



PUC-SP

**PONTIFÍCIA UNIVERSIDADE CATÓLICA DE SÃO PAULO
FACULDADE DE CIÊNCIAS ECONÔMICAS, ADMINISTRAÇÃO,
CONTABILIDADE E ATUARIAIS**

DAVI LIMA MOYA

ANÁLISE SOBRE O BITCOIN: A MOEDA DISSIDENTE

MONOGRAFIA DE BACHARELADO EM CIÊNCIAS ECONÔMICAS

SÃO PAULO

2023

DAVI LIMA MOYA

ANÁLISE SOBRE O BITCOIN: A MOEDA DISSIDENTE

Monografia submetida à apreciação de banca examinadora do Departamento de Economia, como exigência parcial para a obtenção do grau de Bacharel em Ciências Econômicas, elaborada sob a orientação do Professor Doutor Antônio Carlos de Moraes.

SÃO PAULO

2022

PÁGINA DE APROVAÇÃO

Esta monografia foi examinada pelos professores abaixo relacionados e aprovada com nota final _____ (_____).

Nomes legíveis dos examinadores (orientador e demais membros da banca)

O autor desta obra autoriza sua publicação eletrônica na Biblioteca Digital da PUCSP. Este trabalho é somente para uso privado de atividades de pesquisa e ensino. Não é autorizada sua reprodução para quaisquer fins lucrativos. Esta reserva de direitos abrange a todos os dados do documento bem como seu conteúdo. Na utilização ou citação de partes do documento é obrigatório mencionar nome da pessoa autora do trabalho e demais itens da referência bibliográfica.

Moya, Davi Lima.

Análise sobre o Bitcoin: a moeda dissidente / Davi Lima Moya – São Paulo, 2023, 32 p.

Trabalho de Conclusão de Curso de Graduação em Ciências
Econômicas

Orientador: Antonio Carlos de Moraes

1. Bitcoin 2. Sistema Financeiro 3. Monetarismo.

Pontifícia Universidade Católica de São Paulo

Faculdade de Economia, Administração, Contabilidade e Atuariais

AGRADECIMENTOS

Obrigado a minha família por me proporcionar os momentos que me formaram como pessoa.

Obrigado a meus professores pela inspiração e educação.

Obrigado a Simone por me incentivar a acreditar em mim mesmo.

RESUMO

O presente trabalho avalia o impacto do Bitcoin como ativo criptográfico descentralizado e pondera seu potencial como alternativa de meio de pagamento perante o sistema monetário convencional. Constatou-se que a criptomoeda não possui os requisitos para ser utilizada em escala frente aos parâmetros cambiais centralizados como os quais operam na atualidade. É feita uma perspectiva das medidas e competências cabíveis às autoridades e instituições monetárias a fim de demonstrar as deficiências que esse tipo de ativo possui caso sofra com instabilidades e, portanto, não tenha a possibilidade de contar com qualquer intervenção externa. Consequentemente, há também uma análise de seu uso crescente em atividades ilícitas como lavagem de dinheiro e tráfico de drogas medindo o aspecto de sua influência na contribuição do crime organizado.

Palavras-chave: Bitcoin. Criptomoeda. Sistema monetário. Autoridades monetárias. Lavagem de dinheiro.

ABSTRACT

The present paper evaluates the impact of Bitcoins as an decentralized cryptographic asset and ponders its potential as an alternative currency towards our monetary system. The main finding was that cryptocurrency does not require what is needed to be utilized in scale as the centralized exchange parameters are used today. First, it is given a perspective of what monetary authorities are capable of doing, in order to demonstrate its flaws in case it suffers any instability and therefore has no possibility to count with external interventions. According to our research, it will also be analyzed for its growing utilization in money laundering and drug traffic, measuring the aspect of its contribution to organized crime.

Keywords: *Bitcoins. Cryptocurrency. Monetary system. Monetary authorities. Money Laundering.*

SUMÁRIO

1 INTRODUÇÃO	8
2 SURGIMENTO DAS CRIPTOMOEDAS:NASCIMENTO DO BITCOIN ...	10
2.1 <i>SECURE HASH ALGORITHM (SHA)</i>	12
2.2 A “CADEIA DE BLOCOS”	13
2.3 MINERAÇÃO	16
2.4 <i>EXCHANGES</i>	17
2.5 MOEDA VERSUS CRIPTOMOEDA.....	19
3 INTRODUÇÃO AO SISTEMA MONETÁRIO CENTRALIZADO.....	23
3.1 SISTEMA FINANCEIRO INTERNACIONAL	26
3.2 VULNERABILIDADE FUNCIONAL	28
4 IMPACTO ECONÔMICO DA MOEDA DIGITAL	29
4.1 REGULAÇÃO DAS CRIPTOMOEDAS	30
4.2 LAVAGEM DE DINHEIRO.....	32
5 CONSIDERAÇÕES FINAIS	34
REFERÊNCIAS	36

1 INTRODUÇÃO

O Bitcoin e as criptomoedas em geral são ativos virtuais descentralizados que trouxeram a possibilidade de transações com taxas ínfimas de realização e de grande rapidez mesmo que realizadas em escala intercontinental. Seu cerne está retido na eliminação da terceira parte que intercala as transações convencionais representada pela sociedade dos Grandes Bancos, garantindo uma maior autonomia no que convêm ao comprador e vendedor que utilizam do novo método. Possuem características de moeda, como escassez e aceitação de mercado, mas não podem ser consideradas como tal, principalmente por não deter lastro e, portanto, não ser regulamentada por uma autoridade como um Banco Central como acontece no sistema monetário centralizado como conhecemos.

Por esse motivo, o presente trabalho terá como objetivo demonstrar as falhas que o Bitcoin apresenta quando analisado sobre a perspectiva muitas vezes de caráter liberal de que poderíamos em um futuro próximo considerá-lo uma moeda de caráter confiável, apontando as grandes controvérsias que sua própria existência reproduz. Para tal, é necessário ter em mente também o atual nível de desenvolvimento e características do sistema monetário centralizado que opera socialmente. Tarefa esta que será realizada a fim de demonstrar as competências que autoridades monetárias e instituições financeiras detém diante dos problemas de oferta, fluidez e oscilação de valor de uma moeda. Realizada essa tarefa, identificá-lo-emos como o ativo financeiro que carrega seu potencial de tamanha vastidão, mas que no nível do sistema monetário centralizado como o que conhecemos, mais representa os anseios de uma parcela social determinada a se rebelar do sistema do que uma alternativa viável para uma modernização dos meios de pagamento convencionais.

No primeiro capítulo, farei uma análise sobre o funcionamento das criptomoedas a partir do nascimento do Bitcoin, trazendo à tona as características da *Blockchain* e da mineração de novas moedas que determina o volume de circulação do ativo. Também será construído ao final do capítulo, uma linha de raciocínio referente as diferentes faces do monetarismo, a fim de buscar coerências e incoerências quando se analisa as criptomoedas na ótica da teoria econômica.

Será feita uma apresentação do sistema financeiro nacional a fim de demonstrar como funciona a relação das instituições financeiras com o mercado de capitais e os grandes bancos, que possuem uma dinâmica semelhante ao funcionamento das *exchanges*, que são as corretoras responsáveis pela comercialização das criptomoedas em geral, trazendo à tona











então as regulamentações e medidas cabíveis em cenários de incerteza acentuada e fragilidade.

2 SURGIMENTO DAS CRIPTOMOEDAS: O NASCIMENTO DO BITCOIN

O Bitcoin é um ativo criptográfico que teve surgimento em 2008 (NAKAMOTO, 2008), completamente digital e descentralizado, e utiliza do funcionamento de uma tecnologia chamada *Blockchain* para a concretização de sua existência perante encriptação de mensagens por meio de algoritmos. Essa ferramenta detém o histórico de toda e qualquer transação realizada, fornecendo assim o registro contábil eficiente destas. Foi a primeira tendência do novo padrão de criptoativos e é um exemplo deste modelo inovador e, como não é um recurso criado por qualquer governo ou entidade econômica o seu valor é determinado livremente pelos indivíduos no mercado. Seu desenvolvimento ocorreu por parte de um usuário de codinome Satoshi Nakamoto por meio de um *white paper* em um fórum aberto (ULRICH, 2017, p. 11). Em dois anos sua validade no mercado garantia-o paridade com o dólar americano.

Na atualidade existe uma grande variedade de criptomoedas comercializadas no mercado (Figura 1), porém nem sempre seu funcionamento é garantido devido a fatores que devem ser correspondidos, como: o fato da moeda não poder ser usualmente detida de forma proprietária por uma empresa comercial e apresentar um ponto centralizado de falha, não superar o problema do “gasto duplo”(quando uma mesma moeda é utilizada mais de uma vez em diferentes transações em um dado sistema de criptomoedas), ou mesmo que por algum motivo não possua escassez (ULRICH, 2017, p 12).

FIGURA 1 - PRINCIPAIS CRIPTOMOEDAS

#	Nome	Código	Preço (USD)	Capitalização	Vol. (24h)	Vol. Total	Var (24h)	Var (7d)
1	 Bitcoin	BTC	22.711,1	\$431,64B	\$55,17B	43,32%	+2,58%	-25,10%
2	 Ethereum	ETH	1.237,12	\$149,23B	\$37,74B	29,63%	+1,35%	-31,29%
3	 Tether	USDT	1,0004	\$70,79B	\$89,58B	70,33%	+0,01%	-0,03%
4	 USD Coin	USDC	1,0012	\$54,26B	\$10,84B	8,51%	-0,01%	+0,02%
5	 BNB	BNB	234,4	\$38,05B	\$2,27B	1,78%	+6,26%	-19,08%
6	 Cardano	ADA	0,5337	\$18,01B	\$2,36B	1,85%	+11,28%	-16,34%
7	 Binance USD	BUSD	1,0013	\$17,67B	\$8,42B	6,61%	0%	+0,17%
8	 XRP	XRP	0,34217	\$16,48B	\$2,26B	1,78%	+6,19%	-14,83%
9	 Solana	SOL	35,233	\$11,99B	\$2,67B	2,10%	+17,48%	-9,78%
10	 Polkadot	DOT	8,37	\$8,23B	\$1,07B	0,84%	+9,13%	-7,36%

Fonte: Investing.com (2022)

Como pode-se compreender pela tabela, a cotação em dólar do Bitcoin (BTC) e do Ethereum (ETH), superam consideravelmente o valor das outras criptomoedas, demonstrando como esses ativos são facilmente influenciados por tendências de mercado, quando observada a atenção que esses ativos ganham por meio dos principais perfis que lidam com a disponibilização de informação sobre criptomoedas em redes sociais como o *Twitter*. Uma análise feita por meio de uma plataforma chamada Streamr de 10 a 16 de março de 2023, teve como objetivo identificar qual seria a criptomoeda mais mencionada em *tweets*, filtrando e categorizando entre milhões destes por meio do banco de dados do *Twitter* (CRYPTONOMIST, 2023). O resultado identificou o Bitcoin como a criptomoeda mais falada na rede social, alcançando a marca de mais de 1.6 milhões de *tweets* no período estudado, comparado a meros poucos mais de 400 mil sobre Ethereum que ocupou o terceiro lugar no ranking.

Uma problemática que vem sendo enfrentada nos últimos anos é a associação do Bitcoin nos pagamentos das transações de tráfico como no servidor chamado *Silk Road*, ambiente virtual da *Dark Web* criado especificamente para a realização de atividades ilícitas com possibilidade de pagamento na criptomoeda.

Also, bitcoin and crime have been associated, as seen in the Silk Road case, where users sought to exploit the digital currency's anonymity to sell drugs and launders money. Some worry, too, that bitcoin could foment economic crises because it strips government policymakers of the capacity to adjust the money supply and to offset people's instinct to hoard it at times of mass panic. (VIGNA & CASEY, 2015, p. 16).

Ross Ulbricht, estadunidense com o codinome “*Dread Pirate Roberts*” em meio aos *cyber* traficantes, confessa em 2015 que foi o criador da *Silk Road* e é condenado por sete crimes, entre eles lavagem de dinheiro e tráfico de drogas (PORTAL DO BITCOIN, 2023). Ulbricht foi pego em flagrante utilizando o servidor da *Silk Road* em uma biblioteca pública em São Francisco, assim possibilitando que o FBI fizesse o rastreamento de sua atividade. Quando condenado, admitiu portar mais de 140 mil Bitcoins (hoje valendo cerca de R\$ 3,4 Bilhões no mercado) que foram apreendidos pela USMS (*U.S. Marshals Service*), agência americana responsável por resguardar produtos oriundos do crime.

O anonimato e a rapidez transacional intercontinental conferido pelo funcionamento interno da tecnologia da Blockchain exemplificado por Nakamoto (2008) abre a possibilidade

para a utilização do ativo em atividades ilícitas por dificultar o rastreamento das transações, assim contribuindo para a perpetuação do crime organizado.

2.1 SECURE HASH ALGORITHM (SHA)

Devido aos avanços da criptografia de informações nas últimas décadas, a Agência Nacional de Segurança dos Estados Unidos (NSA) desenvolveu este conjunto de sistema de *hash* (impressão digital) que têm por função gerar códigos com os quais documentos e dados podem ser protegidos contra qualquer ataque externo ou agente que deseja modificá-los, garantindo maior privacidade no processamento de informações. Existem três gerações de protocolos SHA: o SHA-0, SHA-1 e SHA-2. Cada um corresponde a um conjunto de algoritmos criptográficos que, com o passar dos anos e o desenvolvimento da tecnologia, houve também a criação de novas variantes dos mesmos, e assim se dá a evolução destes conjuntos.

O SHA-256 é o algoritmo pelo qual Satoshi Nakamoto tomou como exemplo para o desenvolvimento do sistema de proteção da Blockchain, o *proof-of-work*, e se encontra no último sistema de variantes, SHA-2, ou seja, o mais desenvolvido. Desta forma, se demonstra notável o elevado nível da criptografia formadora da base que garante a integridade do funcionamento das transações das moedas. Podemos observar sua própria explicação sobre o mecanismo da “*proof-of-work*” em um trecho do documento “*Bitcoin: a peer-to-peer Electronic Cash System*”:

To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hashcash [6], rather than newspaper or Usenet posts. The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash. For our timestamp network, we implement the proof-of-work by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits. Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it. (NAKAMOTO, 2008, p. 3)

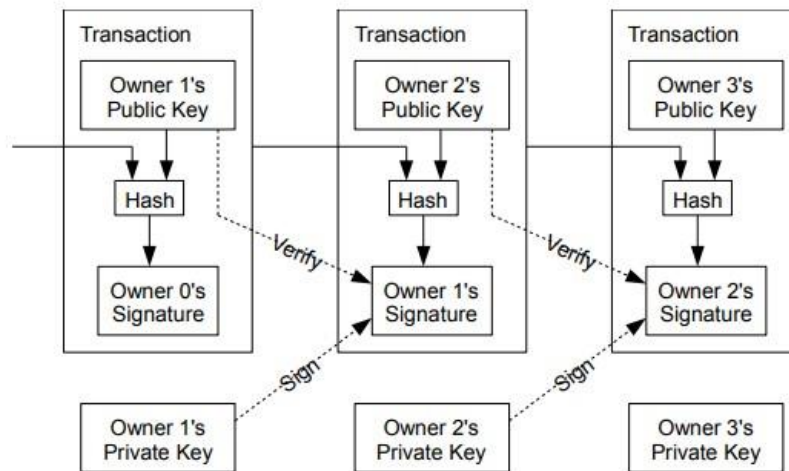
O esquema nomeado de *proof-of-work* demonstrado por Nakamoto nada mais é do que a explicação de como funciona a “mineração” do Bitcoin, e será abordado de forma mais elaborada no tópico “2.3 MINERAÇÃO”. Explica como funciona a verificação da transação que irá adentrar para a cadeia da Blockchain por meio do “esforço da CPU” que é o cálculo que os mineradores precisam fazer com computadores de alta performance para resolver o cálculo exponencial necessário da “hash” (fração) em questão.

2.2 A “CADEIA DE BLOCOS”

Como foi comentado acima, o criador do Bitcoin e da Blockchain desenvolveu um manual, explicando como ocorreu o processo de criação do sistema de criptografia das informações e como ele funciona, assim como os elementos que garantem sua integridade e segurança. Neste capítulo analisarei a fundo esses processos demonstrados no arquivo “*Bitcoin: A peer-to-peer Electronic Cash System*” de forma a buscar um maior entendimento sobre esta ferramenta que possui um grande potencial para administração de informações não só no quesito das moedas digitais, mas como será visto, poderá ser aplicado em diversos outros setores que podem se beneficiar da otimização de tempo, processos e de sua segurança. Como por exemplo: arquivar ou compartilhar músicas, arte, votos, documentos de identificação, prontuários médicos, históricos escolares, diplomas, registros de automóveis ou imóveis, etc. Além do Bitcoin, hoje a tecnologia da Blockchain também é usufruída pelas outras criptomoedas que existem no mercado.

O sistema de funcionamento da Blockchain é inovador e foi desenvolvido com o propósito de garantir a utilização de uma moeda sem que haja a mediação de uma terceira parte, uma autoridade central, garantindo maior autonomia nas ações do comprador e do vendedor. Cada transação que ocorre dentro do sistema possui um fragmento da anterior, uma assinatura que possui uma chave de acesso em cada uma das partes para garantir a segurança da cadeia como um todo. Em seu white paper *Bitcoin: a peer-to-peer electronic cash system* Nakamoto exemplificou em um diagrama essa funcionalidade da cadeia de blocos como representado na Figura 2:

FIGURA 2 – TRANSAÇÕES EM BITCOIN



Fonte: NAKAMOTO (2008)

Este esquema demonstra como funciona o processo de conexão de cada transação da Blockchain, de forma que a atual sempre carregará consigo uma parte (Assinatura digital) da anterior e assim em diante. É desta forma que acontece também o processo inicial de verificação da transação antes mesmo da mineração.

We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership. (NAKAMOTO, 2008, p. 2)

A partir da análise do funcionamento do mecanismo da blockchain, o próprio Nakamoto identificou um problema de “gasto duplo” que invalidaria a performance da moeda em seu sentido próprio, visto que não se encaixaria mais nos critérios necessários para ser enquadrada como tal, e sendo assim perdendo seu valor. A central de confiança (*proof-of-work*) em questão foi aderida no sistema como mediadora para evitar o problema de gasto duplo que criaria *gaps* de funcionamento da *Blockchain*, permitindo que os usuários que utilizassem desta manobra se beneficiassem de forma corrupta. Segundo Nakamoto (2008): “*The problem of course is the payee can't verify that one of the owners did not double-spend the coin. A common solution is to introduce a trusted central authority, or mint, that checks every transaction for double spending*”

Desta forma, ela verifica se todas as transações estão livres de gastos duplos, agindo como a terceira parte que faz a mediação das transações, ou seja, da mesma forma do sistema que conhecemos na atualidade, mediada por instituições bancárias.

To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes. We will show later that the probability of a slower attacker catching up diminishes exponentially as subsequent blocks are added. (NAKAMOTO, 2008, p. 3)

É admirável a engenhosidade deste sistema criptográfico quando analisado este trecho do documento: “Para modificar um bloco anterior da cadeia, um invasor teria que reproduzir a *proof-to-work* do bloco e de todos os outros anteriores a ele para só então alcançar e conseguir ultrapassar o trabalho dos *honest nodes*”. No entanto, não elimina completamente a possibilidade de ataques exteriores de hackers como foi visto em larga escala em 2022.

De acordo com um levantamento feito pela empresa de inteligência em Blockchain TRM Labs, 2022 foi um ano recorde em ataques de hackers no qual a soma de toda a quantia roubada alcança a marca dos U\$ 2,76 Bilhões (COINTELEGRAPH, 2023). Este dado representa somente 75% do total que fora alvo dos criminosos, caso tivessem sucesso como um todo o montante seria elevado para cerca de U\$ 3,7 Bi. Os maiores alvos dos crimes foram protocolos que envolviam finanças descentralizadas (DeFi), que se encontram em maior volume de aplicações em Ethereum, visto que fora a primeira *exchange* a oferecer este tipo de serviço. As aplicações em DeFi surgiram com o intuito de criar um ambiente bancário descentralizado em que qualquer usuário pode realizar negociações executados por algoritmos e *smart contracts*, o que reduz o esforço das duas partes já que suas obrigações já estão pré-definidas por um modelo, e não se necessita da intermediação de uma terceira parte. (INFOMONEY, 2023) De acordo com o levantamento feito pela empresa, dos 10 maiores roubos que ocorreram, em 5 deles *hackers* visaram algum tipo de brecha de infraestrutura, e 3 deles foram viabilizados através de falhas no código dos projetos. Segundo Nakamoto (2008, p. 4): “*The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended.*”

Foi a partir deste entendimento que houve a criação da expressão “minerar bitcoins”, Nakamoto fez a analogia comparando a adição constante de novas moedas com a utilização de recursos por parte dos mineradores de ouro para adicioná-lo em circulação.

2.3 MINERAÇÃO

A mineração de criptomoedas como Bitcoin (BTC), Ethereum (ETH) e Dogecoin (DOGE) é feita por meio da competição de pessoas neste mercado utilizando softwares e hardwares específicos como os chamados circuitos integrados de aplicação específica (ASIC) a computadores de alta performance para encontrar a *hash* do bloco que necessita de validação na Blockchain. A cada 10 minutos em média, é adicionado 1 bloco à cadeia da Blockchain, e os mineradores são responsáveis por verificar a validade dos dados de cada bloco. A cada bloco minerado, é passível do recebimento de 6,25 bitcoins por parte das pessoas que realizam o trabalho de validação de dados, cerca de R\$1,7 milhão.

Devido a elevada migração de mineradores para este setor aumentando a carga de pessoas em um mesmo bloco da cadeia realizando as operações para calcular o código de sua assinatura digital, isto sobrecarrega o sistema, fazendo com que esta tarefa exige cada vez mais esforço de CPU e conseqüentemente gasta muito mais energia, favorecendo a formação de “fazendas” para realizar todo o trabalho. Este tipo de associação garante cada vez mais a competitividade do mercado já que o desenvolvimento tecnológico agregado ao setor está sempre atrelado, para garantir que os cálculos sejam feitos em menor tempo garantindo a remuneração dos agentes que recebem em fragmentos de bitcoins pelo serviço prestado.

Para garantir que a moeda tenha um bom funcionamento no mercado, foi necessário a implementação de um processo que foi denominado como *halving*. Consiste basicamente em reduzir pela metade a remuneração das pessoas que são responsáveis por minerar bitcoins periodicamente, quando se alcança o marco de 210.000 blocos validados na blockchain a cada ciclo - geralmente dura cerca de 4 anos.

Em 2009, o sistema recompensava mineradores com 50 BTC a cada 10 minutos. Três *halvings* depois, a quantidade foi reduzida para 6,25 BTC a cada 10 minutos. O processo terminará quando o número de BTC em circulação atingir 21 milhões. Estima-se que isso ocorrerá em algum momento próximo ao ano de 2140. (INFOMONEY, 2022).

Sendo assim, Nakamoto foi capaz mais uma vez de garantir uma propriedade do Bitcoin que permitiria uma semelhança ao comportamento de uma moeda em um sistema monetário centralizado, a sua escassez. Apesar de não possuir lastro ou vínculo com instituições financeiras e autoridades monetárias, mas por outro lado ter sua comercialização em Bolsas de Valores independentes chamadas de corretoras spot ou “*exchanges*”, a nova moeda digital possui uma grande visibilidade e procura no mercado, abrindo muitas portas para processos inovadores e estabelecendo um novo mercado cheio de oportunidades.

2.4 EXCHANGES

As *exchanges* são também chamadas de corretoras, e podem ser explicadas como plataformas especializadas na comercialização e custódia de carteiras de criptomoedas de seus respectivos clientes investidores. Elas fazem a intermediação nas transações de moedas digitais, seja na compra, venda ou troca de ativos cobrando uma taxa de administração para manter a plataforma em funcionamento. (INFOMONEY, 2023)

A receita federal define as *exchanges* como: “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.” (INFOMONEY, 2023)

A priori funcionam como uma bolsa de valores independente, porém não contam com o resguardo da CVM ou do Banco Central. Portanto, se houver problemas de liquidez dos ativos ou qualquer contrapartida ética referente aos padrões de comportamento das sociedades não cabe a qualquer autoridade intervir e manipular de qualquer forma os dados e informações das operações ou carteiras dos clientes.

Na atualidade existem um grande número de *exchanges* no mercado como pode-se conferir a partir da Figura 3:

FIGURA 3: AS 10 MAIORES EXCHANGES DO MERCADO

#	Corretora	Pontuação	Trading volume(24h)	Liquidez Méd.	Visitas Semanais	# Mercados	# Moedas	Fiat Suportada	Gráfico de Volume (7d)
1	Binance	9.9	R\$29,942,836,079	877	9,171,524	1606	385	EUR, GBP, BRL and +8 more	
2	Coinbase Exchange	8.6	R\$5,906,262,616	814	46,700	477	244	USD, EUR, GBP	
3	Kraken	8.3	R\$2,667,885,506	774	931,514	765	240	USD, EUR, GBP and +4 more	
4	KuCoin	7.4	R\$1,357,258,540	575	1,036,917	1313	727	USD, AED, ARS and +45 more	
5	Bybit	7.4	R\$5,733,090,904	675	2,871,254	655	441	USD, EUR, GBP and +3 more	
6	OKX	7.3	R\$4,743,486,526	649	5,033,122	698	325	AED, ARS, AUD and +43 more	
7	Bitstamp	7.1	R\$989,369,487	586	189,421	170	78	USD, EUR, GBP	
8	Bitfinex	6.9	R\$382,952,898	579	126,194	405	183	USD, EUR, GBP and +1 more	
9	Gate.io	6.9	R\$2,948,523,307	592	2,730,832	3023	1768	EUR, USD, GBP and +19 more	
10	HTX	6.7	R\$5,471,792,929	431	2,145,920	769	607	ALL, AUD, BRL and +47 more	

Fonte: Coin Market Cap (2023)

A que possui um maior volume de transações é a Binance, alcançando em um dia quase R\$ 30 Bilhões, mesmo não detendo uma liquidez média tão abaixo do segundo lugar ocupado pela Coinbase Exchange, a diferença de seu volume de transação diário para o da corretora número um é significativo, cerca de 24 Bilhões de reais.

Um acontecimento que marcou imensamente a história do Bitcoin foi a quebra da segunda maior *exchange* que operava no mercado em 2022, a FTX. Seu fundador e CEO, Sam Bankman-Fried foi capaz em poucos anos construir um império de mais de cem empresas valendo um montante de U\$32 Bilhões e contando com aproximadamente 130 subsidiárias e startups investidas. (VALOR ECONÔMICO, 2023)

Quando o Bitcoin e as demais criptomoedas subiam, era possível exprimir ganhos substanciais nas carteiras dos clientes da plataforma, visto que a Alameda Research, empresa de programação de algoritmos de investimento de criptomoedas que fundou antes de abrir a FTX, prometia a alavancagem de 20 vezes o valor do capital e tesouraria. No entanto, quando houve a grande desvalorização dos criptoativos em 2020, os prejuízos foram avassaladores com a mesma intensidade que se obtinham os ganhos. Levando assim, em 2022 a um processo

judicial devido a sua falência, indicando que deve a seus 50 maiores credores uma quantia de extremos U\$ 3,1 Bilhões (BBC, 2023).

2.5 MOEDA VERSUS CRIPTOMOEDA

Agora que conhecemos o nascimento do Bitcoin e podemos compreender seu funcionamento, a dúvida que ainda assombra muitos de seus investidores e estudiosos é: Podemos considerá-lo como uma moeda? Se sim, como é possível confiar em seu valor? Se não, é possível que seja só uma questão de tempo até que possa ocupar esse lugar ou permanecerá dessa forma?

Não existe outra forma de expressar a dedução que se decorre a essas dúvidas a não ser com um clichê: “Só o tempo dirá”. No momento, como foi repetidamente elucidado neste trabalho, e dado como um consenso no meio acadêmico é o fato de que o Bitcoin e as demais criptomoedas não podem ser considerados como moeda, mas sim como ativos geralmente utilizados como meio de investimento. Elas não possuem lastro, portanto seu valor não tem base em nenhum tipo de metal precioso como já foi a libra-esterlina ou o dólar, portanto seu preço quando convertido obedece somente a lei de oferta e procura. Sua regularização e emissão não é vinculada a um banco central ou qualquer banco específico, sendo que sua venda, compra ou troca é feita por intermédio das plataformas chamadas de *exchanges*, dessa forma se houver queda de sua liquidez no mercado não há qualquer forma de intervir. Assim como em processos investigativos feito pela polícia envolvendo tráfico de drogas e lavagem de dinheiro é uma tarefa significativamente mais árdua refazer os passos dos criminosos a fim de localizar e confiscar as quantias fruto das atividades ilícitas visto que dentro da Blockchain não há a possibilidade de rastrear da mesma forma como é feito no caso da utilização de paraísos fiscais por exemplo.

No entanto, existe a possibilidade de que em um futuro próximo possa haver a aceitação das criptomoedas de uma forma geral, aumentando seu potencial como meio de troca e de certa forma derrubando algumas das barreiras referentes a sua regularização. Há um percentual da população que acredita fielmente nessa hipótese, como a comunidade cyberpunk que são ativistas de visão tecnológica que tiveram notoriedade na década de 1990 ao utilizar ferramentas de privacidade criptográfica como forma de revolução, e ainda teóricos neoliberais em geral também possuem aspirações que se assemelham às condições de liberdade garantidas pelo desvencilhamento do dinheiro dos grandes bancos e do governo como um todo, assim como o anonimato garantido pelo mecanismo da Blockchain. De acordo

com Vigna e Casey (2019, p. 29): “If citizens don’t trust a government to represent their interests, they won’t trust its currency—or better put, they won’t trust the monetary system around which their economy is organized.”

Paul Vigna e Michael Casey (2015) afirmam que as crises constantes em nossa sociedade são de responsabilidade de cada governo, e que a relação conflituosa deste com a população reflete essas falhas, causando uma desconfiança dos civis, assim tornando mais suscetível que haja a introdução de um novo padrão monetário como forma de revolução.

Em função da teoria econômica, é possível distinguir algumas definições de moeda de acordo com suas respectivas teorias monetárias. Dentre elas, a distinção feita por Mollo (2004) possibilitou categorizar entre ortodoxia e heterodoxia quanto a aceitação da Lei de Say ou da Teoria Quantitativa da Moeda (TQM), desenvolvida inicialmente por Irving Fisher, buscava relacionar o nível de preços médio com a quantidade de dinheiro na economia ($M*V=P*Y$. Sendo M= quantidade de dinheiro; V= velocidade de circulação; P= nível de preços e Y= produto real da economia).

Há uma parcela da ortodoxia que se baseia na Lei de Say - há um resultado harmônico de equilíbrio de mercados - e leva em consideração que a moeda é um instrumento de fator exógeno à economia, ou seja, sua ação é neutra e têm a propriedade de equilibrar o mercado de bens e fatores. Diferenciando-se de uma visão heterodoxa que acredita na TQM e se contrapõe à Lei de Say admitindo que a moeda tem efeito endógeno em relação à economia, e que existem instabilidades na demanda, como exemplo os efeitos do entesouramento na produção que causam sua influência sobre as demais variáveis reais, indicando sua não-neutralidade e consequente incompatibilidade no controle de quantidade de moeda corrente por parte do Banco Central. Neste contexto, a não-neutralidade da moeda pode ser explicada também pela atuação do crédito na esfera financeira, que tem a função de potencializar a produção real por meio da viabilização do investimento, mas que no entanto, não se encontra sob controle de decisões absoluto da Autoridade Monetária em questão.

A teoria Marxista se encontra no espectro heterodoxo do monetarismo teórico e traz a tona um aspecto materialista da moeda frente a sua característica de relação mercantil, diferenciando o valor de uso e de troca de todas as mercadorias, e na qual pode-se desprender diferentes faces do dinheiro que opera em meio de relação social, como instância realizadora do capital.

Então, mercadoria determinada, com cuja forma natural se identifica socialmente a forma de equivalente, torna-se mercadoria-dinheiro, funciona como dinheiro.

Desempenhar o papel de equivalente universal torna-se sua função social específica, seu monopólio social, no mundo das mercadorias. (MARX, 1867, p. 91).

O dinheiro como equivalente geral, ou seja, mercadoria-dinheiro se compreende independentemente de seu valor de troca, garantindo seu balanço frente a qualquer outra mercadoria como medida de valor. Sua segunda face é a de meio de circulação, ou seja, a característica que permite que a função de valor seja de fato efetivada através da venda, sendo nessa categoria administradas mais três a partir desse conceito: i) meio de entesouramento ou reserva de valor; ii) meio de pagamento; e iii) dinheiro mundial. (MALDONADO FILHO, 1997) A função de reserva de valor diz respeito ao reconhecimento do dinheiro como valor por excelência, e portanto desejado como tal. Já como meio de pagamento, explicita que não há necessidade da atuação física da mercadoria dinheiro, visto que seu preço é estabelecido por operação contábil, apesar de servir como cobertura de saldos quanto a validação social do valor. Quanto à terceira característica pode-se exprimir sua aceitação de forma mundial, ou seja, seu reconhecimento social como valor.

Em seu Tratado sobre a Moeda, que também se delimita a heterodoxia em meio as teorias monetárias, Keynes (1936) estabelece na economia uma relação da moeda que presta um papel central na determinação do emprego e do produto social, tida como forma de ativo especulativo por meio de sua capacidade de ser mantido como poder aquisitivo em sua forma pura para ser gasto em data futura. No fenômeno descrito como circulação industrial por Keynes, a moeda é utilizada somente para facilitar a circulação dos bens na economia, já na circulação financeira, pode-se identificar a existência de operações de ativos e estoques de riqueza, não necessariamente se relacionando com a troca de bens e permanecendo no espectro de seu caráter especulativo. Portanto, como em Marx, a moeda na teoria Keynesiana é uma variável não-neutra, que desenvolve desdobramentos cruciais sobre os níveis de atividade econômica, remetendo a sua influência sobre as decisões econômicas dos indivíduos que são baseadas em sua busca pela maximização da utilidade marginal e consequentemente a busca pelo lucro.

No entanto, se fossemos colocar as criptomoedas no patamar de moeda, elas ainda não se encaixariam nos moldes delimitados pela teoria Marxista ou Keynesiana, se aproximando de forma mais aparente da concepção desenvolvida por Hayek (2011) em seu estudo sobre a desestatização do dinheiro, na qual moedas privadas e concorrentes pudessem construir sua eficiência e credibilidade por meio de sua confiança perante sua aplicação social. Para ele, o motivo pelo qual se há conflitos referentes à emissão e controle de moeda é seu

monopólio por parte do Estado. É aparente pois como enfatizou Velde (2013), que analisou a relação das moedas digitais à teoria de Hayek, podem ser mais consideradas como autômato com emissão de moedas a uma taxa previsível, limitada pelas regras da Blockchain e do processo de mineração ao qual o Bitcoin está atrelado, incapaz de promover o “bom dinheiro”, no sentido de Hayek, isto é, cuja fidúcia ou poder de compra sejam resultantes da concorrência entre diferentes moedas emitidas privadamente, uma moeda de valor estável por limitação exógena, como o Bitcoin, se enquadra mais na ideia como um “monopólio natural”.

3 INTRODUÇÃO AO SISTEMA MONETÁRIO CENTRALIZADO

O mercado financeiro como opera na atualidade é completamente dependente da relação que a sociedade exprime com a renda. Portanto se faz necessário, além da contextualização do monetarismo teórico, uma apresentação do funcionamento do Sistema Monetário Centralizado em seu grau elevado de desenvolvimento na atualidade. Dessa forma, descrevendo a fundação que existe por trás da emissão e controle de oferta monetária e da viabilização dos processos bancários, assim como evidenciando as competências das autoridades monetárias e instituições de apoio, contempla-se o valor da centralização desse setor da economia.

Para trazer à tona a composição e competências das autoridades e instituições financeiras do Sistema Financeiro Nacional tomaremos como base as definições do livro **Mercado Financeiro** de Osias Santana de Brito, doutor e mestre em finanças pela FEA-USP, que desmistifica de maneira clara e objetiva os conceitos que necessito abordar para a construção do raciocínio.

A atmosfera financeira é composta atualmente pelo Banco Central (BCB), o Conselho Monetário Nacional (CMN), Banco do Brasil (BB) e as demais instituições financeiras públicas e privadas (BRITO, 2020, p.4). Sabemos que existem também autoridades de apoio que atuam juntamente com as instituições citadas anteriormente a fim de gerar a estrutura que permite o funcionamento do mercado. São elas: o Banco Nacional de Desenvolvimento Social (BNDES), a Comissão de Valores Mobiliários (CVM) juntamente com a Caixa Econômica Federal (CEF). Ainda há as comissões consultivas bancárias, de mercado de capitais, crédito rural e crédito industrial que dão suporte ao Conselho Monetário Nacional.

O Conselho Monetário Nacional tem como integrantes o presidente do Banco Central, o presidente da CVM, os secretários do Tesouro Nacional e da Política Econômica do Ministério da Economia, os diretores de Política Monetária, de Assuntos Internacionais e de Normas e Organização do Sistema Financeiro (BRITO, 2020, p. 5). É dever do CMN supervisionar as políticas monetárias, políticas de taxa de câmbio, de investimento, capital estrangeiro, comércio exterior e fiscal (BRITO, 2020, p. 6).

Dentre as formas de atuação do CMN pode-se observar a capacidade de adaptar o volume interno de moeda para combater efeitos de inflação ou deflação, assim como regular o valor interno da moeda e o equilíbrio da balança de pagamentos do país. A entidade ainda

tem o dever de orientar aplicações de recursos de instituições financeiras e realizar um constante aperfeiçoamento do sistema de pagamentos por meio destas, juntamente com seus respectivos instrumentos financeiros para uma melhor captação dos recursos. E é também sua prioridade garantir a liquidez e solvência das instituições financeiras e seus produtos, coordenando política monetária, creditícia, orçamentária e fiscal. Além dessas competências, ainda é responsável pelo gerenciamento das dívidas públicas (BRITO, 2020, p. 6)

O BCB é órgão executivo das decisões referentes a políticas macroeconômicas e de configuração do funcionamento do sistema financeiro nacional. Ele tem como função a normatização e fiscalização desse sistema exercendo sobre ele o monopólio da emissão da moeda, atuando como um “banco dos bancos” e “banqueiro do governo”, e executando as políticas monetária e fiscal (BRITO, 2020, p. 7). O Banco do Brasil por sua vez, atualmente se faz mais como um banco múltiplo, um conglomerado financeiro que possui algumas propriedades de autoridade monetária principalmente no que tange ao desenvolvimento de políticas creditícias do meio industrial e rural e colaborando na execução do Orçamento Geral da União.

A CVM é uma das autoridades monetárias centrais do mercado financeiro e opera diretamente na fiscalização e regulamentação do mercado de títulos e valores de renda variável (BRITO, 2020, p. 10). As Bolsas de Valores que estão sob sua cautela, são instituições nas quais se negociam os títulos e valores mobiliários de emissão ou corresponsabilidade de companhias abertas, registradas na CVM (BRITO, 2020, p. 11). No trecho a seguir, disponibilizado pelo site oficial do governo brasileiro, podemos compreender a composição e diretriz da CVM:

A CVM - Comissão de Valores Mobiliários é uma entidade autárquica em regime especial, vinculada ao Ministério da Fazenda, com personalidade jurídica e patrimônio próprios, dotada de autoridade administrativa independente, ausência de subordinação hierárquica, mandato fixo e estabilidade de seus dirigentes, e autonomia financeira e orçamentária. (Redação dada pela Lei nº 10.411, de 26 de fevereiro de 2002)

Apesar de vinculada ao CMN, a CVM possui autonomia jurídica, financeira e orçamentária, e sendo assim, mesmo tendo que manter suas diretrizes atreladas às políticas determinadas pelo Conselho, ainda há liberdade para “determinar limites máximos de preço, comissões, emolumentos e quaisquer outras vantagens cobradas pelos intermediários do mercado” (GOV.BR, 14 set. 2023), assim como estabelecer os critérios para fiscalização e

inspeção das companhias abertas e Bolsas de Valores. Abaixo podemos ver mais um trecho do documento do site do governo brasileiro apresentando a CVM e o Mercado de Valores Mobiliários (MVM), no qual demonstra a grande importância na existência de uma instituição que regre pelo funcionamento ótimo do mecanismo desse mercado, sem lhe tomar a fluidez dos produtos e autonomia dos agentes:

Ao eleger como objetivo básico defender os investidores, especialmente os acionistas minoritários, a CVM oferece ao mercado as condições de segurança e desenvolvimento capazes de consolidá-lo como instrumento dinâmico e eficaz na formação de poupanças, de capitalização das empresas e de dispersão da renda e da propriedade, através da participação do público de uma forma crescente e democrática e assegurando o acesso do público às informações sobre valores mobiliários negociados e sobre quem os tenha emitido.”(GOV.BR, 2023)

As Bolsas de Valores são entidades sem fins lucrativos as quais realizam as transações de compra e venda de títulos e valores imobiliários (BRITO, 2020, p. 10). E quando se trata da compra e venda de Bitcoins ou qualquer outro criptoativo, a dinâmica pela qual é moldada a plataforma que faz essas transações funciona de forma semelhante a esse tipo de instituição financeira.

Representam afinal o “local ou sistema adequado à realização de operações de compra e venda de títulos e valores mobiliários, em mercado livre e aberto” (BRITO, 2020, p. 10), sendo responsáveis pela eficiência da realização e visibilidade das operações, liquidez do mercado, fornecendo estrutura para as sociedades corretoras membros, mantendo um padrão ético elevado ao estabelecer as normas de comportamento às sociedades, realizando sua fiscalização e aplicando penalidades no que cabe à sua atuação.

Essas autoridades monetárias podem nos exemplificar como é necessária a atuação de agentes exteriores ao mercado para garantir sua eficiência e evitar que esse setor da economia entre em colapso e conseqüentemente possa desencadear uma recessão em momentos de instabilidade econômica nos quais há incerteza e cenários de inflação ou deflação acentuados. Sabe-se que esse não é um debate exclusivamente econômico, entrando na esfera política e portanto ideológica, porém é evidente que independente de partido político, há de se encontrar ideias promissoras no *mainstream* que contribuam para o desenvolvimento econômico.

Considerando que houvesse qualquer possibilidade do Bitcoin eventualmente se transformar em um padrão monetário alternativo regularizado pelo governo, e seu funcionamento - mesmo que somente uma parte, sem alterações na matriz da Blockchain -

fosse vinculado à essas autoridades e instituições, poderia sim ser considerado como uma pseudo-moeda e ser estudada ao lado de outras como dólar, euro ou o real, e assim se tornar uma opção viável de utilidade popular. Mas como essa vinculação trairia toda sua razão de existência e funcionamento descentralizado, no momento ela pode ser analisada ao lado somente dos títulos e valores mobiliários negociados em Bolsas de Valores, e portanto qualquer tipo de atuação exógena ao mercado poderá vir apenas da manipulação do câmbio entre o criptoativo e a moeda da transacionada.

3.1 SISTEMA FINANCEIRO INTERNACIONAL

Como Osias Brito evidenciou, o Mercado Financeiro Internacional no geral possui características semelhantes ao mercado brasileiro, mas devido a sua integração e influência da globalização, pode-se destacar a existência e atuação do Fundo Monetário Internacional (FMI) assim como o *Bank of International Settlement* (BIS). A estrutura desse mercado é também voltada para a estabilidade econômica, propiciando condições adequadas para a geração e manutenção de fluxo de reservas entre poupadores e investidores (BRITO, 2020, p. 25) e tomou maior forma a partir da década de 1970, na qual estavam sendo mais bem definidos os contornos geopolíticos e geoeconômicos mundiais. Além do auxílio do FMI e do BIS, a composição do Mercado Financeiro Internacional é composta por autoridades monetárias, normativas e fiscalizadoras; e instituições financeiras públicas, privadas e auxiliares.

O Banco Central no Mercado Internacional opera na maioria dos países como principal entidade normativa e fiscalizadora, auxiliando e executando as políticas monetárias, cambiais e fiscais. E as Comissões de Valores Mobiliários também se ocupam com a normatização e fiscalização do mercado bursátil e proteção dos investidores minoritários (BRITO, 2020, p. 25). Apesar de semelhante, o papel como entidade fiscalizadora do Banco Central nos outros países geralmente difere do Brasil no fator de independência do governo, às vezes apresentando orçamento próprio e maior autonomia em relação às políticas determinadas pelos *policymakers*.

É evidente que nem sempre a aplicação das decisões que afetam diretamente os setores e conseqüentemente a estabilidade das atividades econômicas serão efetivas ou capazes de obter os resultados exatos esperados pelos autores das políticas monetárias, o que fica muito claro da tentativa de conter a deflação de débitos da Grande Crise de 1929:

Depois que o Federal Reserve e os demais bancos centrais fracassaram em conter a deflação de débitos de 1929-33, tornou-se evidente a inadequação de um regime de política baseado em intervenções do banco central para conter o potencial eruptivo inerente ao desenvolvimento capitalista. (MINSKY, 1994, p. 24)

Mas cabe aos *policymakers* estarem sempre ampliando seu repertório de instrumentais técnicos, aperfeiçoando os modelos teóricos que buscam representar cada vez com maior abstração teórica os fenômenos da realidade, utilizando seu conhecimento dos acontecimentos históricos e consciência social para que sejam cada vez mais assertivos e influenciem positivamente o desenvolvimento econômico das nações.

O próprio sistema dispõe dos mecanismos que o corrompe, ou seja, os pontos instáveis do capitalismo que influenciam as elaborações de política monetária foram instaurados pelo desenvolvimento de seu próprio funcionamento (MINSKY, 1994, p. 24), e portanto a atuação do Estado como protetor do bem-estar social e interesses do mercado é imprescindível para que o caos não seja instaurado. Dito isso, há uma passagem popular de Keynes que representa sua crítica ao *laissez-faire* e, portanto, reflete a indagação a um sistema monetário centralizado sem intervenções competentes ao Estado:

Esclareçamos desde o início os princípios metafísicos ou gerais sobre os quais, de tempos em tempos, se fundamentou o *laissez-faire*. Não é verdade que os indivíduos possuem uma "liberdade natural" prescritiva em suas atividades econômicas. Não existe um contrato que confira direitos perpétuos aos que têm ou aos que adquirem. O mundo não é governado do alto de forma que o interesse particular e o social sempre coincidam. Não é administrado aqui embaixo para que na prática eles coincidam. Não constitui uma dedução correta dos princípios da Economia que o autointeresse esclarecido sempre atua a favor do interesse público. Nem é verdade que o autointeresse seja geralmente esclarecido; mais frequentemente, os indivíduos que agem separadamente na promoção de seus próprios objetivos são excessivamente ignorantes ou fracos até para atingi-los. A experiência não mostra que os indivíduos, quando integram um grupo social, são sempre menos esclarecidos do que quando agem separadamente (Keynes, 1978, p. 120).

Em toda sua capacidade descritiva, John Maynard Keynes pôde exemplificar um problema muito atual, que corresponde a ignorância de se acreditar que o liberalismo de mercado de fato preza pelos interesses individuais de cada um, quando em sua verdadeira face escancarada, explicita que seu objetivo principal é na verdade a alta performance do setor

amalgamado do mercado financeiro composto de Grandes Bancos e Corretoras que detêm imenso poder e influência econômica e política.

3.2 VULNERABILIDADE FUNCIONAL

No capítulo anterior, foram apresentadas as principais instituições e autoridades financeiras e monetárias, assim como suas principais competências frente à performance dos agentes e do mercado em si, englobando as faces das políticas monetárias. É evidente que o tom deste trabalho evidencia que o Bitcoin ainda não pode ser considerado como uma moeda, por não possuir vínculo com qualquer governo ou regularização de oferta por um Banco Central, sendo sua comercialização feita por intermediação de plataformas digitais chamadas *exchanges*, e seu preço então ser definido apenas pelas leis de oferta e procura.

Apesar da grande visibilidade que esse ativo vem ganhando nos últimos anos, exatamente por ter uma característica de alta velocidade e facilidade transacional, além de possuir taxas consideravelmente menores que de bancos para sua utilização e estocagem, a criptomoeda constrói suas próprias instabilidades a partir de seu funcionamento descentralizado, ficando fora de qualquer possibilidade de intervenção externa em casos de perda de valor de mercado.

4 IMPACTO ECONÔMICO DA MOEDA DIGITAL

A popularidade súbita do Bitcoin confere a referida confiança que os cidadãos colocam na moeda de seu país, afinal, em pouco tempo seu valor e demanda no mercado se tornaram altíssimos, mesmo perdendo força nos últimos tempos. Algum dia poderá ser chamada de moeda? Pois, sem um governo para fiscalizar e aplicar qualquer tipo de política monetária e com um crescente aumento do uso da criptomoeda em transações que envolvem tráfico de drogas e lavagem de dinheiro, como é possível acreditar nos benefícios que uma transação sem o intermédio de uma terceira parte pode oferecer? Como medir o impacto que esse tipo de transação terá nos governos do mundo todo sabendo que os modelos financeiros ainda são centralizados? É possível realizar medidas para mitigar esses impactos mesmo sem controle sobre o ativo?

Nos dias de hoje sabe-se que o bitcoin e as criptomoedas em geral não são comercializadas nas bolsas de valores, mas sim em *exchanges* (INFOMONEY, 2022), que são plataformas especializadas nesse tipo de transação e portanto fazem a intermediação entre compradores e vendedores, oferecendo ainda produtos e serviços com pagamento em ativos criptográficos e caso os usuários não desejarem guardar suas quantias em carteiras próprias, também funcionam como depósito. As *exchanges*, apesar de não atuarem ilegalmente, não são vinculadas e monitoradas pelo BCB, nem pela CVM, o que torna cada uma Bolsa de Valores independente, e sendo assim, a flutuação do preço dos criptoativos são vinculados somente à oferta e procura no mercado e portanto intrinsecamente sujeitos a especulação.

O fato de não estarem vinculadas a nenhuma autoridade monetária ou instituição de apoio do governo implica que não há como se esperar qualquer tipo de reajuste ou apoio em situações de alta volatilidade no nível de preços desses ativos, o que de fato corresponde ao cerne de toda sua existência desde que o Bitcoin foi desenvolvido em 2008 por Satoshi Nakamoto, mas também representa sua maior fragilidade quando analisada a possibilidade da nova moeda digital se tornar algo mais que um ativo. Proporcionando então uma nova opção de meio de pagamento viável para que principalmente os idealistas “Cyberpunks” que são ativistas extremistas de ideologia liberal possam realizar transações sem a intermediação de uma terceira parte como um banco e sentirem uma efêmera sensação de liberdade ao não pagarem suas taxas de transação.

The rise of bitcoin has attracted many with the metallist mindset, a group led by libertarians and anarcho-capitalists, who want government to get its greedy mitts

out of the money supply. Overlooking the intangible nature of bitcoin, they've treated the digital currency as a scarce commodity, a thing to be "mined" and stored, a thing whose mathematically proven finite supply ensures that its value will rise and outstrip that of unlimited fiat currencies such as the dollar. (VIGNA & CASEY, 2008:44)

Mas até onde essa narrativa deixa de representar um tipo de investimento inovador e anseio de uma parcela da sociedade e começa a representar uma ameaça real à segurança nacional e ao bem-estar da população de um país? Pois foi visto que além de muito associado a lavagem de dinheiro e mercado negro, as criptomoedas também tem o início de um relacionamento próximo com o tráfico de drogas e armas, por teoricamente não poderem ser rastreadas por nenhum intermediador, mas somente pelas duas partes envolvidas no negócio.

4.1 REGULAMENTAÇÃO DAS CRIPTOMOEDAS

No Brasil existe a Lei 14.478/2022 que está em vigor, sancionada pelo ex-presidente Jair Bolsonaro determinando que as *exchanges* somente poderão atuar no mercado brasileiro “mediante prévia autorização de órgão ou entidade da Administração Pública Federal” (Redação dada pela Lei 14.478/2022, de 21 de dezembro de 2022).

O documento também realiza a definição de ativo virtual em seu Artigo 3º: “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”.

É também de sua determinação os deveres estabelecidos ao respectivo órgão de administração:

- I - livre iniciativa e livre concorrência;
- II - boas práticas de governança, transparência nas operações e abordagem baseada em riscos;
- III - segurança da informação e proteção de dados pessoais;
- IV - proteção e defesa de consumidores e usuários;
- V - proteção à poupança popular;
- VI - solidez e eficiência das operações; e
- VII - prevenção à lavagem de dinheiro e ao financiamento do terrorismo e da proliferação de armas de destruição em massa, em alinhamento com os padrões internacionais.

Art. 5º Considera-se prestadora de serviços de ativos virtuais a pessoa jurídica que executa, em nome de terceiros, pelo menos um dos serviços de ativos virtuais, entendidos como:

I - troca entre ativos virtuais e moeda nacional ou moeda estrangeira;

II - troca entre um ou mais ativos virtuais;

III - transferência de ativos virtuais;

IV - custódia ou administração de ativos virtuais ou de instrumentos que possibilitem controle sobre ativos virtuais; ou

V - participação em serviços financeiros e prestação de serviços relacionados à oferta por um emissor ou venda de ativos virtuais. (Redação dada pela Lei 14.478/2022, de 21 de dezembro de 2022)

Deveres estes que se assemelham de forma clara aos que as próprias Bolsas de Valores têm em relação a CVM, demonstrando que o mercado de ativos digitais no Brasil direciona-se em sentido a concretização da regularização parcial da moeda descentralizada.

Além das responsabilidades do órgão, realiza-se o acréscimo do Art. 171- A ao Decreto-Lei nº 2.848, de 7 de dezembro de 1940 configurando “fraude com a utilização de ativos virtuais, valores mobiliários ou ativos financeiros”:

Art. 171-A. Organizar, gerir, ofertar ou distribuir carteiras ou intermediar operações que envolvam ativos virtuais, valores mobiliários ou quaisquer ativos financeiros com o fim de obter vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil ou qualquer outro meio fraudulento. (Redação dada pela Lei 14.478/2022, de 21 de dezembro de 2022)

Nos EUA, em 26 de julho de 2023, no comitê da Câmara foram aprovados dois projetos de lei envolvendo a regulamentação dos ativos digitais. A primeira é chamada de Lei de Inovação Financeira e Tecnologia para o Século XXI, que assim como no Brasil estabelece os deveres das corretoras de criptomoedas a partir de seu registro em algum dos órgãos de regulamentação dos Estados Unidos, a Comissão de Negociação de Futuros de Commodities (CFTC) ou na Comissão de Valores Mobiliários (SEC).

O segundo projeto de lei desmistifica as relações de prestadores de serviço da Blockchain, estabelecendo diretrizes para facilitar o acesso aos requisitos de profissionais como mineradores e prestadores de serviços de assinaturas e plataformas financeiras descentralizadas (COINTELEGRAPH, 2023).

Além dos projetos de lei mais recentes, pode-se destacar também a atuação do órgão norte-americano de fiscalização de crimes financeiros (FinCEN), assim como a implementação do ato de sigilo bancário, *Bank Secrecy Act* (BSA) os quais ambos são responsáveis pelo combate a esquemas de lavagem de dinheiro, apesar de ainda encontrarem barreiras em sua atuação devido a descentralização das criptomoedas.

Apesar de se aproximar as determinações do governo brasileiro em relação as determinações das regulamentações dos ativos digitais frente as autoridades monetárias e instituições financeiras, os Estados Unidos não se mobilizaram na definição de leis de combate ao uso de criptomoedas em lavagem de dinheiro.

Ao abordar o tema da regulamentação dos ativos digitais na região da União Europeia, pode-se observar o projeto do parlamento suíço que fora aprovado em fevereiro de 2021, visando proporcionar suporte legal na negociação de criptomoedas, assim como os projetos de lei estadunidenses. Na Alemanha, o Bitcoin e já e considerada como meio de pagamento, sendo isenta de imposto sobre ganhos de capital. A União Europeia admitiu que planeja rever suas leis de lavagem de dinheiro propostas em 2021, adicionando as mesmas casos envolvendo finanças descentralizadas (DeFi), promovendo regulamentações as organizações autônomas descentralizadas (DAOs) a qual são vinculadas a fim de combater a lavagem de dinheiro e o financiamento do terrorismo.

4.2 LAVAGEM DE DINHEIRO

Assim que a regulamentação das criptomoedas foi exemplificada em diferentes perspectivas de diferentes nações, deve-se observar também o atual estado do envolvimento de sua utilização nos crimes de lavagem de dinheiro e financiamento do terrorismo, assim como as características que fazem de seu uso propício para sua propagação.

De acordo com Bueno (2020, p. 113), as 5 características decisivas para a utilização dos ativos digitais em esquemas criminosos são:

- i. Inexistência física;
- ii. Transmissão direta entre as partes;
- iii. Irreversibilidade das operações;
- iv. Alcance global
- v. Baixo custo de operações.

Todas essas características permitem que os criminosos burlam com mais facilidade os procedimentos realizados em contas bancárias para o rastreamento das atividades ilegais, assim como se mostrou uma alternativa substancialmente mais veloz e prática de meio de pagamento quando realizado em longas distâncias.

Um relatório realizado pela *Chain Analysis* revelou dados alarmantes sobre lavagem de dinheiro por meio de ativos digitais:

Os dados obtidos pela Chain Analysis, em seu *The 2023 Crypto Crime Report*, relativos à lavagem de dinheiro a partir de criptomoedas (o que inclui o BTC, mas não se limita a ele), indicam que, em 2022, US\$ 22,8 bilhões foram lavados por meio desses ativos virtuais. Trata-se de um crescimento de 68% sobre os US\$14,2 bilhões do ano de 2021. É necessário ressaltar que esses números são provisórios, uma vez que constantemente são identificadas novas operações ilícitas. Assim, muito provavelmente os números reais são maiores. (CONJUR, 2023)

Esses dados remetem somente as operações que foram possíveis de serem rastreadas a partir da regulamentação que está sendo implementada na atualidade, no entanto os níveis de movimentação de capital por meio da utilização de criptomoedas em atividades ilícitas tem uma proporção ainda desconhecida as autoridades visto que além de permanecer praticamente indetectáveis devido a falta de informação por parte das *exchanges* referente as contas e transações existentes antes das regulamentações, ainda há a recente utilização de finanças descentralizadas (DeFi) que utilizam de *smart contracts* para seu funcionamento simplificando as responsabilidades de ambas as partes e não possuem vinculação a instituições financeiras.

5 CONSIDERAÇÕES FINAIS

O Bitcoin e as demais criptomoedas estão cada vez mais adentrando na sociedade e conquistando seu espaço. Nakamoto em 2008 quando criou a moeda para alguns anos depois colocar a *Blockchain* em operação buscava revolucionar os meios de pagamento com o nascimento de um meio de pagamento descentralizado que independe da intermediação de uma terceira parte eliminando a burocracia e manipulação de dados do sistema bancário.

No entanto, apesar de bem elaborado em função da mecânica da *Blockchain*, o documento *Bitcoin: A peer-to-peer Electronic Cash System* não detalhou como funcionaria o comportamento da moeda frente a problemas econômicos reais. A falta de uma autoridade monetária controlando a emissão das moedas somente foi mencionada no momento de explicação do processo de mineração em que se oferece o incentivo ao validar-se a transação, distribuindo moedas em circulação e impulsionando a performance da rede.

Talvez isso possa ser explicado pelo caráter do anonimato de Nakamoto, transparecendo que apesar de altruisticamente desenvolver um sistema complexo de meio de pagamentos de caráter descentralizado não haveria como saber os níveis de sua repercussão assim como o caráter das transações que seriam realizadas utilizando sua moeda digital.

De certa forma ao esconder sua verdadeira identidade tenha cogitado diferentes cenários, nos quais qualquer tipo de ideia que fosse tão revolucionária quanto a ferramenta que criara poderia acelerar significativamente as mudanças da percepção de um sistema financeiro, ou derrocá-lo por completo.

É evidente que como qualquer inovação ela possui suas vantagens e desvantagens. Após o efeito “*Boom*” do Bitcoin percebeu-se a criação de um novo setor da área financeira, uma nova extensão de vagas no mercado de trabalho. Assim como pode-se perceber também como efeito, paralelamente, um crescimento dos níveis de investimento, o qual passou por grande processo de desmistificação, aumentando em geral a disposição de informação e educação referentes o funcionamento de Bolsas de Valores, diferentes ativos e produtos financeiros.

Mas depois que percebeu-se o potencial do anonimato garantido pelos processos da *Blockchain* e viu-se como era simplificada a transação tanto em largo volume de escala quanto em termos de distância a popularidade das criptomoedas aumentou em meio a atividades criminosas. E a sociedade enfrenta hoje grandes ameaças ao se esforçar para conseguir designar projetos de lei regularizando a atividade das corretoras, e promovendo novas

definições enquadrando lavagem de dinheiro e financiamento de terrorismo devido aos desdobramentos dos conflitos policiais.

Assim como na Europa feudal do século XV na qual houveram diferentes processos revolucionários que culminaram na transformação das relações sociais e conseqüentemente na transição do feudalismo para o capitalismo, é possível que estejamos presenciando o início de um processo de evolução do sistema financeiro que acarretará em diferentes interpretações da noção de meio de pagamento, o dinheiro como na relação de Hayek (2011) em seu exercício de desestatização já se consagra: a moeda não precisa existir fisicamente para entrar em circulação. Em relação a aceitação popular, mesmo antes das criptomoedas verifica-se a utilização do pagamento em *pix*, que apesar de não possuir a mesma estrutura de funcionamento, ainda se configura como a representação do dinheiro virtual.

Da mesma forma que no Império Romano no período das moedas de cunho usavam sal como equivalente de troca exprimindo seu peso em ouro, as criptomoedas se mostram como uma alternativa promissora no processo de inovação do sistema financeiro nos dias de hoje. Mas assim como as modernizações referentes aos avanços da Inteligência Artificial, deve-se tomar muito cuidado com o rumo que a utilização dessas alternativas pode tomar frente a segurança e bem-estar social, assim como em relação a proteção de castas sociais que sofrerão devido a simplificação de processos no mercado de trabalho, aumentando os níveis de desemprego.

Após realizar o raciocínio deste trabalho, pode-se concluir que o futuro das criptomoedas ainda permanece incerto quanto a tornar-se um padrão cambial viável e aceito universalmente na sociedade. O que se sabe é que há grande potencial de crescimento, e que cada vez mais as nações buscam encaixá-lo em seu lugar. Descentralizado do sistema financeiro convencional, assim mantendo sua essência, mas protegendo os agentes de mercado por meio de regulamentações que o consolidam, mas dificultam a utilização corrupta do anonimato garantido pela criptografia das informações.

REFERÊNCIAS

BARROS, Walter. **10 maiores hacks de criptomoedas em 2022 causam prejuízo de 2,7 bilhões e respondem por 75% dos fundos roubados.** 2022. Disponível em:

<<https://br.cointelegraph.com/news/10-biggest-cryptocurrency-hacks-in-2022-cause-27-billion-losses-and-account-for-75-of-stolen-funds>> Acesso em: 20 out. 2023.

BBC NEWS BRASIL. **Criptomoedas: a bilionária dívida deixada pela quebra da corretora FTX.** Disponível em: <<https://www.bbc.com/portuguese/geral-63701885>> Acesso em: 18 out. 2023.

BIT2ME ACADEMY. **O que é SHA-256.** 23 jul. 2023. Disponível em:

<<https://academy.bit2me.com/pt/sha256-algoritmo-bitcoin/>>. Acesso em: 2 dez. 2022.

BRITO, Osias Santana de. **Mercado Financeiro.** 3ª Ed. Saraiva Educação, São Paulo, 2020

BUENO, Thiago Augusto. **Bitcoin e crimes de lavagem de dinheiro.** 1ª Edição. Campo Grande: Contemplar: 2020.

COINDESK. **União Europeia quer aumentar combate à lavagem de dinheiro via metaverso, DeFi e NTFs.** 2022. Disponível em:

<<https://www.infomoney.com.br/mercados/uniao-europeia-quer-aumentar-combate-a-lavagem-de-dinheiro-via-metaverso-defi-e-ntfs/>> Acesso em: 25 out. 2023.

EICHENGREEN, B. **História e reforma do sistema monetário internacional.** Economia e Sociedade, Campinas, SP, v. 4, n. 1, p. 53–78, 2016.

GOV.BR. **O que é a CVM?** [S.I.] Disponível em: <<https://www.gov.br/cvm/pt-br/aceso-a-informacao-cvm/servidores/estagio/2-materia-cvm-e-o-mercado-de-capitais#:~:text=A%20Comiss%C3%A3o%20de%20Valores%20Mobili%C3%A1rios,mat%C3%A9ria%20de%20mercado%20de%20capitais.>>. Acesso em: 14 set. 2023

HAYEK, F. A. **Desestatização do dinheiro: Uma análise da teoria e prática das moedas simultâneas**. São Paulo. Instituto Ludwig Von Mises. Brasil, 2011.

INFOMONEY. **O que é DeFi?** 2022. Disponível em:

<<https://www.infomoney.com.br/guias/defi/>> Acesso em: 20 out. 2023.

_____. **Exchange de criptomoedas: o que são e como escolher uma**. 8 nov. 2022.

Disponível em: <<https://www.infomoney.com.br/guias/exchange-de-criptomoedas/>>.

[Acesso em: 13 set. 2023.](https://www.infomoney.com.br/guias/exchange-de-criptomoedas/)

_____. **O que é o Halving do Bitcoin?**. 7 nov. 2022. Disponível em:

<<https://www.infomoney.com.br/guias/halving-do-bitcoin/>>. Acesso em 2 dez. 2022

_____. **O que é Proof-of-work (PoW)? Conheça a tecnologia que torna o**

Bitcoin seguro. 7 nov. 2022. Disponível em : <[https://www.infomoney.com.br/guias/proof-of-](https://www.infomoney.com.br/guias/proof-of-work-pow/)

[work-pow/](https://www.infomoney.com.br/guias/proof-of-work-pow/)>. [Acesso em: 2 dez. 2022](https://www.infomoney.com.br/guias/proof-of-work-pow/)

INVESTING.COM. **Todas as criptomoedas**. [S.I.]. Disponível em:

<<https://br.investing.com/crypto/currencies>>. Data de acesso: 15 jun. 2022.

KEYNES, J. M. **Keynes: economia**. São Paulo: Ática, 1978.

KEYNES, J. M. **A Teoria Geral do Emprego, do Juro e da Moeda**. São Paulo: Atlas, 1982 [1936].

MALDONADO FILHO, E. **Notas sobre a Teoria Monetária e do Juro em Marx**.

Revista ANPEC, n. 3, ago. 1997, p. 55-69

MARX, Karl. **O capital: crítica da economia política**. Rio de Janeiro: Record, Ed. 37, 2020

MENDONÇA, Lawrence Lino Monteiro de. **Lavagem de dinheiro e criptomoedas: a utilização de serviços off-ramping**. 6 Mar. 2023. Disponível em:

<<https://www.conjur.com.br/2023-mar-06/lawrence-lino-lavagem-dinheiro-criptomoedas-off-ramping>>. Data de acesso: 29/09/2023

MICHELHILL, Tom. **Projetos de lei sobre criptomoedas são aprovados pelo comitê do Congresso dos EUA em ‘grande vitória’ para indústria.** 2023. Disponível em: <<https://br.cointelegraph.com/news/crypto-regulatory-framework-bill-pass-house-congressional-committee>>. Acesso em: 24 out. 2023.

MINSKY, H. P. **Integração financeira e política monetária.** Economia e Sociedade, Campinas, SP, v. 3, n. 1, p. 21–38, 2016.

MOLLO, M. L. R. **Ortodoxia e Heterodoxia Monetárias: a Questão da Neutralidade da Moeda.** Revista de Economia Política, vol. 24, n. 3 (95), jul.-set., 2004.

NAKAMOTO, Satoshi. **Bitcoin: A Peer-to-Peer Electronic Cash System.** 2008. Disponível em: <<https://bitcoin.org/bitcoin.pdf>>. Data de acesso: 10/05/2022

NICOCELI, Arthur; MALAR João Pedro. **Regulação de criptomoedas avançou em diversos países em 2021.** CNN Brasil Business, São Paulo, 2021. Disponível em: <<https://www.cnnbrasil.com.br/economia/regulacao-de-criptomoedas-avancou-em-diversos-paises-em-2021-confira/>>. Acesso em: 25 out. 2023

PORCELLI, Andrea. **The most mentioned crypto on Twitter is Bitcoin, but analysis highlights growing interest in the entire sector.** *The cryptonomist.* 8 abr. 2023. Disponível em: <<https://en.cryptonomist.ch/2023/04/08/what-most-searched-crypto-twitter/#:~:text=While%20Bitcoin%20remains%20the%20dominant,terms%20of%20popularity%20and%20sentiment.>>. Acesso em: 12 out. 2023.

PRESIDENCIA DA REPÚBLICA /SECRETARIA-GERAL. **Lei nº 14.478, de 21 de dezembro de 2022.** Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/Lei/L14478.htm>. Acesso em: 24 out. 2023

RAEESI, Reza. **The Silk Road, Bitcoins and the Global Prohibition Regime on the International Trade in Illicit Drugs: Can this Storm Be Weathered?** [S.I.] Disponível em:

<<https://gjis.journals.yorku.ca/index.php/gjis/article/view/38935/36402>>. Acesso em 17 out. 2023

SCIARRETTA, Toni; BONFIM, Ricardo. **Quebra da FTX chama atenção para ‘ética de negócio’ do setor cripto**. Valor Econômico. São Paulo, 2022. Disponível em: <<https://valor.globo.com/financas/criptomoedas/noticia/2022/12/16/quebra-da-ftx-chama-atencao-para-etica-de-negocio-do-setor-cripto.ghtml>>. Acesso em: 18 out. 2023

ULRICH, Fernando. **Bitcoin: A moeda na era digital**. Instituto Ludwig von Mises Brasil, São Paulo, 2017.

VELDE, F. **Bitcoin: A Primer**. Chicago. The Federal Reserve Bank of Chicago. Chicago Fed Letter nº 317, 2013. Disponível em: <<https://www.chicagofed.org/publications/chicago-fed54letter/2013/december-317>>.

VIGNA, Paul & CASEY, Michael J. ***The age of cryptocurrency: How bitcoin and digital money are challenging the global economic order***. St. Martin’s Press, 2015.

