até o advento do Bitcoin, essa questão só poderia ser solucionada por meio de um terceiro de confiança que empregasse um registro histórico de transações. (ULRICH, 2014, p.17).

De uma forma geral, pode-se dizer que o gasto duplo ocorre quando um indivíduo realiza múltiplas transações com um dinheiro que não deveria mais existir. Enquanto as moedas tradicionais contornaram esse problema com a utilização de instituições financeiras como intermediárias, as criptomoedas, até 2008, não haviam

encontrado uma solução para tal. E, sem solução, não seria possível o desenvolvimento dessas moedas.

Foi então que Satoshi Nakamoto, no documento que criou o Bitcoin, propôs a resposta para esse problema. O método encontrado foi através do processo de validação de transações da rede Bitcoin: a mineração.

Como o Bitcoin opera em uma rede *peer-to-peer*, não há uma autoridade central encarregada de criar moeda e de validar todas as transações realizadas. Na verdade, quem é responsável por essa atividade são os usuários que proveem a força computacional do sistema, conhecidos como mineradores. Ulrich (2014) explica a importância deles, conforme o trecho abaixo:

O protocolo, portanto, foi projetado de tal forma que cada minerador contribui com a força de processamento de seu computador visando à sustentação da infraestrutura necessária para manter e autenticar a rede da moeda digital. Mineradores são premiados com bitcoins recém-criados por contribuir com força de processamento para manter a rede e por verificar as transações no *blockchain*. E à medida que mais capacidade computacional é dedicada à mineração, o protocolo incrementa a dificuldade do problema matemático, assegurando que bitcoins sejam sempre minerados a uma taxa previsível e limitada. (ULRICH, 2014, p. 20).

Assim, o processo de mineração do Bitcoin consiste na competição entre os mineradores para encontrar soluções para uma equação matemática enquanto se processam as transações (ANTONOPOULOS, 2016). Portanto, qualquer participante da rede pode ser um minerador, necessitando apenas utilizar o poder de processamento de seu computador para verificar e registrar transações.

Essa competição funciona através de um mecanismo de consenso, conhecido como *Proof-of-Work*, que, em resumo, é um problema matemático complexo que deve ser solucionado pelos mineradores. Para garantir a manutenção do sistema, o processo de mineração está ligado a uma taxa de dificuldade, que aumenta conforme o crescimento da rede de usuários (PRYPTO, 2016).

Como forma de recompensa, o minerador que encontrar a solução válida recebe uma quantidade de Bitcoin. Mas cabe ressaltar que o processo de mineração não é infinito, visto que, desde o início, o protocolo projetou uma oferta total máxima de 21 milhões de unidades, que reduz à metade a cada 4 anos (ANTONOPOULOS, 2016).

Embora a mineração seja fundamental para o sistema como um todo, ela traz alguns desafios. O processo de recompensa, levando em consideração a escassez

do Bitcoin, resulta na valorização e especulação desse ativo. Dessa forma, o seu preço passa a apresentar elevada instabilidade, dificultando no enquadramento como moeda.

Além do mais, a mineração do Bitcoin requer um grande consumo de energia devido ao processo computacional intensivo. De acordo com o índice CBECI, que mede o consumo de eletricidade na mineração de criptomoedas, a mineração do Bitcoin consome mais energia que países como Argentina e Holanda (UNIVERSITY OF CAMBRIDGE, 2023)<sup>4</sup>.

Assim, o Bitcoin é criado à medida que milhares de computadores dispersos resolvem problemas matemáticos complexos, sendo esse processo validado e registrado em uma rede descentralizada conhecida como *blockchain* (PRYPTO, 2016).

Um de seus conceitos é dado por Ulrich (2014), conforme o trecho abaixo:

Todas as transações que ocorrem na economia Bitcoin são registradas em uma espécie de livro-razão público e distribuído chamado de *blockchain* (corrente de blocos, ou simplesmente um registro público de transações), o que nada mais é do que um grande banco de dados público, contendo o histórico de todas as transações realizadas. Novas transações são verificadas contra o *blockchain* de modo a assegurar que os mesmos bitcoins não tenham sido previamente gastos, eliminando assim o problema do gasto duplo. A rede global *peer-to-peer*, composta de milhares de usuários, torna-se o próprio intermediário. (ULRICH, 2014, p. 18).

O *blockchain* do Bitcoin é conhecido por ser uma espécie de livro-razão público, armazenando todas as transações, e servindo como uma ferramenta de escrituração e transparência, conforme Kelly (2014). E, tratando-se de uma rede descentralizada, as informações são compartilhadas de forma que cada agente conectado à rede possua uma cópia completa do arquivo (CROSBY *et al*, 2016).

Essas informações são gravadas na forma de uma corrente de blocos, cada um contendo um determinado número de transações. Novos blocos são introduzidos ao final do último bloco já existente, permitindo verificar a validade de todas as transações desde a sua origem e garantindo a continuidade do sistema (CROSBY *et al*, 2016). Quanto maior a quantidade de blocos, maior será o tamanho da rede (EHA, 2017).

---

<sup>4</sup> Números de agosto de 2023, calculados pelo índice CBECI, mostram que o consumo advindo da mineração do Bitcoin esteja por volta de 151 TWh por ano. Enquanto isso, Argentina e Holanda consomem, respectivamente, 127 TWh e 113 TWh por ano (UNIVERSITY OF CAMBRIDGE, 2023).

Portanto, de acordo com Silva e Albuquerque (2017), toda transação é digitalmente assinada e autenticada, mantendo-se no *blockchain* um registro de toda movimentação financeira. Assim, quando uma nova transação é recebida, os seus blocos executam alguns algoritmos que avaliam se o histórico e as assinaturas da transação em questão são válidos e, chegando a um consenso, permitem que ela seja aceita e que um novo bloco seja adicionado a esta cadeia. Caso ocorra algum erro, essa entrada será negada e não adicionada à *blockchain*.

Dessa forma, o único modo possível de manipular as informações introduzidas na corrente é tendo mais poder computacional do que todo o restante da rede, algo inviável devido ao grande número de usuários. Logo, esse modelo faz com que o *blockchain* funcione como um registro distribuído, seguro e transparente para validar as transações e prevenir o gasto duplo sem a presença de uma autoridade reguladora (SILVA; ALBUQUERQUE, 2017).

Outro componente importante para a segurança da rede é a criptografia. Segundo Ciriaco (2015), a criptografia é um conjunto de técnicas para proteger informações de modo que apenas o remetente e o destinatário consigam acessá-la.

Esse processo é alcançado através do uso de algoritmos e chaves criptográficas que garantem a segurança e a privacidade das comunicações e dados em ambientes digitais. No caso do Bitcoin, as transações são protegidas por chaves públicas e privadas, tornando-as extremamente seguras.

As chaves públicas servem para criar endereços de carteiras digitais que podem ser compartilhados, permitindo aos usuários receber fundos. Por outro lado, as chaves privadas são usadas para assinar digitalmente as transações, garantindo que apenas o proprietário da carteira possa autorizar transferências. Portanto, essas devem ser mantidas em segredo pelo titular, sob pena de perda do acesso aos seus fundos. Estima-se que 20% de todas as unidades do Bitcoin estejam em carteiras perdidas, fora de circulação no mercado (KRAUSE, 2018).

Ulrich (2014) exemplifica esses conceitos, conforme trecho abaixo:

As transações são verificadas, e o gasto duplo é prevenido, por meio de um uso inteligente da criptografia de chave pública. Tal mecanismo exige que a cada usuário sejam atribuídas duas “chaves”, uma privada, que é mantida em segredo, como uma senha, e outra pública, que pode ser compartilhada com todos. Quando a Maria decide transferir bitcoins ao João, ela cria uma mensagem, chamada de “transação”, que contém a chave pública do João, assinando com sua chave privada. Olhando a chave pública da Maria, qualquer um pode verificar que a transação foi de fato assinada com sua

chave privada, sendo, assim, uma troca autêntica, e que João é o novo proprietário dos fundos. A transação – e portanto uma transferência de propriedade dos bitcoins – é registrada, carimbada com data e hora e exposta em um “bloco” do *blockchain* (o grande banco de dados, ou livro-razão da rede Bitcoin). A criptografia de chave pública garante que todos os computadores na rede tenham um registro constantemente atualizado e verificado de todas as transações dentro da rede Bitcoin, o que impede o gasto duplo e qualquer tipo de fraude. (ULRICH, 2014, p. 19).

Dessa forma, a criptografia no Bitcoin é um componente fundamental para preservar o anonimato, pois, embora as transações sejam registradas e visíveis no *blockchain*, os agentes são identificados apenas através de sua chave pública, uma sequência de caracteres que atua como uma forma de pseudônimo na rede (ULRICH, 2014). Como a chave pública não se associa a qualquer informação pessoal, isso proporciona um alto nível de privacidade e confidencialidade aos usuários da rede.

### 3.4 CONSIDERAÇÕES FINAIS DO CAPÍTULO

À medida que este capítulo conclui o estudo das criptomoedas e, em particular, do Bitcoin, fica evidente que a mineração e criptografia desempenham papéis centrais na viabilização e segurança dessas moedas virtuais. No entanto, elas abrem portas para desafios significativos, como a instabilidade nos preços, o consumo energético e a lavagem de dinheiro. A interligação entre a criptografia, as transações financeiras e os potenciais riscos associados à lavagem de dinheiro destaca a importância de compreender não apenas os aspectos técnicos das criptomoedas, mas também suas implicações mais amplas no cenário econômico e regulatório contemporâneo. Nesse sentido, a análise das criptomoedas e de suas tecnologias serve como ponto de partida para a exploração das complexidades da lavagem de dinheiro no contexto digital.

## 4 LAVAGEM DE DINHEIRO

A lavagem de dinheiro é uma complexa atividade financeira que tem despertado crescente preocupação nas últimas décadas. Trata-se de um processo pelo qual recursos provenientes de atividades ilegais são ocultados, dissimulados ou integrados ao sistema financeiro de forma a aparentarem origem legítima. Tal prática oferece uma rota de escape para criminosos, possibilitando o usufruto dos lucros de suas atividades ilícitas sem levantar suspeitas ou rastros que possam levar à sua identificação e responsabilização.

Desse modo, este capítulo trata de forma geral o crime de lavagem de dinheiro, a fim de esclarecer ao leitor sobre o mesmo para poder analisá-lo no âmbito das criptomoedas.

### 4.1 ORIGEM E HISTÓRIA DA LAVAGEM DE DINHEIRO

A Itália e os Estados Unidos foram os primeiros países a tipificar a lavagem de dinheiro como crime. No entanto, foi nos EUA que essa prática começou a adquirir uma escala significativa e se tornar mais amplamente disseminada.

Aro (2013) comenta que a primeira tipificação legal do crime de lavagem de dinheiro apareceu na Itália, em 1978. De acordo com o autor, as Brigadas Vermelhas, o maior grupo armado italiano de extrema-esquerda da época, buscavam desarticular o poder político estatal e, para isso, obtinham recursos financeiros ilícitos por meio de extorsões, sequestros e roubos.

Esses ganhos ilegais precisavam ser ocultados e, dessa forma, a lavagem de dinheiro desempenhou um papel crucial para as Brigadas Vermelhas, permitindo-lhes converter seus recursos ilícitos em fundos aparentemente legítimos. Como resposta, o governo italiano anunciou a Lei nº 191 de 18 de maio 1978, incriminando a substituição de dinheiro ou de valores provenientes de roubo qualificado, extorsão qualificada ou extorsão mediante sequestro por outros valores ou dinheiro (ARO, 2013).

No caso dos Estados Unidos, a criminalização da lavagem de dinheiro remete à década de 1920. Durante esse período, foi criada a “Lei Seca” no país. Mas, ao passo que proibia a produção e comercialização de bebidas alcoólicas, gerava um mercado ilegal de milhões de dólares (ARO, 2013).

Foi nesse contexto que surgiram as primeiras máfias norte-americanas. O caso de maior notoriedade internacional é o de Alphonse (Al) Capone, criminoso americano que obtinha suas receitas da comercialização de bebidas alcoólicas. Para ocultar a origem ilegal dos lucros obtidos com atividades ilícitas, utilizava de negócios de fachada, como lavanderias e lavagem de automóveis, para misturar os recursos ilegais com dinheiro proveniente de atividades legítimas.

Em função do uso das lavanderias como forma de dissimular a origem do capital, esse processo ganhou o nome de "lavagem de dinheiro" (RAMOS, 2014). Porém, essa não é a única explicação para o nome deste crime. Segundo Paulsen (2023), há também quem entenda que dar aparência de licitude ao produto do crime, que é dinheiro sujo, corresponderia a lavá-lo.

De acordo com Prado (2016), o crime de lavagem de capitais nasce para combater a criminalidade organizada, sendo configurado internacionalmente apenas no final dos anos 1980, pela ONU, através da Convenção de Viena de 1988 e, posteriormente, em 1989, pelo Grupo de Ação Financeira – GAFI.

Conforme Ramos (2014), o Brasil se atentou a essa atividade criminosa ao ratificar a Convenção de Viena em 1991, mas, somente no ano de 1998, a lavagem de dinheiro foi tipificada com crime, com a criação da Lei nº 9.613/1998.

## 4.2 CONCEITO DE LAVAGEM DE DINHEIRO

De maneira geral, a lavagem de dinheiro é caracterizada como um conjunto de operações que buscam integrar bens, direitos e valores obtidos oriundos de atividades criminosas ao sistema financeiro, dando-lhes a aparência de terem sido obtidos de maneira lícita (ARO, 2013). Para Paulsen (2023), lavar dinheiro consiste em ações que envolvem o produto ou o proveito de infrações penais antecedentes de modo a mantê-los a salvo do conhecimento das autoridades.

Segundo o GAFI (1989) *apud* IPHAN ([201-]), a lavagem de dinheiro é o processo que tem por objetivo disfarçar a origem criminosa dos proveitos do crime. Com uma visão semelhante, a Interpol (1995) *apud* IPHAN ([201-]) define a lavagem de dinheiro como sendo qualquer ação ou tentativa de ação para ocultar ou disfarçar a origem de ativos financeiros obtidos ilegalmente, de maneira que pareçam originar-se de fontes legítimas.

No Brasil, o crime de lavagem de dinheiro foi instituído pela Lei nº 9.613 de 1998, sendo caracterizado no art. 1º, conforme abaixo:

Dos Crimes de "Lavagem" ou Ocultação de Bens, Direitos e Valores  
Art. 1º. Ocultar ou dissimular a natureza, origem, localização, disposição, movimentação ou propriedade de bens, direitos ou valores provenientes, direta ou indiretamente, de crime:  
I - de tráfico ilícito de substâncias entorpecentes ou drogas afins;  
II - de terrorismo;  
III - de contrabando ou tráfico de armas, munições ou material destinado à sua produção;  
IV - de extorsão mediante seqüestro;  
V - contra a Administração Pública, inclusive a exigência, para si ou para outrem, direta ou indiretamente, de qualquer vantagem, como condição ou preço para a prática ou omissão de atos administrativos;  
VI - contra o sistema financeiro nacional;  
VII - praticado por organização criminosa.  
Pena: reclusão de três a dez anos e multa. (BRASIL, 1998, p. 1).

A Lei estabeleceu sete crimes antecedentes à lavagem de dinheiro, determinando uma pena de reclusão de três a dez anos e multa. Além disso, criou o Conselho de Controle de Atividades Financeiras (COAF).

Esse órgão ficou responsável por regular políticas de prevenção e combate ao crime de lavagem de dinheiro, além de fiscalizar os setores obrigados ao cumprimento da lei frente às diretrizes de prevenção. Por se tratar de uma unidade de inteligência financeira, seu objetivo é receber e analisar informações das instituições financeiras e de outros setores obrigados a comunicar operações suspeitas.

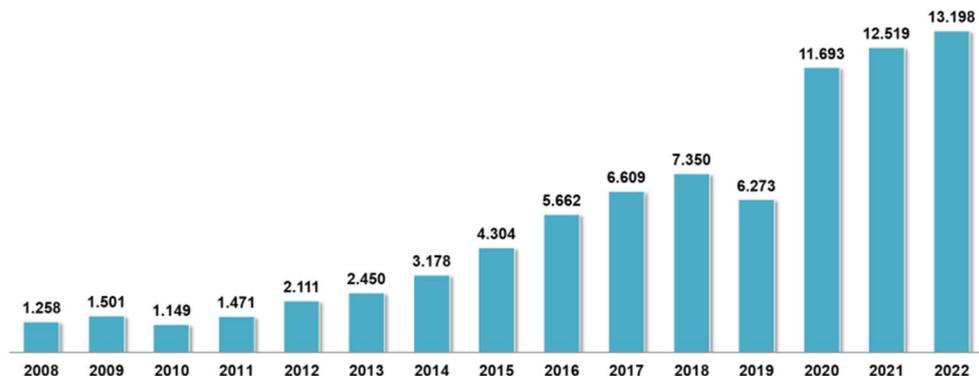
Para tornar mais eficiente a persecução penal dos crimes de lavagem de dinheiro, foi promulgada, em julho de 2012, a Lei nº 12.683, atualizando a Lei nº 9.613/1998 e trazendo como principal mudança a revogação da lista dos sete crimes antecedentes. Com essa alteração, a caracterização da lavagem de dinheiro deixou de estar limitada aos crimes previstos na lista anterior, ampliando o escopo do crime.

Outra mudança introduzida foi a inclusão de novos setores obrigados a manter registros atualizados de clientes e a comunicar operações suspeitas, como por exemplo: cartórios, juntas comerciais e comércio de bens de luxo. O teto da multa também foi ampliado, de R\$ 200 mil para R\$ 20 milhões. Além disso, a nova lei introduziu a possibilidade de aplicação de medidas cautelares, como o sequestro de bens e a suspensão de atividades comerciais ou financeiras, como forma de prevenir a dissipação dos ativos lavados (BRASIL, 2012).

Com as mudanças introduzidas pela Lei 12.683/2012, o Brasil avançou significativamente na prevenção e no combate ao crime de lavagem de dinheiro. A partir de 2012, a elaboração do Relatório de Inteligência Financeira (RIF) pelo COAF cresceu notavelmente e continuamente, exceto pelo ano de 2019. A Figura 4 mostra esses números.

Vale destacar que esses relatórios são produzidos apenas quando o órgão conclui pela existência de fundados indícios do cometimento de ilícitos, após a análise das comunicações recebidas.

**Figura 4 – Relatórios de Inteligência Financeira produzidos pelo COAF**



Fonte: COAF (2023, p. 35)

### 4.3 FASES DA LAVAGEM DE DINHEIRO

O crime de lavagem de dinheiro tem como objetivo a incorporação de recursos, bens e valores de origem ilícita na economia de um país. Ele é caracterizado por um conjunto de operações comerciais ou financeiras, e que se desenvolvem por meio de um processo dinâmico que envolve, teoricamente, três fases independentes que, com frequência, ocorrem simultaneamente (BRASIL, 2023).

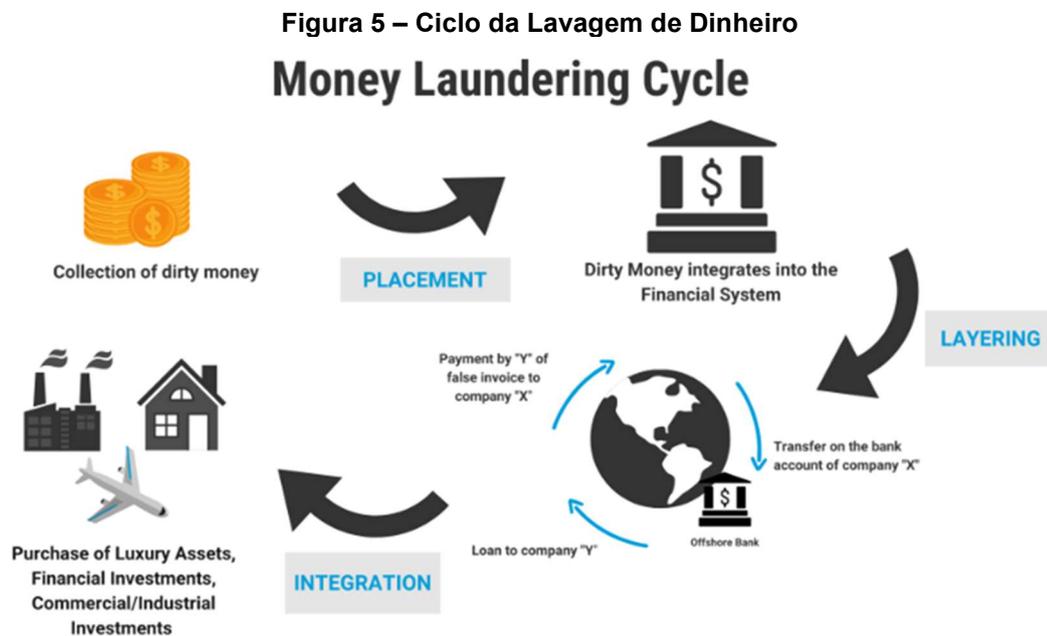
- a) fase da colocação (*placement*);
- b) fase da ocultação (*layering*);
- c) fase da integração (*integration*).

A primeira fase é a colocação do dinheiro no ecossistema financeiro. Essa fase consiste na introdução do recurso ilícito na economia formal, visando ocultar a sua origem e procedência. A colocação se efetua por meio de depósitos, compra de instrumentos negociáveis ou compra de bens (BRASIL, 2023).

Na fase da ocultação ocorre a camuflagem das evidências, efetuando-se o maior número de movimentações financeiras possíveis a fim de dificultar o rastreamento contábil dos recursos ilícitos. Essa é a fase da lavagem propriamente dita (ARO, 2013).

A última fase é a da integração. Nessa etapa, já com aparência lícita, os ativos são formalmente incorporados ao sistema econômico. Segundo Aro (2013), tipicamente são feitos investimentos no mercado mobiliário e imobiliário.

A Figura 5 abaixo apresenta de forma sucinta e visual as etapas do processo de lavagem de dinheiro.



Fonte: UNODC (2023, p. 1)

#### 4.4 CONSIDERAÇÕES FINAIS DO CAPÍTULO

Em síntese, esse capítulo permitiu compreender as fases e conceitos da lavagem de dinheiro, assim como dar ciência às leis criadas para combater esse crime. A partir desses conhecimentos, é possível estudar o envolvimento das criptomoedas nessa prática, examinando como as suas características podem ser exploradas por criminosos para movimentar fundos ilegais.

## 5 ANÁLISE DA RELAÇÃO ENTRE A UTILIZAÇÃO DE CRIPTOMOEDAS E O CRIME DE LAVAGEM DE DINHEIRO

O avanço tecnológico e a crescente popularidade das criptomoedas têm levantado preocupações sobre o potencial de seu uso indevido para fins ilícitos, especialmente no que diz respeito à lavagem de dinheiro. Com suas características de anonimato, descentralização e transações globais instantâneas, os criptoativos oferecem uma nova gama de oportunidades para criminosos ocultarem suas atividades ilegais e camuflarem a origem ilícita de fundos (ESTELLITA, 2020).

Neste capítulo, são explorados os desafios e as estratégias utilizadas pelos agentes maliciosos nesse contexto, bem como as iniciativas regulatórias e tecnológicas em curso para mitigar esse risco crescente e proteger a integridade do sistema financeiro global.

### 5.1 CRIPTOMOEDAS COMO INSTRUMENTO NA LAVAGEM DE DINHEIRO

A lavagem de dinheiro desempenha um papel de fundamental importância em todos os crimes de cunho financeiro, uma vez que possibilita aos criminosos o acesso aos recursos originados de suas atividades ilícitas. O mesmo é válido no ambiente das criptomoedas. O objetivo da lavagem de dinheiro com ativos virtuais é mover fundos para endereços onde a fonte criminosa original não pode ser detectada ou para serviços que permitam a troca por dinheiro fiduciário – como as *exchanges*<sup>5</sup> (CHAINALYSIS, 2023).

Segundo a DCiber (2023), a lavagem de dinheiro com criptoativos normalmente envolve dois tipos de empresas e serviços:

- a) serviços intermediários e carteiras;
- b) pontos de saída para moeda fiduciária.

O primeiro inclui carteiras pessoais, misturadores (*mixers*<sup>6</sup>), mercados da *darknet*<sup>7</sup> e outros serviços, tanto legais quanto ilegais. Os criminosos que atuam com

---

<sup>5</sup> *Exchanges* são agentes intermediários cuja finalidade é oferecer serviços referentes a operações com criptoativos, como intermediação, negociação ou custódia. (BRASIL, 2019).

<sup>6</sup> *Mixers* são serviços que embaralham as criptomoedas de vários usuários com o objetivo de esconder a origem do fundo e o usuário que está por trás daquela transação (CHAINALYSIS, 2022).

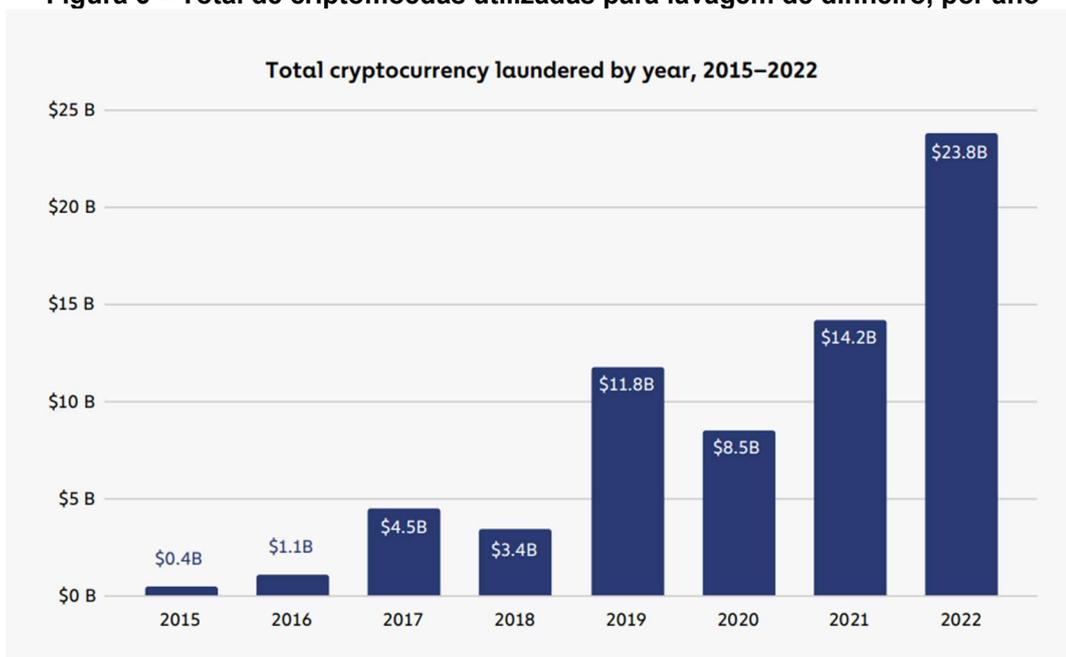
<sup>7</sup> *Darknet* é o termo usado para classificar partes da internet que estão escondidas e podem ser de difícil acesso sem a utilização de um software especial (CAVALCANTE, 2018).

criptoativos utilizam esses serviços para armazenar fundos temporariamente, esconder as suas movimentações e transferências ou realizar trocas entre diferentes ativos.

Por sua vez, o segundo item refere-se a serviços que permitem a troca de criptomoedas por moeda fiduciária. Essa é a parte mais importante do processo de lavagem de dinheiro, pois uma vez que os fundos atingem um serviço, eles não podem mais ser rastreados por meio da *blockchain*. A maioria dos pontos de saída para moeda fiduciária são as *exchanges* centralizadas, mas as *exchanges peer-to-peer* e outros serviços também podem desempenhar essa função (CHAINALYSIS, 2023).

Apesar do progresso e amadurecimento do mercado de criptoativos, ainda persiste o uso desses ativos digitais por parte de criminosos para dissimular os fundos adquiridos por meio de atividades ilícitas. A Figura 6 mostra o montante total de criptomoedas utilizadas para lavagem de dinheiro ao longo dos anos. No geral, endereços ilícitos enviaram quase US\$ 23,8 bilhões em criptomoedas em 2022, representando um aumento de 68% em relação a 2021. O valor de 2022 é o maior da série histórica da Chainalysis, acompanhado do ano de 2021, com US\$ 14,2 bilhões movimentados e 2019, com US\$ 11,8 bilhões.

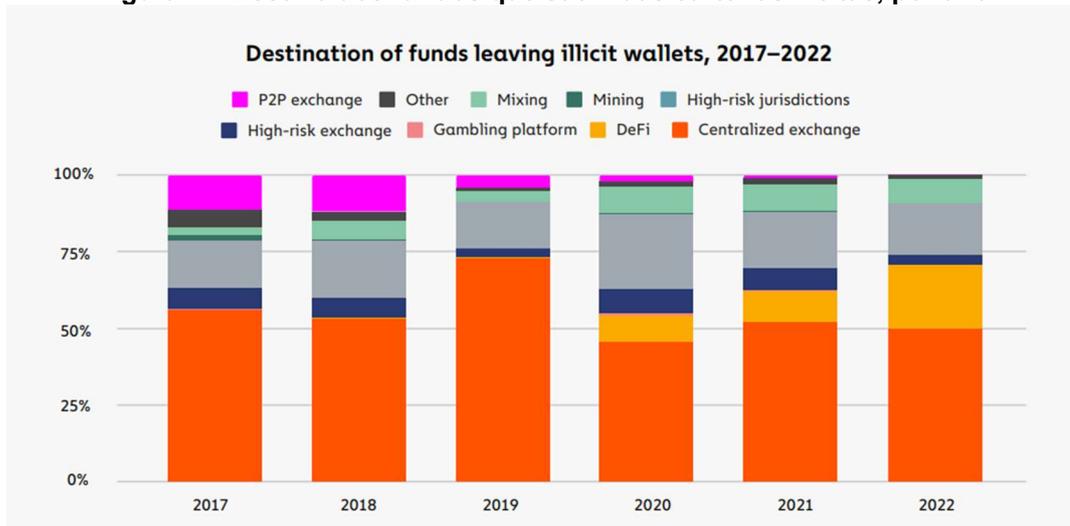
**Figura 6 – Total de criptomoedas utilizadas para lavagem de dinheiro, por ano**



Fonte: Chainalysis (2023, p. 43)

A maioria dessas criptomoedas ilícitas foi enviada para *exchanges* centralizadas, que receberam quase metade de todos os fundos enviados a partir de endereços ilícitos, conforme mostra a Figura 7. De acordo com a Chainalysis (2023), um dos motivos para isso é o fato das *exchanges* serem saídas fiduciárias, ou seja, plataformas que permitem a conversão da criptomoeda ilícita em dinheiro.

**Figura 7 – Destino dos fundos que saem das carteiras ilícitas, por ano**

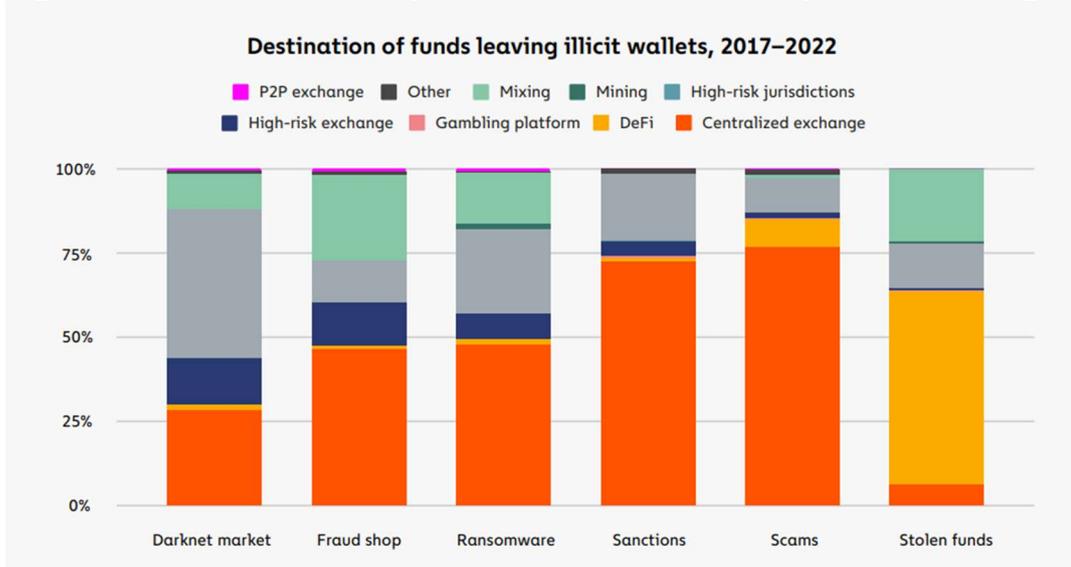


Fonte: Chainalysis (2023, p. 44)

Embora o destino preferido dos fundos ilícitos continue sendo as *exchanges* centralizadas, os protocolos *DeFi*<sup>8</sup> receberam mais fundos ilícitos do que em qualquer ano anterior, continuando uma tendência que começou em 2020. Porém, como eles não permitem a conversão de criptomoedas em moeda fiduciária, a maioria desses fundos é movida, na sequência, para outros serviços, como pontos de saída para moeda fiduciária (DCIBER, 2023). Além disso, quase todo o uso de protocolos *DeFi* para lavagem de dinheiro é realizado por um grupo criminoso específico: *hackers* que roubam criptomoedas. A Figura 8 evidencia isso.

<sup>8</sup> *DeFi* é a sigla para *decentralized finance* (finanças descentralizadas), um conjunto de aplicações que utiliza a rede *blockchain* para remover intermediários das transações financeiras (SHARMA, 2022).

**Figura 8 – Destino dos fundos que saem das carteiras ilícitas, por atividades ilegais**



Fonte: Chainalysis (2023, p. 44)

Os *hackers* que mantêm criptomoedas roubadas são a única categoria criminosa que envia a maioria dos fundos para protocolos *DeFi*, cuja participação é superior a 50%. Segundo a Chainalysis (2023), o ano de 2022 foi marcado por um número enorme de ataques cibernéticos, o que explica por que esses criminosos virtuais quase que exclusivamente impulsionaram o aumento geral no uso de protocolos *DeFi* para a lavagem de dinheiro. Além disso, o fato de os próprios protocolos terem sido o principal alvo de ataques cibernéticos em 2022 também influencia esses números.

Em ataques a protocolos *DeFi*, os *hackers* costumam se apropriar de criptomoedas que não são listadas em outras *exchanges*, tornando necessário o uso de *exchanges* descentralizadas para trocá-las por outras mais líquidas. No entanto, essas corretoras não permitem o saque de criptomoedas, sendo necessário recorrer à uma *exchange* centralizada ou outro ponto de saída para moeda fiduciária.

Embora a maioria das categorias criminosas costume destinar seus fundos ilegais para as corretoras centralizadas, há outra exceção notável: os vendedores e administradores de mercados da *darknet*. Esses enviaram a maior parte de seus fundos para outros serviços ilícitos, principalmente mercados da *darknet* com serviços de lavagem de dinheiro (CHAINALYSIS, 2023). Além disso, esses endereços de mercados da *darknet* também enviaram uma parte considerável dos seus fundos para *exchanges* de alto risco, como a *Bitzlato* – uma *exchange* baseada

na Rússia que foi fechada recentemente em uma operação internacional de aplicação da lei devido a suas atividades de lavagem de dinheiro (DCIBER, 2023).

De uma maneira geral, observa-se que mais da metade de todos os fundos enviados a partir de endereços ilícitos são direcionados diretamente para corretoras centralizadas, tanto as principais como as de alto risco, onde podem ser trocados por moeda fiduciária. No entanto, mais de 40% dos fundos ilícitos são primeiro enviados para serviços intermediários, como *mixers* e protocolos *DeFi* (DCIBER, 2023).

De acordo com a Chainalysis (2023), os misturadores são um popular serviço de embaralhamento usado por criminosos que atuam com criptomoedas, recebendo 8% de todos os fundos enviados a partir de endereços ilícitos em 2022. Eles funcionam reunindo criptomoedas de vários indivíduos, misturando-as e enviando para cada um o valor que foi depositado. Assim, a criptomoeda de cada usuário só pode ser rastreada até o misturador, e não mais até a sua fonte original.

Embora existam muitos casos legítimos de uso para misturadores, a maioria relacionada à privacidade financeira, eles também são aproveitados pelos criminosos, o que explica sua popularidade como destino de fundos ilícitos. Isso fez com que, em 2022, o OFAC proibisse dois misturadores pela primeira vez na história: o *Blender.io* e o *Tornado Cash*, ambos por envolvimento na lavagem de criptomoedas roubadas pelo grupo *hacker* norte-coreano *Lazarus Group*.

Segundo a Chainalysis (2023), o banimento desses misturadores pode ter contribuído para duas tendências observadas em 2022: a quantidade total de criptomoedas enviadas para misturadores diminuiu significativamente, e os fundos que foram para esses serviços tinham mais probabilidade de serem provenientes de fontes ilícitas, conforme ilustra a Figura 9.

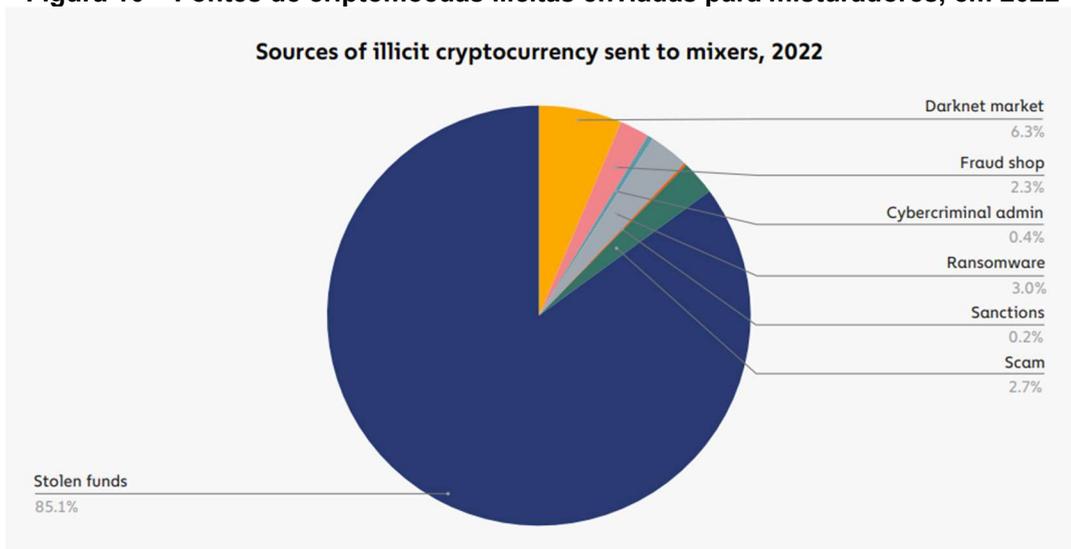
**Figura 9 – Criptomoedas recebidas pelos misturadores, por origem**



Fonte: Chainalysis (2023, p. 46)

Conforme se observa na Figura 10, a grande maioria do valor ilícito processado pelos misturadores é composta por fundos roubados, sendo uma parcela significativa roubada por *hackers* associados à Coreia do Norte, que provavelmente não serão dissuadidos pela ameaça de sanções dos Estados Unidos, uma vez que residem em uma jurisdição não cooperativa (DCIBER, 2023).

**Figura 10 – Fontes de criptomoedas ilícitas enviadas para misturadores, em 2022**

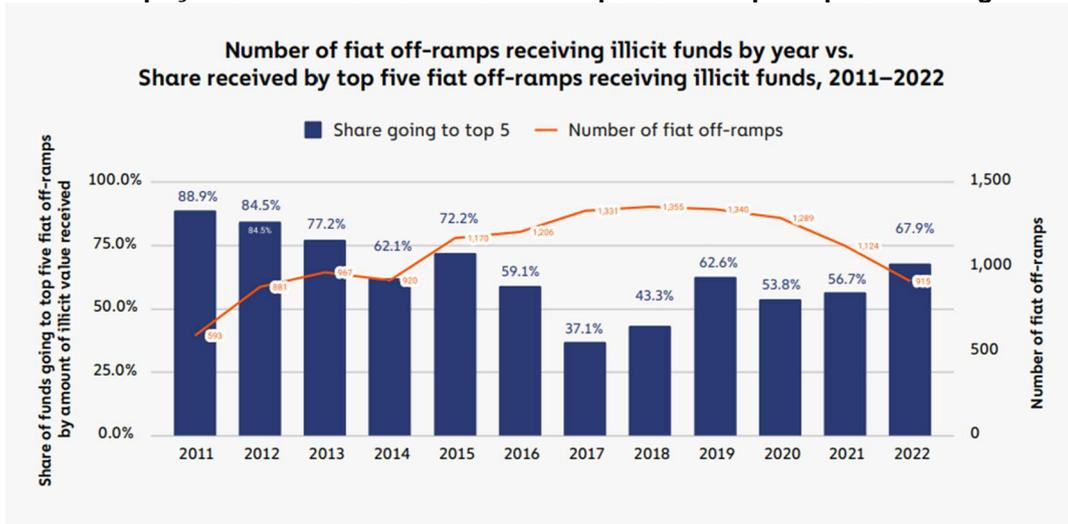


Fonte: Chainalysis (2023, p. 46)

Além disso, como já discutido, os serviços de saída para moeda fiduciária, como as *exchanges*, são cruciais para a lavagem de dinheiro, pois são nesses

serviços que os criminosos podem transformar criptomoedas em dinheiro, que provavelmente é o seu objetivo final. No entanto, embora existam milhares de serviços que oferecem a conversão para moeda fiduciária, apenas alguns poucos recebem a maioria dos fundos ilícitos, conforme pode ser observado na Figura 11.

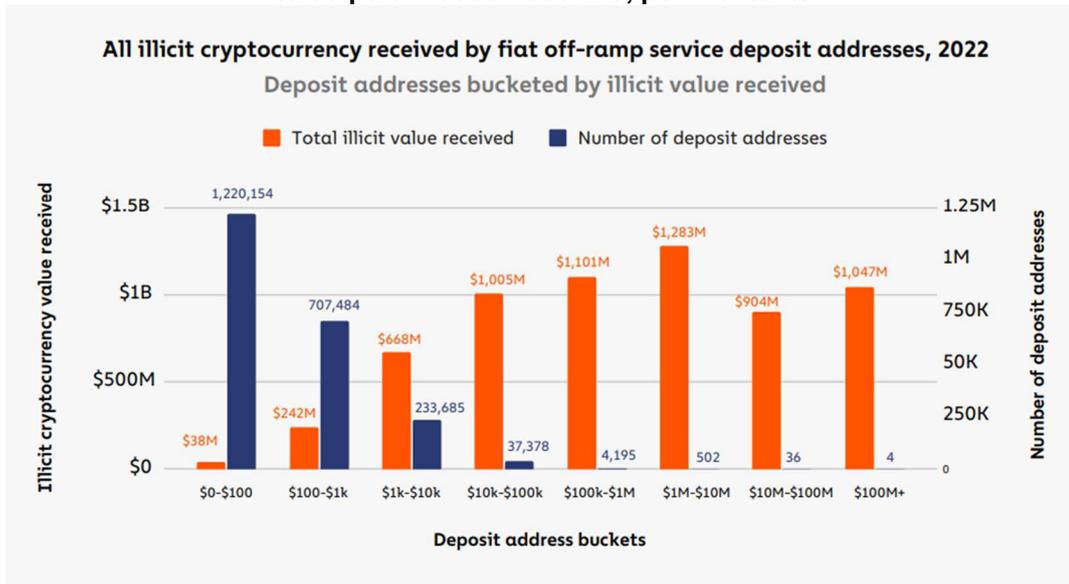
**Figura 11 – Número de serviços de saídas para moeda fiduciária recebendo fundos ilícitos vs. Participação em fundos ilícitos recebidos pelas cinco principais exchanges**



Fonte: Chainalysis (2023, p. 48)

Além da maioria dos fundos ilícitos estarem sendo destinados a poucas *exchanges*, eles também estão concentrados em poucos endereços. A Figura 12 mostra que quatro endereços de depósito receberam mais de US\$ 100 milhões em criptomoedas ilícitas em 2022, totalizando pouco mais de US\$ 1 bilhão, enquanto 1,2 milhão de endereços de depósito que receberam menos de US\$ 100 em fundos ilícitos somaram um total de US\$ 38 milhões. Conforme o estudo da Chainalysis (2023), a maior parte da lavagem de dinheiro de criptomoedas é facilitada por um grupo muito pequeno de pessoas, em que mais da metade dos fundos ilícitos recebidos pelos serviços de saída para moeda fiduciária em 2022 foram destinados a apenas 542 endereços de depósito.

**Figura 12 – Valor de criptomoeda ilícita recebida pelos endereços de depósito de serviços de saída para moeda fiduciária, por montante**

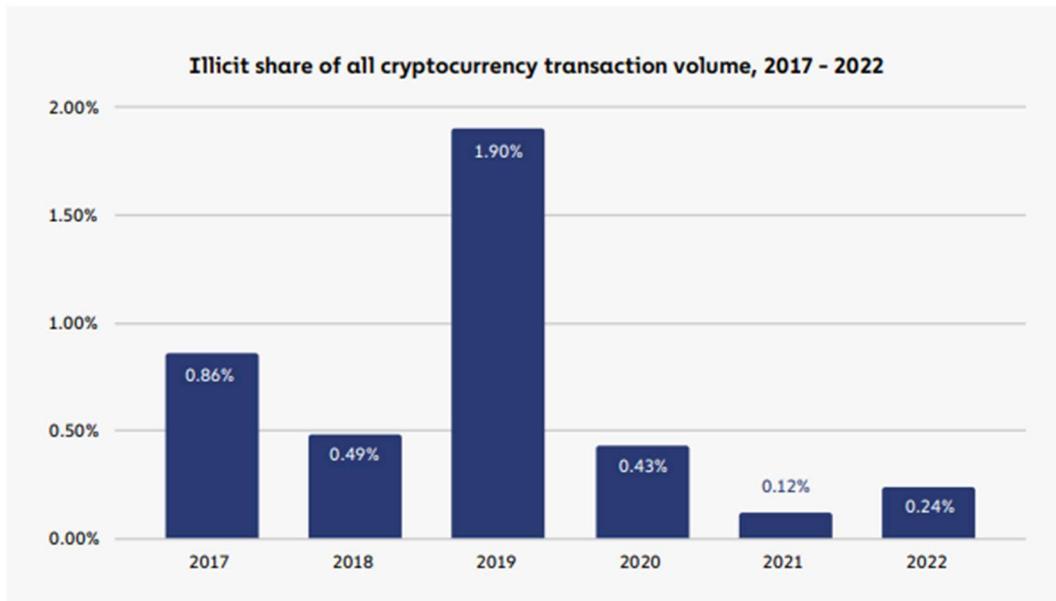


Fonte: Chainalysis (2023, p. 49)

Como se observou, há um alto nível de concentração na atividade de lavagem de dinheiro com criptoativos. Dessa forma, se as autoridades policiais e as equipes de monitoramento conseguissem interromper as atividades dos indivíduos e grupos por trás desses endereços, tornar-se-ia muito mais difícil para os criminosos lavarem criptomoedas em grande escala, o que contribuiria significativamente para tornar o ecossistema mais seguro.

Porém, apesar do crescimento, o ecossistema de lavagem de dinheiro por meio de criptomoedas continua relativamente pequeno quando comparado ao uso de criptomoeda para outros fins. No geral, a atividade ilícita em criptomoedas continua a representar uma pequena parcela do volume total, menos de 1%, conforme ilustra a Figura 13.

**Figura 13 – Participação ilícita no volume total de transações de criptomoedas, por ano**



Fonte: Chainalysis (2023, p. 7)

E, ao comparar com a quantidade estimada de dinheiro lavado globalmente em um ano, percebe-se que a participação de criptomoedas é insignificante. Segundo o Escritório de Drogas e Crimes da ONU (2022), estima-se um total entre US\$ 800 bilhões e US\$ 2 trilhões em lavagem de dinheiro no mundo todo, por ano.

Em conclusão, a análise dos dados apresentados nessa seção evidencia que, embora as criptomoedas sejam utilizadas como ferramenta para a lavagem de dinheiro, sua representatividade nesse contexto é notavelmente baixa. Apesar de alguns casos de atividades ilícitas associadas a esses ativos, é importante ressaltar que a vasta maioria das transações de criptomoedas ocorre de forma legítima.

A combinação de avanços na tecnologia de análise na *blockchain* e o aprimoramento das medidas de conformidade por parte das *exchanges* e serviços de criptomoedas tem desempenhado um papel fundamental na redução da criminalidade no ecossistema das criptomoedas. Assim, apesar de suas características pseudonímias, *blockchains* públicos são transparentes desde o início, dado que cada transação é acrescentada a um registro público e aberto e compartilhada entre todos os participantes da rede. No entanto, se faz necessária uma contínua vigilância e colaboração entre as autoridades e o setor privado para combater quaisquer atividades ilícitas e assegurar um ambiente seguro e confiável para os usuários de criptomoedas.

## 5.2 REGULAMENTAÇÃO DAS CRIPTOMOEDAS

Uma das melhores formas para mitigar o uso indevido das criptomoedas na prática de crimes, em especial a lavagem de dinheiro, é estabelecendo um ambiente regulatório sólido e abrangente. A clareza nas leis e diretrizes regulatórias pode trazer maior segurança jurídica tanto para os usuários como para as empresas que operam no ecossistema dos criptoativos.

Através de regulamentações bem elaboradas, é possível implementar controles mais efetivos, exigir procedimentos de identificação dos usuários, rastrear transações suspeitas e fortalecer os mecanismos de supervisão e monitoramento. Além disso, a colaboração entre governos, instituições financeiras e empresas do setor é essencial para o compartilhamento de informações relevantes e o desenvolvimento de soluções conjuntas para o enfrentamento dos desafios impostos pela criminalidade no universo das criptomoedas.

No Brasil, a primeira regulamentação governamental que trata de criptomoedas entrou em vigor em 1º de agosto de 2019 com a publicação da Instrução Normativa RFB nº 1.888, de maio de 2019. Emitida pela Receita Federal do Brasil, ela dispõe sobre a obrigatoriedade de reporte de informações relativas às operações realizadas com criptoativos (BRANDÃO, 2019).

Nela constam as definições para os criptoativos e para *exchanges* de criptoativos, sob a ótica da RFB:

Art. 5º - Para fins do disposto nesta Instrução Normativa, considera-se:

I - criptoativo: a representação digital de valor denominada em sua própria unidade de conta, cujo preço pode ser expresso em moeda soberana local ou estrangeira, transacionado eletronicamente com a utilização de criptografia e de tecnologias de registros distribuídos, que pode ser utilizado como forma de investimento, instrumento de transferência de valores ou acesso a serviços, e que não constitui moeda de curso legal; e

II - *exchange* de criptoativo: a pessoa jurídica, ainda que não financeira, que oferece serviços referentes a operações realizadas com criptoativos, inclusive intermediação, negociação ou custódia, e que pode aceitar quaisquer meios de pagamento, inclusive outros criptoativos.

Parágrafo único. Incluem-se no conceito de intermediação de operações realizadas com criptoativos, a disponibilização de ambientes para a realização das operações de compra e venda de criptoativo realizadas entre os próprios usuários de seus serviços. (BRASIL, 2019, p. 1).

O art. 6º da IN 1888/2019 especifica quem está obrigado a prestar informações:

Art. 6º - Fica obrigada à prestação das informações a que se refere o art. 1º:  
I - a *exchange* de criptoativos domiciliada para fins tributários no Brasil;  
II - a pessoa física ou jurídica residente ou domiciliada no Brasil quando:  
a) as operações forem realizadas em *exchange* domiciliada no exterior; ou  
b) as operações não forem realizadas em *exchange*. (BRASIL, 2019, p. 1).

No caso das *exchanges* brasileiras, deverão ser informadas todas as operações dos clientes que ali transacionam. Para pessoas físicas ou jurídicas, as informações deverão ser prestadas sempre que o valor mensal das operações, isolado ou conjuntamente, ultrapassar R\$ 30.000,00. Além disso, a normativa determina que as empresas e corretoras que realizam operações com criptoativos devem manter registros detalhados das operações e identificação dos clientes, permitindo maior rastreabilidade das transações e identificação de possíveis atividades ilícitas (BRANDÃO, 2019).

É importante destacar que o objetivo principal da Instrução Normativa (IN) 1888/2019 é de natureza tributária. O seu propósito é regulamentar as operações envolvendo criptoativos no país, especialmente no que se refere à declaração de operações com criptomoedas, para fins de tributação. No entanto, mesmo sua finalidade principal sendo tributária, ela também busca coibir a prática de crimes financeiros, como a lavagem de dinheiro, promovendo maior segurança e confiança no mercado de criptoativos.

Recentemente, em dezembro de 2022, foi sancionada a Lei nº 14.478/2022 que regulamenta o mercado de criptomoedas no Brasil, colocando o país em um grupo seleto de países que estabeleceram regras específicas para o funcionamento de empresas do setor (MALAR, 2023). A nova lei foi originada com o propósito de combater a criminalidade e lidar com a crescente complexidade do crime no mundo digital.

De acordo com Malar (2023), a legislação traz mais segurança aos investidores e clientes, criando exigências para a operação das corretoras e com tipificações específicas para crimes envolvendo ativos digitais. Além disso, foram adotadas medidas em linha com as orientações de organismos internacionais especializados no combate e prevenção à lavagem de dinheiro, como o GAFI (PAZ; PAGLIUSO, 2023).

O art. 3º da Lei nº 14.478/2022 define o que são ativos virtuais, conforme abaixo:

Art. 3º - Para os efeitos desta Lei, considera-se ativo virtual a representação digital de valor que pode ser negociada ou transferida por meios eletrônicos e utilizada para realização de pagamentos ou com propósito de investimento, não incluídos:

I - moeda nacional e moedas estrangeiras;

II - moeda eletrônica, nos termos da Lei nº 12.865, de 9 de outubro de 2013;

III - instrumentos que provejam ao seu titular acesso a produtos ou serviços especificados ou a benefício proveniente desses produtos ou serviços, a exemplo de pontos e recompensas de programas de fidelidade; e

IV - representações de ativos cuja emissão, escrituração, negociação ou liquidação esteja prevista em lei ou regulamento, a exemplo de valores mobiliários e de ativos financeiros. (BRASIL, 2022, p. 1).

Ainda, é definido o Banco Central como o órgão responsável pela supervisão do mercado de criptoativos no Brasil. Com isso, Duque (2023) afirma que o BCB tem as funções de definir as regras do setor, autorizar a concessão de licenças de operação e fiscalizar as *exchanges* e os prestadores de serviços relacionados aos ativos. Ao mesmo tempo, a Comissão de Valores Mobiliários (CVM) deverá supervisionar empresas e criptoativos considerados valores mobiliários.

Entre os principais pontos, a lei acrescenta no Código Penal um novo crime de estelionato especializado em ativos virtuais com pena de reclusão entre 4 e 8 anos, além de multa. Além do mais, o crime de lavagem de dinheiro terá pena maior no caso da operação de lavagem por intermédio de ativos virtuais. Neste caso, a ocorrência entra como agravante e pode crescer de um a dois terços no total da pena, a depender da recorrência (DUQUE, 2023).

Outro aspecto importante da Lei nº 14.478/2022 – Marco Legal das Criptomoedas – é que as prestadoras de serviços virtuais se tornaram equiparadas às instituições financeiras (DUQUE, 2023). Desse modo, são obrigadas a identificar clientes e manter registros para repassar informações aos órgãos de fiscalização e combate ao crime organizado e à lavagem de dinheiro.

Assim, a regulamentação desempenha um papel essencial no combate ao crime com criptoativos, trazendo uma maior segurança às operações realizadas com o uso de ativos virtuais. Além do mais, contribui para a construção de uma imagem positiva e legítima para as criptomoedas, tornando-as mais acessíveis e compreensíveis.

### 5.3 CONSIDERAÇÕES FINAIS DO CAPÍTULO

A análise realizada nesse capítulo entre a utilização de criptomoedas e o crime de lavagem de dinheiro revelou um resultado distinto da narrativa frequentemente associada a esses ativos digitais. Os dados examinados expuseram a presença de práticas ilegais, porém em uma escala reduzida, confrontando assim as noções que associam as criptomoedas a atividades criminosas apenas. Os resultados aqui apresentados ressaltam a importância de se olhar além das percepções superficiais e reconhecer que as criptomoedas podem ser utilizadas legalmente para uma série de finalidades. No entanto, é fundamental reconhecer também a necessidade de uma regulamentação do setor, a fim de mitigar quaisquer possibilidades de aumento dos crimes relacionados às criptomoedas.

Nesse contexto, o Brasil se destaca como um dos poucos países que possuem uma lei específica para o mercado de criptomoedas. A Instrução Normativa 1888/2019, a Lei nº 14.478/2022 e outros avanços regulatórios demonstram o compromisso do país em acompanhar o rápido crescimento desse setor e em promover a inovação de forma responsável e segura, criando um ambiente de confiança para investidores, empreendedores e usuários, ao mesmo tempo que protege o sistema financeiro e a sociedade contra práticas criminosas.

## 6 CONCLUSÃO

O trabalho buscou aprofundar a compreensão sobre a interação entre as criptomoedas e o crime de lavagem de dinheiro. Com a finalidade de verificar uma relação entre ambos, o estudo foi estruturado em quatro capítulos que buscaram fornecer uma base sólida de conhecimento teórico.

O primeiro traçou uma linha do tempo desde a história das trocas até o surgimento das criptomoedas. Essa contextualização histórica permitiu entender as raízes, importância e funções da moeda ao longo do tempo. Embora hoje a moeda já esteja generalizada na economia, sua concepção foi uma das maiores inovações sociais e econômicas, permitindo uma transição das formas primitivas de troca para uma unidade comum de valor. A moeda, em sua forma física, materializou a confiança mútua necessária para facilitar transações e estimular o comércio. Ela possibilitou o progresso material e humano, viabilizando uma economia mais eficiente e uma divisão do trabalho mais elaborada (ABREU; COELHO, 2009).

O segundo capítulo foi responsável por analisar as moedas virtuais, em especial, o Bitcoin. Criado em 2008, ele introduziu inovações antes inimagináveis, destacando-se: a sua natureza descentralizada, o compartilhamento de um registro público e universal por todos os usuários, a capacidade de transações instantâneas e internacionais, e a ausência de um intermediário para validar as transferências (ULRICH, 2014). Assim, esse capítulo teve como objetivo analisar as características, funcionamento e tecnologias do Bitcoin, a fim de compreender as particularidades que podem contribuir na sua utilização em atividades criminosas, como a lavagem de dinheiro.

No terceiro capítulo, contextualizou-se o crime de lavagem de dinheiro, sua origem histórica, conceitos fundamentais e fases distintas. O objetivo foi fornecer um entendimento sólido, permitindo assim uma análise no âmbito das criptomoedas.

Por fim, o último capítulo buscou compilar os conceitos dos capítulos anteriores a fim de verificar um possível envolvimento das criptomoedas na prática do crime de lavagem de dinheiro. A partir de indicadores e dados fornecidos pela empresa Chainalysis, a análise permitiu concluir que as criptomoedas são usadas como instrumento para a lavagem de dinheiro. Por conta de sua natureza descentralizada e relativo anonimato, elas são exploradas para ocultar a proveniência ilícita de fundos.

Entretanto, os dados mostraram que a utilização de criptomoedas para atividades criminosas representa apenas uma pequena fração de sua aplicação total e a vasta maioria das transações tem fins legais. Portanto, é necessário reconhecer que a narrativa que as associa ao crime é muitas vezes desproporcional e desinformada. Em vez disso, é necessário compreender que as criptomoedas, assim como qualquer tecnologia, podem ser utilizadas de maneiras positivas e inovadoras, desde que haja um entendimento aprofundado de seu funcionamento e aplicações.

Este trabalho destacou a importância de uma regulamentação no contexto das criptomoedas, a fim de evitar que elas se tornem uma ferramenta aberta para atividades ilegais, ao mesmo tempo em que se preserva seu potencial inovador. A construção de um ambiente regulatório balanceado requer uma compreensão profunda das particularidades das criptomoedas, a fim de não sufocar sua evolução com restrições excessivas, mas também não negligenciar os riscos de lavagem de dinheiro e outros crimes financeiros. Portanto, a regulamentação se revela como um componente crítico para garantir uma coexistência harmoniosa entre a inovação tecnológica e a segurança financeira.

Embora o estudo tenha apontado pela baixa participação do uso como lavagem de dinheiro e da importância das regulações específicas, não se pretendeu no presente trabalho avançar em conclusões sobre o potencial de uso de criptomoedas de forma mais disseminada na economia, cabendo para estudos futuros retomar discussões para tal no sentido de sua alta instabilidade, que dificultam as funções de reserva de moeda e unidade de conta – trazidas no primeiro capítulo após a introdução. Ainda, cabem investigar as questões relacionados ao intensivo uso energético na função de mineração.

## REFERÊNCIAS

- ABREU, Yolanda Vieira de; COELHO, Sanay Bertelle. **Evolução histórica da moeda**: estudo de caso: Brasil (1889-1989). Madri, 2009. Disponível em: <https://books.google.com.br/books?hl=pt-BR&lr=&id=TTOJwxRteQ0C&oi=fnd&pg=PA9&dq=surgimento+da+moeda&ots=Pp6ZUDdJey&sig=ga3Mhrza1cJT6lNh7ksFdENrlu4#v=onepage&q=surgimento%20da%20moeda&f=false>. Acesso em: 2 ago. 2023.
- AMADO, Adriana Moreira. Limites monetários ao crescimento: Keynes e a não-neutralidade da moeda. **Revista Ensaios FEE**, Porto Alegre, v. 21, n. 1, p. 44-81, 2000. Disponível em: <https://core.ac.uk/download/pdf/235711743.pdf>. Acesso em: 19 jul. 2023
- ANTONOPOULOS, Andreas. **Mastering Bitcoin**: Unlocking Digital Cryptocurrencies. Sebastopol: O'Reilly Media, 2016.
- ARO, Rogério. Lavagem de dinheiro – Origem histórica, conceito, nova legislação e fases. **Revista Jurídica da Universidade do Sul de Santa Catarina**, [S.l.]. v. 3, n. 6, p. 167-177, 2013. Disponível em: [https://portaldeperiodicos.animaeducacao.com.br/index.php/U\\_Fato\\_Direito/article/view/19488/12977](https://portaldeperiodicos.animaeducacao.com.br/index.php/U_Fato_Direito/article/view/19488/12977). Acesso em: 2 ago. 2023.
- BAL, Aleksandra. How to tax Bitcoin? *In*: CHUEN, David Lee Kuo. **Handbook of Digital Currency**: Bitcoin, Innovation, Financial Instruments, and Big Data. Amsterdam: Elsevier, 2015. p. 267-282.
- BERTOLUCCI, Gustavo. Bitcoin com preço estável seria a nova revolução financeira? **Livecoins**, São Paulo, 2022. Disponível em: <https://livecoins.com.br/Bitcoin-com-preco-estavel-seria-a-nova-revolucao-financeira/#:~:text=O%20Bitcoin%20%C3%A9%20uma%20tecnologia,n%C3%A3o%20passe%20despercebido%20de%20cr%C3%ADticas>. Acesso em: 16 jul. 2023.
- BITCOIN USD (BTC-USD). **Yahoo Finance**, New York, 2023. Disponível em: <https://finance.yahoo.com/quote/BTC-USD?p=BTC-USD>. Acesso em: 19 ago. 2023.
- BRANDAO, Graziela. IN 1888 2019 – Obrigatoriedade de prestação de informações de operações com criptomoedas e criptoativos. **BL Consultoria**, [S.l.], 2019. Disponível em: <https://blconsultoriadigital.com.br/in-1888-2019/>. Acesso em: 2 ago. 2023.
- BRASIL. Banco Central do Brasil. **Fique por dentro**, Brasília. v. 4, n. 1, p. 5-31, 2008. Disponível em: [https://www.abscm.com.br/uploads/publicacoes/Banco%20Central%20do%20Brasil\\_Fique%20por%20dentro.pdf](https://www.abscm.com.br/uploads/publicacoes/Banco%20Central%20do%20Brasil_Fique%20por%20dentro.pdf). Acesso em: 13 ago. 2023.

BRASIL. **Instrução Normativa RFB nº 1888, de 03 de maio de 2019**. Institui e disciplina a obrigatoriedade de prestação de informações relativas às operações realizadas com criptoativos à Secretaria Especial da Receita Federal do Brasil (RFB). Brasília, 2019. Disponível em: <http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?idAto=100592>. Acesso em: 29 jul. 2023.

BRASIL. **Lei nº 9.613, de 3 de março de 1998**. Dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselho de Controle de Atividades Financeiras - COAF, e dá outras providências. Brasília, 1998. Disponível em: <https://www2.camara.leg.br/legin/fed/lei/1998/lei-9613-3-marco-1998-372359-publicacaooriginal-1-pl.html>. Acesso em: 29 jul. 2023.

BRASIL. **Lei nº 12.683, de 9 de julho de 2012**. Altera a Lei nº 9.613, de 3 de março de 1998, para tornar mais eficiente a persecução penal dos crimes de lavagem de dinheiro. Brasília, 2012. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_Ato2011-2014/2012/Lei/L12683.htm](https://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12683.htm). Acesso em: 29 jul. 2023.

BRASIL. **Lei nº 14.478, de 21 de dezembro de 2022**. Dispõe sobre diretrizes a serem observadas na prestação de serviços de ativos virtuais e na regulamentação das prestadoras de serviços de ativos virtuais; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para prever o crime de fraude com a utilização de ativos virtuais, valores mobiliários ou ativos financeiros; e altera a Lei nº 7.492, de 16 de junho de 1986, que define crimes contra o sistema financeiro nacional, e a Lei nº 9.613, de 3 de março de 1998, que dispõe sobre lavagem de dinheiro, para incluir as prestadoras de serviços de ativos virtuais no rol de suas disposições. Brasília, 2022. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2019-2022/2022/lei/L14478.htm](http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/L14478.htm). Acesso em: 29 jul. 2023.

BRASIL. Ministério da Fazenda. **Prevenção à lavagem de dinheiro e combate ao financiamento do terrorismo**. Brasília, 2023. Disponível em: <https://www.gov.br/fazenda/pt-br/assuntos/prevencao-lavagem-dinheiro>. Acesso em: 13 jul. 2023.

BUNTINX, Jean Pierre. Top 4 Cryptocurrency Projects Created Before Bitcoin. **The Merkle News**, San Francisco, 2016. Disponível em: <https://themerke.com/top-4-cryptocurrency-projects-created-ahead-of-bitcoin/>. Acesso em: 24 jul. 2023.

CABRAL, Felipe. Seis histórias intrigantes sobre as moedas digitais pré-Bitcoin. **MB Blog**, Barueri, 2023. Disponível em: <https://www.mercadobitcoin.com.br/economia-digital/criptomoedas/6-historias-intrigantes-sobre-moedas-pre-bitcoin/>. Acesso em: 24 jul. 2023.

CARVALHO, Fernando José Cardim de et al. **Economia monetária e financeira: teoria e política**. Rio de Janeiro: Elsevier, 2000.

CARVALHO, Patrícia Nasser de. Uma Análise Teórico-Crítica da Crise do Euro a partir da Teoria Cartalista da Moeda. **Revista OIKOS**, Rio de Janeiro, v. 16, n. 3, p. 6-21, 2017. Disponível em: <https://revistas.ufrj.br/index.php/oikos/article/view/51979/28268>. Acesso em 10 ago. 2023.

CARVALHO, Carla. Whitepaper: o que é e para que serve? **Yubb**, São Paulo, 2021. Disponível em: <https://yubb.com.br/artigos/conceitos/whitepaper-o-que-e-e-para-que-serve>. Acesso em: 3 ago. 2023.

CAVALCANTE, Beatriz de Sá. O que é dark net? **Jusbrasil**, [S.l.], 2018. Disponível em: <https://www.jusbrasil.com.br/artigos/o-que-e-dark-net/617613889>. Acesso em: 5 ago. 2023.

CHAINALYSIS. **The 2023 Crypto Crime Report**. New York, 2023. Disponível em: <https://go.chainalysis.com/2023-crypto-crime-report.html>. Acesso em: 29 jul. 2023.

CIRIACO, Douglas. O que é criptografia e por que você deveria usá-la. **Canaltech**, [S.l.], 2015. Disponível em: <https://canaltech.com.br/seguranca/o-que-e-criptografia-e-por-que-voce-deveria-usa-la/>. Acesso em: 28 jul. 2023.

CONSELHO DE CONTROLE DE ATIVIDADES FINANCEIRAS – COAF. **Relatório Integrado de Gestão 2022**. Brasília, 2023. Disponível em: <https://www.gov.br/coaf/pt-br/centrais-de-conteudo/publicacoes/publicacoes-do-coaf-1/rig-coaf-2022-publica-20230308.pdf>. Acesso em: 30 jul. 2023

COSTA, Fernando Nogueira da. **Economia Monetária e Financeira: Uma Abordagem Pluralista**. Campinas: Blog Cultura & Cidadania, 2020.

CROSBY, Michael et al. BlockChain Technology: Beyond Bitcoin. **Applied Innovation Review**, Berkeley, vol. 2, n. 1, p. 6-19, 2016. Disponível em: <https://j2-capital.com/wp-content/uploads/2017/11/AIR-2016-Blockchain.pdf>. Acesso em: 30 jul. 2023.

CRYPTO Mixers and AML Compliance. **Chainalysis**, New York, 2022. Disponível em: <https://blog.chainalysis.com/reports/crypto-mixers/>. Acesso em: 4 ago. 2023.

DALTO, Fabiano et al. **Teoria monetária moderna: A chave para uma economia a serviço das pessoas**. Fortaleza: Nova Civilização, 2020.

DORNELAS, Larissa Naves de Deus; TERRA, Fábio Henrique Bittes. Um percurso pela história das ideias: a moeda em Keynes. **Revista Geosul**, Florianópolis, v. 36, n. 80, p.145-169, 2021. Disponível em: <https://doi.org/10.5007/2177-5230.2021.e71751>. Acesso em: 5 jul. 2023.

DUQUE, Gabriel. Marco Legal das Criptomoedas: entenda o impacto da nova lei para as empresas do setor. **Idblog**, [S.l.], 2023. Disponível em: <https://blog.idwall.co/marco-legal-das-criptomoedas/#:~:text=Segundo%20o%20Marco%20Legal%20das,ou%20com%20pr op%C3%B3sito%20de%20investimento>. Acesso em: 2 ago. 2023.

EHA, Brian Patrick. **How money got free**: Bitcoin and the fight for the future of finance. London: Oneworld, 2017.

ESTELLITA, Heloisa. Criptomoedas e lavagem de dinheiro. Resenha de Johanna Grzywotz. Virtuelle Kryptowährungen und Geldwäsche. Berlin: Duncker & Humblot, 2019. **Revista Direito GV**, São Paulo, v. 16, n. 1, p. 1-13, 2020.

FERNANDES, Luciano Ferro. **O uso de moedas metálicas no Brasil**. [S.l.], 2018. Disponível em: [https://repositorio.animaeducacao.com.br/bitstream/ANIMA/11885/1/LUCIANO\\_FERRO\\_FERNANDES-%5B48358-11301-2-726943%5DO\\_uso\\_de\\_moedas\\_metalicas\\_no\\_Brasil.pdf](https://repositorio.animaeducacao.com.br/bitstream/ANIMA/11885/1/LUCIANO_FERRO_FERNANDES-%5B48358-11301-2-726943%5DO_uso_de_moedas_metalicas_no_Brasil.pdf). Acesso em: 24 jun. 2023.

FROYEN, Richard. **Macroeconomia**: Teorias e aplicações. 2. ed. São Paulo: Saraiva, 2013.

GALBRAITH, John Kenneth. **Moeda**: De onde veio, para onde foi. 2. ed. São Paulo: Pioneira, 1983.

GIROTTI, Vitor Guidorzi. **Moeda e Tecnologia**: uma análise a partir da Teoria Cartalista da Moeda. Araraquara, 2021. Disponível em: <https://agendapos.fclar.unesp.br/agenda-pos/economia/5529.pdf>. Acesso em: 10 set. 2023.

GRANT, Conor. A decade before crypto, one digital currency conquered the world — then failed spectacularly. **The Hustle**, [S.l.], 2018. Disponível em: <https://thehustle.co/beenz-pre-bitcoin-digital-currency/>. Acesso em: 23 jul. 2023.

GUIMARÃES, Ingrid; AGUIAR, Jady Mondeque de. Bitcoin: A Nova moeda internacional. In: SALÃO INTERNACIONAL DE ENSINO, PESQUISA E EXTENSÃO – SIEPE, 9., 2017, Santana do Livramento. **Anais [...]**. Santana do Livramento: Universidade Federal do Pampa, 2017. Disponível em: [https://guri.unipampa.edu.br/uploads/evt/arq\\_trabalhos/14793/seer\\_14793.pdf#:~:text=As%20criptomoedas%20surgiram%20ap%C3%B3s%20a,totamente%20digital%2C%20as%20chamadas%20criptomoedas](https://guri.unipampa.edu.br/uploads/evt/arq_trabalhos/14793/seer_14793.pdf#:~:text=As%20criptomoedas%20surgiram%20ap%C3%B3s%20a,totamente%20digital%2C%20as%20chamadas%20criptomoedas). Acesso em: 1 ago. 2023.

HARARI, Yuval Noah. **Uma Breve História da Humanidade Sapiens**. 7ª ed. Porto Alegre: L&PM Editores, 2016.

HE, Dong. Monetary Policy in the digital age. **Finance & Development**, Washington, 2018. Disponível em: <https://www.imf.org/Publications/fandd/issues/2018/06/central-bank-monetary-policy-and-cryptocurrencies-he>. Acesso em: 10 ago. 2023.

HILLBRECHT, Ronald O. **Economia monetária**. São Paulo: Atlas, 1999.

ICHIOKA, Mariana Tiemi; COIMBRA, Marina Teles. **As vantagens e características da criptomoeda Bitcoin**. Presidente Prudente, 2018. Disponível em: <http://intertemas.toledoprudente.edu.br/index.php/CONGRESSO/article/viewFile/6855/67646803>. Acesso em: 24 jul. 2023.

INSTITUTO DO PATRIMÔNIO HISTÓRICO E ARTÍSTICO NACIONAL – IPHAN. **Cnart**. Brasília, [201-]. Disponível em: <http://portal.iphan.gov.br/cnart/pagina/detalhes/1340>. Acesso em: 1 ago. 2023.

IVASCHENKO, Alla. Using Cryptocurrency in the Activities of Ukrainian Small and Medium Enterprises in order to Improve their Investment Attractiveness. **Problemi Ekonomiki**, Kyiv, v. 1, n.03, p. 267-273, 2016. Disponível em: <https://oaji.net/articles/2016/728-1479730699.pdf>. Acesso em: 25 jul. 2023.

KELLY, Brian. **The Bitcoin Big Bang: How Alternative Currencies Are About to Change the World**. New Jersey: Wiley, 2014.

KEYNES, John Maynard. **The collected writings of John Maynard Keynes: The General Theory of Employment, Interest and Money**. Cambridge: Macmillan, 1936.

KEYNES, John Maynard. **The collected writings of John Maynard Keynes: A treatise on money: the pure theory of money**. Cambridge: Macmillan, 1971.

KNAPP, Georg Friedrich. **The State Theory of Money**. London: Macmillan & Company Limited, 1924.

KRAUSE, Elliott. A Fifth of All Bitcoin Is Missing. These Crypto Hunters Can Help. **The Wall Street Journal**, New York, 2018. Disponível em: <https://www.wsj.com/articles/a-fifth-of-all-bitcoin-is-missing-these-crypto-hunters-can-help-1530798731>. Acesso em: 28 jul. 2023.

KURMANAEV, Anatoly; AVELAR, Bryan. A Poor Country Made Bitcoin a National Currency. The Bet Isn't Paying Off. **The New York Times**, New York, 2022. Disponível em: <https://www.nytimes.com/2022/07/05/world/americas/el-salvador-bitcoin-national-currency.html>. Acesso em: 19 ago. 2023.

LAVAGEM de dinheiro criptográfico: quatro endereços de depósito em bolsa receberam mais de US\$ 1 bilhão em fundos ilícitos em 2022. **DCiber**, Rio de Janeiro, 2023. Disponível em: <https://dciber.org/lavagem-de-dinheiro-criptografico-quatro-enderecos-de-deposito-em-bolsa-receberam-mais-de-us-1-bilhao-em-fundos-ilicitos-em-2022/>. Acesso em: 10 ago. 2023.

LOPES, João do Carmo; ROSSETTI, José Paschoal. **Economia Monetária**. 9ª ed. São Paulo: Atlas, 2005.

MALAR, João Pedro. Marco Legal das Criptomoedas entra em vigor no Brasil; veja mudanças para o setor. **Exame**, São Paulo, 2023. Disponível em: <https://exame.com/future-of-money/marco-legal-das-criptomoedas-entra-em-vigor-brasil/>. Acesso em: 2 ago. 2023.

MITCHELL, William; WRAY, Randall; WATTS, Martin. **Modern Monetary Theory and Practice: An Introductory Text**. New Castle: CreateSpace, 2016.

NIFA, Thalita. Peer-to-Peer (P2P): o que é, como negociar, é seguro? **iDinheiro**, Belo Horizonte, 2022. Disponível em: <https://www.idinheiro.com.br/investimentos/criptomoedas/peer-to-peer/>. Acesso em: 3 ago. 2023.

NOTÁRIO, Gabriel Bueno Fioravante. Proof of Work: O que é e Como Funciona. **Portal do Trader**, Santos, 2023. Disponível em: <https://portaldotrader.com.br/blog/criptomoedas/proof-of-work/>. Acesso em: 3 ago. 2023.

OLIVEIRA, Fabio Machado de; TOTTI, Maria Eugênia Ferreira; NEY, Vanuza de Silva Pereira. Bitcoin: o dinheiro com tecnologia de fonte aberta em rede ponto-a-ponto. *In*: ENCONTRO VIRTUAL DE DOCUMENTAÇÃO EM SOFTWARE LIVRE E CONGRESSO INTERNACIONAL DE LINGUAGEM E TECNOLOGIA ONLINE – EVIDOSOL/CILTEC-ONLINE, 11. e 8., 2014, Rio de Janeiro. **Anais [...]**. Rio de Janeiro: Universidade Estadual do Norte Fluminense; Universidade Federal Fluminense, 2014. Disponível em: [http://www.periodicos.letras.ufmg.br/index.php/anais\\_linguagem\\_tecnologia/article/view/5879](http://www.periodicos.letras.ufmg.br/index.php/anais_linguagem_tecnologia/article/view/5879). Acesso em: 18 jul. 2023.

OLIVEIRA, José Nuno Costa. **Aplicação da Tecnologia Blockchain na Área Financeira Portuguesa**. Lisboa, 2022. Disponível em: [https://repositorio.iscte-iul.pt/bitstream/10071/26276/1/master\\_jose\\_costa\\_oliveira.pdf](https://repositorio.iscte-iul.pt/bitstream/10071/26276/1/master_jose_costa_oliveira.pdf). Acesso em: 18 jul. 2023.

ORRELL, David; CHLUPATÝ, Roman. **The Evolution of Money**. Nova York: Columbia University Press, 2016.

OVERTURE, Benjamin. 7 Criptomoedas que Vieram Antes do Bitcoin. **Portal do Bitcoin**, [S.l.], 2017. Disponível em: <https://portaldobitcoin.uol.com.br/7-criptomoedas-que-vieram-antes-do-bitcoin/>. Acesso em: 23 jul. 2023.

PAIVA, Carlos Águedo Nagel; CUNHA, André Moreira. **Noções de Economia**. Brasília: Fundação Alexandre de Gusmão, 2008.

PAULSEN, Leandro. **Tratado de Direito Penal Tributário Brasileiro**. 2ª ed. São Paulo: Saraiva Jurídicos, 2023.

PAZ, André Vinícius Oliveira da; PAGLIUSO, Roberto Garcia Lopes. Aspectos criminais da Lei 14.478/2022: criptoativos e Direito Penal Econômico. **Boletim IBCCRIM**, São Paulo, v. 31, n. 365, p. 27-30, 2023.

POLANYI, Karl. **A subsistência do homem e ensaios correlatos**. Rio de Janeiro: Contraponto, 2012.

PRADO, Luiz Regis. **Curso de Direito Penal Brasileiro**. 11ª ed. São Paulo: Revista dos Tribunais, 2016.

PRYPTO. **Bitcoin for dummies**. New Jersey: John Wiley & Sons, 2016.

RAMOS, Samuel Ebel Braga. Lavagem de dinheiro: Aspectos históricos e processo de branqueamento de capitais. **Jusbrasil**, [S.I.], 2014. Disponível em: <https://www.jusbrasil.com.br/artigos/lavagem-de-dinheiro-aspectos-historicos-e-processo-de-branqueamento-de-capitais/129905516#:~:text=O%20m%C3%A9todo%20utilizado%20e%20batizado,dinheiro%20oriundo%20de%20atividade%20criminosa>. Acesso em: 10 jul. 2023.

SHARMA, Rakesh. What Is Decentralized Finance (DeFi) and How Does It Work? **Investopedia**, [S.I.], 2022. Disponível em: <https://www.investopedia.com/decentralized-finance-defi-5113835>. Acesso em: 5 ago. 2023.

SICHEL, Ricardo Luiz; CALIXTO, Sidney Rodrigues. Criptomoedas: impactos na economia global. Perspectivas. **Revista de Direito da Cidade**, Rio de Janeiro, v. 10, n. 3, p. 1622-1641, 2018. Disponível em: <https://www.e-publicacoes.uerj.br/index.php/rdc/article/view/33096>. Acesso em: 5 ago. 2023.

SILVA, Marcos Eugênio da. O Conceito de Moeda em Keynes e a Circulação Financeira. **Estudos Econômicos**, São Paulo, v. 17, n. 3, p. 333-348, 1987. Disponível em: <https://www.revistas.usp.br/ee/article/view/157400/152760>. Acesso em: 29 jul. 2023.

SILVA, Simone da; ALBUQUERQUE, Vanessa. **Descobrendo a BITCOIN**. São Paulo: Novatec, 2017.

TELLES, Christiana Mariani da Silva. **Bitcoin, Lavagem de Dinheiro e Regulação**. Curitiba: Juruá, 2020.

TRELEAVEN, Philip; BROWN, Richard Gendal; YANG, Danny. Blockchain Technology in Finance. **IEEE Computer Society**, Washington, v. 50, n. 9, p. 14–17, 2017. Disponível em: <https://ieeexplore.ieee.org/document/8048631/metrics#metrics>. Acesso em: 28 jul. 2023.

ULRICH, Fernando. **Bitcoin - A moeda na era digital**. São Paulo: Instituto Ludwig von Mises Brasil, 2014.

UNITED NATIONS OFFICE ON DRUGS AND CRIME – UNODC. **Money Laundering**. [S.I.], 2023. Disponível em: <https://www.unodc.org/unodc/en/money-laundering/overview.html>. Acesso em: 2 ago. 2023.

UNIVERSITY OF CAMBRIDGE. **Cambridge Bitcoin Electricity Consumption Index**. Cambridge, 2023. Disponível em: <https://ccaf.io/cbnsi/cbeci>. Acesso em: 20 ago. 2023.