PONTIFÍCIA UNIVERSIDADE CATÓLICA DE SÃO PAULO (PUC-SP)

ANA BEATRIZ DOS SANTOS BORGES

**BITCOIN - A MOEDA DIGITAL QUE DESAFIA O SISTEMA FINANCEIRO
TRADICIONAL E SEUS ASPECTOS LEGAIS**

MESTRADO EM DIREITO

SÃO PAULO

2019

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE SÃO PAULO (PUC-SP)

ANA BEATRIZ DOS SANTOS BORGES

**BITCOIN - A MOEDA DIGITAL QUE DESAFIA O SISTEMA FINANCEIRO
TRADICIONAL E SEUS ASPECTOS LEGAIS**

Dissertação apresentada à Banca Examinadora da Pontifícia Universidade Católica de São Paulo, como exigência parcial para a obtenção do título de MESTRE em Direito, sob a orientação da Prof^ª. Dra. Maria Eugênia Reis Finkelstein

SÃO PAULO

2019

ANA BEATRIZ DOS SANTOS BORGES

Banca Examinadora

Dedico este trabalho “in memoriam” ao meu admirável irmão Marcos Aurélio dos Santos Borges, que sempre foi e será o meu norte, a minha fonte de exemplo, inspiração e orientação.

AGRADECIMENTOS

Agradeço primeiramente a Deus pela iluminação, força e coragem no momento que eu mais precisei de ajuda, devido a repentina perda de meu irmão.

Ao meu querido irmão Marcos Aurélio, que nos deixou em 10 de abril de 2019, pois sempre foi meu grande apoiador, incentivador nos meus estudos, mentor, exemplo de pessoa íntegra, alegre, resiliente e conciliadora.

Aos meus pais, Norma Maria e Magno José, por sempre estarem ao meu lado me apoiando e incentivando em todos os momentos de minha vida.

A minha orientadora Prof^ª. Dra. Maria Eugênia Reis Finkelstein, pela sua valiosa orientação, suporte, encorajamento, carinho e compreensão, especialmente durante o período de meu luto. Sob sua orientação, no momento tão difícil de minha vida, foi possível organizar as ideias, os assuntos para a concretização deste trabalho. Muito obrigada, professora, pela sua dedicação e atenção.

Aos professores das matérias que tive a oportunidade de cursar, Prof. Dr. Cláudio Finkelstein, , Prof. Dr. Fábio Ulhoa Coelho, Prof^ª. Dra. Márcia Cristina de Souza Alvim, Prof^ª. Dra. Maria Helena Diniz, Prof. Dr. Marcus Elidius Michelli de Almeida, Prof. Dr. Miguel Horvath Júnior.

Aos membros de minha família (tios, tias, primos) e amigos pelas mensagens de apoio e incentivo. Em especial aos amigos Thiago César, por sua brilhante palestra que me motivou a começar as minhas pesquisas sobre o mundo das criptomoedas; Idean Alves, pelas interessantes conversas desde os tempos de faculdade sobre Economia e investimentos; e Antonio Goés pelas ajudas tecnológicas e incentivos para a efetivação da dissertação.

Aos professores do Centro Universitário do Pará, Prof. Dr. Fabrício de Oliveira Vasconcelos e Prof^ª. Dra. Tássia Baía Miranda, pelas oportunas orientações que me oportunizaram ingressar no Mestrado.

Aos amigos do IBRACHINA e do Thomas Law Advogados, em especial a Ana Kaline e Thomas Law, pelo incentivo e companheirismo.

Aos amigos, companheiros de Mestrado, que tive a oportunidade de conhecer e consolidar amizades nesses dois anos de Mestrado.

RESUMO

O presente trabalho tem como assunto principal de estudo a criptomoeda Bitcoin. Busca mostrar, ao leitor, a revolução digital a qual esta moeda faz parte, seu contexto de surgimento, suas características e importância de seu desafio face ao sistema financeiro tradicional.

Neste trabalho, procuraremos também estudar os aspectos legais dessa criptomoeda, como ela está sendo percebida pelas autoridades brasileiras e os possíveis modos de como regular.

Palavras-chave: Bitcoin, criptomoeda, revolução digital, regulação, sistema financeiro.

ABSTRACT

The present work, has as main subject the study about the cryptocurrency Bitcoin. Search show to the reader, the digital revolution that this cryptocurrency made part, your context of rise, your features, and the importance of your challenge face de traditional financial market.

In this work, we will also search to study, the legal aspects of the cryptocurrency, how is it being perceived by the Brazilian authorities and their possible ways of regulating.

Keywords: Bitcoin, cryptocurrency, digital revolution, regulation, financial system

SUMÁRIO

INTRODUÇÃO.....	9
CAPÍTULO 1 - A QUARTA REVOLUÇÃO INDUSTRIAL.....	10
1.1 - Internet das Coisas	14
1.2 - Revolução Digital.....	15
CAPÍTULO 2 - A CRISE FINANCEIRA MUNDIAL DE 2008	16
2.1 - Fim do “Glass-Steagall Act”	16
2.2 - Liberalismo Econômico	17
2.3 - Falta de Regulação	18
2.4 - Atividades Bancárias Paralelas	19
2.5 - Classificação de Risco de Crédito (Agências de Classificação)	21
2.6 - Balanços Patrimoniais Não Computados	22
2.7 - A Crise dos <i>Subprimes</i> - A Bolha Especulativa.....	22
2.7.1 - <i>Alternativas Após a Crise dos “Subprimes”</i>	27
CAPÍTULO 3 - MOEDA	28
3.1 - Tipos de Moeda.....	30
3.1.1 - <i>Metal/Papel - Moeda/Moeda Eletrônica</i>	30
3.1.2 - <i>Moeda Virtual (Criptomoeda)</i>	31
3.2 - Funções da Moeda.....	34
3.2.1 - <i>Unidade de Conta ou Medida Comum de Valor</i>	35
3.2.2 - <i>Meio de Pagamento</i>	36
3.2.3 - <i>Reserva de Valor</i>	37
CAPÍTULO 4 - BITCOIN.....	38
4.1 - Internet of Money (Internet do Dinheiro)	38
4.2 - O que é o Bitcoin?.....	39
4.3 - Rede <i>Peer-To-Peer</i>	41
4.4 - Tecnologia <i>Blockchain</i>	42
4.5 - Servidor de Validação (Timestamp Server).....	44
4.6 - O Gasto Duplo.....	45
4.7 - Transações em Bitcoin	46
4.8 - Funcionamento das Transações e da Rede.....	47
4.9 - Mineração.....	47
4.10 - Privacidade	50
4.11 - Armazenamento dos Bitcoins.....	51
4.12 - Como Obter Bitcoins.....	52
4.13 - Exchanges	52
4.14 - Divisão do Bitcoin.....	53
4.15 - Bitcoin Para Além da Ideia de Moeda	55
4.16 - Bitcoin Ameaça ao Sistema Financeiro Tradicional?	57
4.17 - Altcoins	59
4.18 - O que Determina o Preço do Bitcoin	60
4.19 - Confiança no Bitcoin.....	62
4.20 - Bitcoin: Pode ser uma Rede de Pagamento?.....	62
4.21 - Acessibilidade do Bitcoin.....	63
4.22 - Como o Bitcoin Vira “Dinheiro”?.....	63

4.23 - É Possível Comprarmos no Comércio Utilizando Bitcoins?	63
4.24 - Bitcoin X Libra	63
CAPÍTULO 5 - BITCOIN E SEUS ASPECTOS LEGAIS	66
a) Natureza jurídica de moeda	66
b) Natureza jurídica de ativo	68
c) Natureza jurídica de commodities	68
d) Natureza jurídica de bem imaterial	69
e) Natureza jurídica de valor mobiliário.....	69
5.1 - A Questão da Regulação	71
a) <i>Documentos exigidos pelas Exchanges</i>	71
b) <i>Fechamento de Exchange e a não garantia de criptomoedas depositadas</i>	71
c) <i>Fiscalização de lavagem de dinheiro</i>	72
d) <i>Invasão cibernética</i>	72
e) <i>Partilha de bens e Sucessão</i>	72
f) <i>Declaração de Imposto de Renda</i>	72
g) <i>Fraudes e Pirâmides Financeiras</i>	73
5.2 - A Regulação	73
5.3 - Projeto de Lei 2.303/2015	77
5.4 - Projeto de Lei Nº 2.060/2019	80
5.5 - Instrução Normativa da Receita Federal	83
5.6 - Comunicados do Banco Central.....	84
5.7 - Nota da Comissão de Valores Mobiliários (CVM).....	84
5.8 - Meios de Regulação	85
5.8.1 - <i>Regulação do Usuário Final</i>	86
5.8.2 - <i>Regulação nos Provedores de Internet</i>	86
5.8.3 - <i>Regulação dos Intermediários de Informação</i>	87
5.8.4 - <i>Regulação de Intermediários Específicos</i>	88
5.8.5 - <i>Regulação de Mineradores</i>	89
5.8.6 - <i>Regulação do Código Base</i>	92
5.8.7 - <i>Regulação de Hardware</i>	94
5.8.8 - <i>Regulação do Mercado que Utiliza o Sistema Blockchain</i>	95
5.8.9 - <i>Regulação por Meio de Normas Sociais</i>	97
CONCLUSÃO.....	99
REFERÊNCIAS BIBLIOGRÁFICAS	101
ANEXO I.....	106
ANEXO II: INSTRUÇÃO NORMATIVA RFB Nº 1888, de 03 DE MAIO DE 2019.	108
ANEXO III: COMUNICADOS DO BANCO CENTRAL	112
ANEXO IV- NOTAS DA COMISSÃO DE VALORES MOBILIÁRIOS.....	115

INTRODUÇÃO

Com o advento da tecnologia e as mais recentes inovações, mais especificamente as criptomoedas, podemos observar uma quebra de paradigmas no que diz respeito ao sistema financeiro mundial, principalmente após a crise financeira no ano de 2008.

O presente trabalho tem como objetivo estudar o Bitcoin, o expoente entre as criptomoedas. O tema é de relevante importância em nossos dias, devido à inovadora tecnologia presente em sua base, bem como a maneira o qual o Bitcoin está transformando o sistema financeiro mundial. Além de quebrar paradigmas na economia, o mesmo também influencia nos aspectos sociais e regulatórios.

Para o Direito, é importante compreender o Bitcoin, visto que, como não há regulação específica sobre o tema em nosso país, e cada vez mais o mercado das criptomoedas tem aumentado no Brasil e no mundo, é necessário direcionarmos algumas possibilidades de regulação, a fim de que possa ter mais segurança e garantias para usuários, *Exchanges* e Economia Nacional.

Antes de estudar detalhadamente a criptomoeda Bitcoin, pretende-se conceder ao leitor um panorama sobre a Quarta Revolução Industrial, dissertando sobre o seu contexto histórico, o que é, e como se desenvolve.

No segundo capítulo, estudaremos a crise financeira mundial de 2008, seus aspectos, como se desenvolveu, e como foi o *insight* para o desenvolvimento da criptomoeda Bitcoin.

No terceiro capítulo, dissertaremos sobre o significado de Moeda, seu contexto histórico, suas funções e especificidades, permitindo ao leitor ter um entendimento mais aprofundando desse objeto tão presente em nossa sociedade.

No quarto capítulo, estudaremos mais específico e aprofundado a criptomoeda Bitcoin, como se desenvolveu, como funciona, como adquirir e sobre suas especificidades.

No quinto capítulo, teremos o enfoque na parte do Bitcoin e o Direito Brasileiro, sua natureza jurídica, seus aspectos legais, como as autoridades observam o Bitcoin, seu processo de regulação no país e sugestões para os modos de regulação.

CAPÍTULO 1 - A QUARTA REVOLUÇÃO INDUSTRIAL

Para termos o entendimento do que é a Quarta Revolução Industrial, primeiramente precisamos entender a etimologia da palavra “revolução” e seu contexto histórico.

Revolução, a palavra tem sua origem no latim *revolutione*, que tem como significado, no primeiro momento, toda e qualquer transformação radical nos mais diversos aspectos da vida. Também é um ato ou finalidade de *revolver* ou *revolucionar*. A palavra tem o seu significado aplicado em diversas situações. A exemplo de, na esfera política, a revolução é uma mudança significativa nas instituições de um país, ocorrendo por meio de uma rebelião ou um motim, como foi o caso da Revolução Francesa, causando uma alteração drástica na sociedade, no campo político, econômico, social e cultural, estabelecendo, portanto, uma nova ordem. Já no sentido figurado, a “revolução” pode ser uma mudança profunda na maneira de agir, pensar de uma pessoa, após um acontecimento.

Podemos assim dizer que a “revolução” é uma mudança no *status quo* de uma pessoa, pensamento, sociedade, instituições, e essa mudança vem de uma forma repentina e drástica, alterando de maneira significativa o que antes estava intacto, estava de uma maneira, e passou a ser entendido de outra forma.

É verdadeiramente uma mudança de paradigma.

A palavra “revolução” denota mudança abrupta e radical. Em nossa história, as revoluções têm ocorrido quando novas tecnologias e novas formas de perceber o mundo desencadeiam uma alteração profunda nas estruturas sociais e nos sistemas econômicos. Já que a história é usada como referência, as alterações podem levar para se desdobrarem. (SCHWAB, p. 15)

Com o crescimento da população e a consequente migração das pessoas do campo para as cidades, o que levou à urbanização e ao surgimento das cidades, possibilitou que novas necessidades na sociedade surgissem. Com isso, desencadeou-se revoluções industriais, ou seja, houve a transição do uso da força muscular para a energia mecânica, possibilitando o surgimento das primeiras máquinas.

Dessa forma, as sociedades, ao longo dos séculos, se transformaram e se adaptaram aos avanços criados pela Revolução Industrial, que se originou na Inglaterra no século XVIII. A sociedade necessitava cada vez mais de bens de produção, e, a partir dessa carência, se reinventava, saindo da manufatura para a produção em série por meio da máquina no processo fabril (maquinofatura). A partir desse momento, surgem as fábricas, onde os mais diversos bens eram fabricados em grande escala para atender a demanda. Ainda com o nascimento da

fábrica, tem-se a corrida para a extração do carvão mineral, matéria-prima necessária para suprir energeticamente as máquinas das fábricas. Nasce também novas classificações de classes sociais, como a burguesia e o proletariado.

A Primeira Revolução Industrial se deu no período que compreende entre os anos 1760 e 1840, onde a produção passou de manufatura para mecanizada, principalmente pelo fato da construção das ferrovias e também pela invenção da máquina a vapor, dando início, portanto, à produção mecânica.

A Segunda Revolução ocorreu por volta de 1850 (final do século XIX, início do século XX), impulsionada com o surgimento da eletricidade e da linha de montagem, a qual possibilitou a produção em massa.

A terceira ocorreu em meados do século XX, mais especificamente na década de 1960, com o advento da eletrônica, da tecnologia da informação e das telecomunicações.

Ela costuma ser chamada de revolução digital ou do computador, pois foi impulsionada pelo desenvolvimento dos semicondutores, da computação em *mainframe* (década de 1960), da computação pessoal (década de 1970 e 1980) e da internet (década de 1990). (SCHWAB, p. 16)

A Quarta Revolução, para os estudiosos, tem como característica a interação de tecnologias digitais, físicas e biológicas, onde os robôs conectados a sistemas ciberfísicos proporcionarão essa mudança, sendo, portanto, o início de uma revolução que alterará significativamente o modo como vivemos, trabalhamos e nos relacionamos na sociedade, sendo esta em um nível jamais vivenciado na história da humanidade.

A Quarta Revolução Industrial iniciou-se na virada do século XX. Esta é uma revolução digital que, no contexto atual, está em pleno andamento e é definida por uma internet mais móvel e universal, por sensores pequenos e mais potentes e também pela inteligência artificial e aprendizagem automática, ou seja, o aprendizado da máquina, conseguido por meio da técnica de programação.

É fato que atualmente vivenciamos um momento revolucionário. A evolução trazida pela Internet adentrando a vida do Homem comum equipara-se, sem dúvida alguma, a uma revolução, ainda que cultural. Por esse motivo, é comum referir-se ao atual momento histórico como a **Revolução Informática**. (FINKELSTEIN, p. 54) (grifo nosso)

Com isso, as tecnologias as quais possuem como base os computadores, *software* e redes, as mesmas não são atuais, mas estão causando transformações na chamada Terceira

Revolução Industrial, se tornando, portanto, tecnologias mais refinadas e assimiladas, possibilitando uma ruptura e a consequente mudança da sociedade e da economia global.

Nota-se, diante de um sistema globalizado, assim como altamente competitivo, **em plena 4ª Revolução Industrial, onde o que mais se propaga são as informações e a velocidade das relações negociais**, de tal forma que o mundo tende a caminhar de maneira uniforme. (ROVAL, p. 49) (grifo nosso)

É de fato que essas tecnologias irão se manifestar fortemente, por intermédio da automação e de meios sem precedentes na história da humanidade, ou seja, a presença da tecnologia em nosso cotidiano estará muito forte e imprescindível, propiciando a incessante busca pela inovação, que é a mola propulsora para a evolução.

A automatização acontece através de sistemas ciberfísicos, que foram possíveis graças à internet das coisas e à computação na nuvem. Os sistemas ciberfísicos, que combinam máquinas com processos digitais, são capazes de tomar decisões descentralizadas e de cooperar - entre eles e com humanos - mediante a internet das coisas. (PERASSO, p. 3)

Com as inovações tecnológicas, distâncias foram diminuídas, barreiras foram derrubadas, maior interação e conectividade em escala global foram alcançadas. Disrupções ocorreram e estão ocorrendo, especialmente no sistema financeiro, quando falamos nas criptomoedas. Exemplos dessas novidades tecnológicas atuais são: Inteligência Artificial (IA), robótica, Internet das Coisas (IOT), veículos autônomos, impressão 3D, nanotecnologia, biotecnologia, ciência dos materiais, armazenamento de energia e computação quântica.

A partir desse cenário, as inovações originárias da Quarta Revolução Industrial, na Alemanha, no ano de 2011, na feira de Hannover, foi designado o termo “indústria 4.0”, para detalhar como esta revolução tecnológica irá modificar as organizações das cadeias globais de valor.

O termo “indústria 4.0” irá permitir a existência de “fábricas inteligentes”, ou seja, criará um mundo onde haverá a integração dos sistemas físicos e virtuais, admitindo a assistência em um formato mundial e com maior flexibilidade. Com isso, terá produtos personalizados e a geração de novos modelos de operação.

A “indústria 4.0” não se limita à conexão e inteligência de máquinas e sistemas, e sim vai muito além, propiciando descobertas em várias áreas do conhecimento, permitindo, portanto, a interação, a conectividade, entre as mais diversas áreas, ocasionando experiências à sociedade moderna jamais vistas na história da humanidade.

A quarta revolução industrial, no entanto, não diz respeito apenas a sistemas e máquinas inteligentes e conectadas. Seu escopo é muito mais amplo. Ondas de novas descobertas ocorrem simultaneamente em áreas que vão desde o sequenciamento genético até a nanotecnologia, das energias renováveis à computação quântica. O que torna a quarta revolução industrial fundamentalmente diferente das anteriores é a fusão dessas tecnologias e a interação entre os domínios físicos, digitais e biológicos. (SCHWAB, p.16)

Devemos compreender que as “revoluções” alcançam sua plenitude quando é adotada pelos cidadãos, ou seja, só irá haver evolução quando as novidades tecnológicas forem adotadas pela sociedade. Sabemos que Estados e instituições privadas devem contribuir para a difusão e aceitação da tecnologia, mas esta fundamentalmente precisa ser aceita na medida do possível pela sociedade, do contrário não irá haver “revolução”.

É válido ressaltar que cada vez mais a interação, o compartilhamento de conhecimento serão essenciais para o futuro da sociedade, pois assim possibilitará a construção de valores e objetivos comuns.

O conhecimento compartilhado passa a ser especialmente decisivo para moldarmos um futuro coletivo que reflita valores e objetivos comuns. Precisamos de uma visão compartilhada abrangente e global sobre como a tecnologia tem mudado nossas vidas e mudará a das gerações futuras, e sobre como ela está remodelando o contexto econômico, social, cultural e humano em que vivemos. (SCHWAB, 2016, p. 12)

O teórico Klaus Schwab explica as três razões para afirmar que atualmente estamos vivendo a Quarta Revolução Industrial, que compreende: velocidade, amplitude e profundidade e impacto sistêmico.

Velocidade: ao contrário das revoluções industriais anteriores, esta evolui em um ritmo exponencial e não linear. Esse é o resultado do mundo multifacetado e profundamente interconectado em que vivemos; além disso, as novas tecnologias geram outras mais novas e cada vez mais qualificadas.

Amplitude e profundidade: ela tem a revolução digital como base e combina várias tecnologias, levando a mudança de paradigma sem precedentes da economia, dos negócios, da sociedade e dos indivíduos. A revolução não está modificando apenas o “o que” e o “como” fazemos as coisas, mas também “quem” somos.

Impacto sistêmico: ela envolve a transformação de sistemas inteiros entre países e dentro deles, em empresas, indústrias e em toda sociedade. (SCHWAB, p.13)

Devemos observar que a Quarta Revolução Industrial é uma mudança de paradigma e não só mais uma etapa evolutiva da tecnologia. Possui como uma das características a automatização total das fábricas, propiciada pelos sistemas ciberfísicos, que existem em decorrência da internet das coisas e da computação na nuvem. Uma curiosidade desse sistema ciberfísico é que une as máquinas com processos digitais fazendo com que sejam capazes de

tomar decisões descentralizadas e de cooperar entre si e com humanos por meio da internet das coisas (IOT)

Assim, essa revolução digital propicia disrupções como no sistema financeiro, principalmente quando diz respeito às criptomoedas, especialmente ao Bitcoin, que é totalmente virtual, descentralizado, baseado em consenso da rede, não pertence a nenhum Estado, não há uma autoridade central, com isso a confiança que existe é na rede, permitindo uma maior liberdade de utilização pelo usuário.

1.1 - Internet das Coisas

Em nossos tempos atuais estamos vivendo uma revolução digital, principalmente no que se refere à Internet das Coisas. Mas o que seria a “Internet das Coisas”?

A Internet das Coisas é uma definição que diz respeito à interconexão digital de objetos, coisas, com a internet. É uma interação mais das coisas do que as pessoas com a internet, permitindo que os objetos físicos sejam capazes de reunir e difundir dados.

Por causa do aumento contínuo da capacidade de processamento e a queda dos preços do *hardware* (que ainda está em sintonia com a lei de Moore), é economicamente viável conectar tudo, literalmente, à internet. Sensores inteligentes já estão disponíveis a preços muito competitivos. Todas as coisas serão inteligentes e estarão conectadas à internet, permitindo maior comunicação e novos serviços orientados por dados com base no aumento das capacidades da análise de dados (*analytics*).

(...) 89. A lei de Moore afirma que, em geral, a velocidade dos processadores ou o número de transistores em uma unidade central de processamento dobram a cada dois anos. (SCHWAB, p. 129-130)

Em tempo, é válido ressaltar os impactos positivos e negativos de tal interconexão digital. Klaus Schwab afirma que os impactos positivos são: aumento da eficiência na utilização dos recursos; aumento da produtividade; melhoria da qualidade de vida; efeito sobre o meio ambiente; menor custo de prestação de serviços; maior transparência em torno do uso e estado dos recursos; segurança (por exemplo: aviões, comida); eficiência (logística); maior demanda por armazenamento e largura de banda; mudança no mercado de trabalho e competências; criação de novas empresas; até mesmo os aplicativos em tempo real crítico são viáveis em redes de comunicação padrão; projeto de produtos para que sejam “digitalmente conectáveis”; adição de serviços digitais para os produtos; “gêmeos digitais” (*digital twin*) fornecem dados precisos para monitoramento, controle e previsão; “gêmeos digitais” tornam-se participantes ativos em negócios, informações e processos sociais; as coisas poderão

perceber seu ambiente de forma abrangente e agir e reagir autonomamente; geração de conhecimento adicional e valor com base em coisas “inteligentes” conectadas.¹

A respeito dos pontos negativos da Internet das Coisas, os quais são: privacidade; perdas de emprego para o trabalho não qualificado; *hacking*, ameaça à segurança (por exemplo, rede elétrica); maior complexidade e perda de controle.²

Dessa forma, mesmo havendo pontos positivos e negativos, a Internet das Coisas veio para revolucionar a forma de percepção de mundo e o modo como utilizamos os objetos físicos de nossa era.

1.2 - Revolução Digital

A Revolução Digital é um dos principais propulsores da Quarta Revolução Industrial, pois propicia a abordagem radical de temas, como exemplo a Internet das Coisas e o *Blockchain* (este assunto será abordado mais detalhadamente em capítulo específico). Portanto, o mundo digital está revolucionando o nosso cotidiano. Um outro exemplo que podemos ter é com relação a economia compartilhada, o que permitiu uma forma inovadora de interagir e de consumir bens e serviços.

Em uma escala mais ampla, as plataformas tecnológicas tornam possível aquilo que hoje chamamos de economia sob demanda (chamada por alguns de economia compartilhada). Essas plataformas, fáceis de usar em um *smartphone*, reúnem pessoas, ativos, e dados, criando formas inteiramente novas de consumir bens e serviços. Elas derrubam barreiras para que empresas e indivíduos criem riqueza, alterando ambiente pessoais e profissionais. (SCHWAB, p. 28)

Assim, a “indústria 4.0” está transformando o nosso mundo, com quebras de paradigmas, permitindo a interação entre o ser humano e a máquina ou software, de uma forma ainda não vista na história da humanidade.

¹ SCHWAB, Klaus. **A Quarta Revolução Industrial**. Tradução Daniel Moreira Miranda. São Paulo: Edipro, 2016. p. 131.

² *Ibidem*, p. 132.

CAPÍTULO 2 - A CRISE FINANCEIRA MUNDIAL DE 2008

Para entendermos o surgimento do Bitcoin, precisamos compreender o que aconteceu anteriormente para motivar a criptomoeda a entrar em circulação no mercado. No ano de 2008, ocorreu o colapso do tradicional sistema financeiro mundial devido a uma série de erros, que iremos detalhar em seguida.

2.1 - Fim do “Glass-Steagall Act”

O “GLASS-STEAGALL ACT” foi uma lei instituída nos Estados Unidos da América (EUA) pelo Presidente Franklin D. Roosevelt, no ano de 1933, com o objetivo de evitar um colapso no sistema financeiro norte-americano, como o ocorrido em 1929, ano da “Grande Depressão”.

Essa lei tinha como um de seus objetivos separar as atividades entre os bancos comerciais e os bancos de investimentos, bem como impedir suas afiliações, que seriam juntar os bancos comerciais com os de investimentos.

Como essa separação, ou seja, com a total desvinculação da banca comercial - esta com regulação específica - com a banca de investimento - sem regulação -, o governo dos EUA pretendia proteger os poupadores, principalmente no que diz respeito às operações de compensação bancária.

Dessa forma, os bancos de investimentos não poderiam utilizar o dinheiro dos poupadores depositados nos bancos comerciais em investimentos no mercado financeiro, investimentos estes, muitas vezes, especulativos.

Contudo, com o *lobby* de grandes corporações financeiras, com o discurso de que os Estados Unidos precisavam de bancos maiores e mais expansivos para competirem na era da globalização, então o Presidente Clinton, no ano de 1999, pôs fim a essa lei, afirmando que:

(...) This “historical legislation”, Clinton said at the time, “will modernize our financial service laws, stimulating greater innovation and competition in the financial services industry. America’s consumers, our communities, and the economy will reap the benefits of this. (CASEY E VIGNA p. 61)³

³ Esta “histórica legislação”, Clinton disse na época, “irá modernizar nossas leis de serviços financeiros, estimulando grande inovações e competições na indústria de serviços financeiros. Consumidores americanos, nossas comunidades e a economia vão colher os benefícios disto.” (tradução livre)

Assim, a assinatura do Presidente Clinton colocou fim a lei do “Glass-Steagall” com o discurso do liberalismo econômico, o qual o Estado propõe o “Estado-mínimo”, ou seja, o menos interventor possível, e acelerou o processo para uma das maiores crises financeiras que o mundo viu em oitenta anos.

2.2 - Liberalismo Econômico

O Liberalismo Econômico é uma ideia preceituada que surgiu no século XVIII, tendo como principal representante o teórico escocês Adam Smith, o autor da famosa expressão “mão invisível”. Também temos como representantes dessa teoria, Thomas Malthus e David Ricardo.

A teoria do Liberalismo Econômico preconiza:

- a) a não intervenção do Estado na economia;
- b) Estado-mínimo;
- c) a livre concorrência;
- d) a propriedade privada; e
- e) o câmbio livre.

Quando Adam Smith utilizou a expressão “mão invisível”, ele explicou, por meio de uma metáfora, a ideia de intervenção mínima do Estado na economia. Assim, o Estado deveria ser apenas um observador e aparar as arestas do mercado quando fosse necessário, mas deveria deixar o interesse pessoal, ou seja, o interesse do mercado, se autorregular. Portanto, o Estado não deveria regular o mercado, e sim ser um mero expectador, permitindo a livre concorrência. Os teóricos liberais entendiam que, somados os interesses pessoais de cada um, ocorreria o benefício de toda uma sociedade. Dessa forma, passaram essa ideia para o mercado.

O papel do interesse pessoal. A “mão invisível” é uma forma sintética de expressar a lei da oferta e da demanda (veja o capítulo 2), e explica como o “puxa e empurra” desses dois fatores serve para beneficiar toda a sociedade. Em termos simples, o conceito é o seguinte: não há nada de errado se as pessoas agem em interesse pessoal. Num mercado livre, a força combinada de todos que lutam por seus interesses individuais beneficia a sociedade como um todo, enriquecendo todos. Smith usou a frase apenas três vezes em sua obra-prima *A riqueza das nações*, de 1776, mas um trecho fundamental realça sua importância:

[o indivíduo] não tem a intenção de promover o interesse público, nem sabe o quanto promove... ao dirigir [sua] atividade de maneira a valorizar ao máximo a sua produção, visa apenas seu próprio lucro, e nisto, como em muitos outros casos, é

guiado por uma mão invisível a promover um fim que não fazia parte de sua intenção... Ao buscar seu interesse pessoal, frequentemente ele promove o da sociedade de maneira mais eficiente do que quando de fato tem a intenção de promovê-lo. Nunca soube de bons feitos por parte daqueles que afetam as trocas em nome do bem público. (CONWAY, p. 10 e 11).

A partir da ideia de “mão invisível”, podemos observar o fato de os mercados livres serem tão importantes para a evolução de sociedades modernas complexas, bem como também a expressão “*Laissez Faire, Laissez Passer*”- deixai fazer, deixai passar -, ideia esta também difundida pelos liberais econômicos, pois para eles o próprio indivíduo é o agente econômico. Desse modo, o Estado não deve intervir na economia com muitas normas, pois, se houver alguma desconformidade, será o próprio mercado quem corrigirá, ou seja, o mercado se autorregulará, cabendo ao Estado, na ideologia liberal, ser um mantenedor da ordem, da paz e da propriedade privada.

A ideologia liberal, no que tange a livre concorrência, difundiu o pensamento de que o comércio produz, fixa preço e comanda a qualidade da produção. De acordo com a lei da oferta e da procura, o próprio mercado se autoajustaria, observando a demanda, e fixa o valor dos produtos, não havendo, portanto, a interferência do Estado. Já no que concerne ao câmbio livre, a ideologia liberal refere-se ao fato de derrubar as tarifas alfandegárias, as quais levam ao protecionismo por parte do Estado.

2.3 - Falta de Regulação

Baseado nos ensinamentos do Liberalismo Econômico, ou do Neoliberalismo, como foi chamado na década de 90, o Presidente Clinton extinguiu com a lei “Glass-Steagall”, permitindo, portanto, o liberalismo financeiro e monetário, suprimindo nos EUA as barreiras entre os bancos de depósitos e os bancos de investimentos, desencadeando uma ultraliberação das atividades bancárias, com a utilização indevida de técnicas financeiras.

A ideia do Estado-mínimo, menos interventor, com a mínima regulação possível, permitiu que instituições financeiras nos EUA - estas se autorregulavam - atuassem com a menor regulamentação possível.

Os reguladores não viram nenhuma necessidade de regulação das atividades bancárias paralelas antes da crise. Argumentavam que, sem garantias bancárias explícitas, a ameaça de falência imporia “disciplina de mercado” suficiente às instituições financeiras que operavam fora do setor bancário regulado. Na medida que a securitização e os canais de ABCP aparentemente afastavam o risco de crédito

dos bancos, a inovação financeira era percebida como um fator de estabilização do sistema financeiro e da economia.(MCMILLAN, p. 91)

Diante desse cenário de pouca, ou quase nenhuma regulação por parte do governo norte-americano, instituições financeiras norte-americanas começaram a aplicar técnicas financeiras indevidas dentro e fora dos Estados Unidos da América, tornando também globais os seus investimentos.

Mas quais técnicas financeiras seriam essas? São as chamadas atividades bancárias paralelas, que serão abaixo estudadas.

2.4 - Atividades Bancárias Paralelas

Com o advento da revolução digital na década de 70, os bancos deixaram de controlar suas atividades bancárias tradicionais de forma manual - digo, papel e lápis -, e passaram a fazer seus balanços patrimoniais de forma digital.

A tecnologia adotada pelos bancos tem seus benefícios e seus malefícios. No que se refere aos benefícios, permitiu uma maior agilidade nas atividades bancárias. Sobre os malefícios, permitiu aos mesmos que praticassem atividades às escondidas das autoridades, conseguiam simplesmente, com a ajuda da tecnologia, manipular números, pois os bancos manipulavam estruturas financeiras mais complexas, possibilitando vários níveis de balanços patrimoniais. Dessa forma, *“os bancos se tornaram capazes de fatiar, picar e redistribuir o crédito, através de uma cadeia de balanços patrimoniais, a custos desprezíveis.”* (MCMILLAN, p. 67).

Com a tecnologia da informação e a revolução digital, os bancos exploraram diversas formas de oportunidades de realizarem suas atividades, e, diante desse cenário, podemos observar a ascendência das atividades bancárias paralelas.

Neste livro, eu adoto exclusivamente para denotar a criação de moeda por meio do crédito, fora do setor bancário tradicional. O adjetivo “paralelo”, aqui, refere-se a atividades bancárias executadas na sombra, ou seja, fora dos holofotes dos reguladores bancários.(MCMILLAN, p. 67)

A partir da atuação nas sombras que grandes instituições financeiras norte-americanas começaram a operar dentro e fora dos EUA, manipulando números, com essa forma de operação, balanços patrimoniais começaram a ser manobrados, ou seja, nem todas as atividades ficavam registradas nos balanços patrimoniais, permitindo, portanto, atividades

especulativas e, sem controle, não reguladas, visto que as atividades bancárias eram reguladas pela denominada *regulação Q*⁴.

Mas o que seria essa *regulação Q*? Na década de 1970, os bancos tradicionais estavam subordinados a um teto na taxa de juros que podiam oferecer aos depositantes, a chamada *regulação Q*, regulada pelo Estado. Tal *regulação* não era atraente, principalmente em épocas de alta inflação, onde ocorre o aumento dos juros, pois os impediam de atrair os depósitos dos clientes.

Assim, seria mais conveniente aos bancos migrarem para as *atividade paralelas*, ou seja, atuarem nas sombras, pois às escondidas não há a interferência do Estado, permitindo, portanto, que as instituições financeiras criassem as suas próprias regras.

Um mecanismo criando para atuar às escondidas foi o surgimento de uma forma de instituição financeira, os chamados *Fundos de Investimento em Renda Fixa (MMF)*. Estes ofertavam algo muito parecido com os depósitos bancários, mas, como estas instituições ofertavam uma semelhança de depósito, não eram classificados como bancos, e, portanto, não eram regulados, não estavam subordinados ao teto das taxas de juros, oferecendo, então, retornos mais elevados que o dos próprios bancos.

Os MMFs eram uma alternativa atraente, porque não estavam sujeitos à *regulação* bancária. Mas eles *são apenas uma parte* das atividades bancárias paralelas. Na década de 1970, surgiram novas instituições financeiras que, em conjunto, prestavam atividades bancárias - criando moeda por meio do crédito - sem estar sujeitas à *regulação* bancária. Ao mesmo tempo, as atividades bancárias paralelas possibilitavam que os bancos contornassem a *regulação* bancária. (MCMILLAN, p. 69)

É válido ressaltar que o Comitê de Supervisão Bancária de Basileia, na Suíça, sobre os requisitos de capital impostos, regulavam os bancos e não suas atividades bancárias, o que na verdade foi uma grande falha, mas infelizmente ocorreu. Dessa forma, praticavam o chamado *arbitragem do capital regulatório*.

Requisitos de capital tipo Basileia I fracassaram porque regulavam os bancos, não atividades bancárias. Os bancos transferiam ativos para balanços patrimoniais remotos, ao mesmo tempo que mantinham o risco econômico. Também desenvolviam as relações com os balanços patrimoniais remotos, de modo que os requisitos de capital não se aplicassem aos ativos lá mantidos. Em consequência, contornavam os requisitos de capital e aumentavam a tomada de riscos, sem arriscar a própria pele. Esse comportamento é denominado *arbitragem de capital regulatório*. (MCMILLAN, p. 69)

⁴ MCMILLAN, p. 68.

Dessa forma, os bancos criaram uma forma de burlar a regulação e a fazerem operações que não eram demonstradas em seus balanços patrimoniais, criando uma falsa existência de liquidez, pois a criação de moeda interna na forma de depósito bancário é como se desenvolve as atividades bancárias tradicionais, sendo necessário ter as três características dos depósitos bancários para ser ter moeda, liquidez, que são: *“Primeiro, eles apresentam a mesma divisibilidade da moeda externa, ou seja, têm a mesma denominação da moeda externa, ou dinheiro corrente. Segundo, são percebidos como livres de risco. Terceiro, têm a mesma liquidez da moeda externa.”* (MCMILLAN, p. 71)

Assim, os bancos começaram a possuir menos patrimônio líquido, o que, infelizmente, ocorreu no ano de 2008 em um colapso no sistema financeiro mundial.

2.5 - Classificação de Risco de Crédito (Agências de Classificação)

Com a falta de regulação e o crescente aumento das atividades paralelas realizadas pelas instituições financeiras, era necessário que alguém classificassem os riscos de créditos dos ativos, e esse papel cabe às agências de classificação, como: Fitch, Moody's e Standard & Poor's, por exemplo.

Note 7- Agences de Notation

Il faut revenir un peu en arrière dans le temps, à l'aube des agences de notation. L'Agence Poor qui précéda Standard and Poor était un éditeur de données chiffrées. De même pour Moody's et Fitch. Au début du siècle dernier et même à la fin du siècle précédent, il existait des journaux d'information destinés à des décideurs dans les entreprises. Leurs lecteurs payaient au numéro ou sur abonnement pour avoir à leur disposition les données, les chiffres, les prix, rassemblés sur une parution.

Beaucoup plus tard, les agences se sont lancées dans la vente d'information qualifiée via les exercices de notation. Il s'agissait d'ajouter de la valeur à l'information primaire et brute. En plus de montrer les bilans des entreprises pétrolières, les agences d'information économique proposèrent de vendre des jugements... Donc les clients des agences payaient pour des informations sur d'autres entreprises.

Les Agences de notation « notent » donc les entreprises et toutes les institutions. Elles ont par la suite ajouté à ces notations des notes sur les actifs en tous genres, actions, obligations, prêts etc. et subprimes.

On a attribué une part de la crise de 2008 à leurs opinions trop souvent positives sur les titrisations de subprimes. (ORDONNEAU, p. 31)⁵

⁵ Nota 7 - Agências de Classificação

Precisamos voltar um passo atrás no tempo, no alvorecer das agências de classificação. A agência Poor que precedeu a Standard and Poor era uma agência igual a Moody's e Fitch. No início do século passado, e mesmo no final do século passado, havia jornais de notícias destinados a tomadores de decisão das empresas. Seus leitores pagavam por edição ou por assinatura para ter à disposição os dados, os números, os preços, reunidos na publicação. Muito tempo depois, as agências de classificação se lançaram na venda de informações, por meio dos exercícios de pontuação. Elas começam a adicionar valor para as informações primárias e brutas. Além de mostrar os balanços de companhias petrolíferas, as agências de informação econômica propuseram a vender julgamentos... Então os clientes da agência estavam pagando por informações de outras empresas. As agências de classificação, portanto, forneciam “graus” às empresas e a todas as instituições. Subsequentemente,

Mas, para que houvesse essa classificação, alguém tinha que financiar essas agências, e quem financiava eram as próprias instituições financeiras (emitentes). Para não perder clientela, essas agências foram muito benéficas em classificar ativos tóxicos, ou seja, ativos que na verdade não tinham liquidez, afirmando que estes eram bons para investir, o que na verdade não eram.

O risco moral na avaliação dos produtos de atividades bancárias paralelas resultou em avaliações quase sempre muito generosas. Os emitentes sabiam das deficiências das agências e as exploravam sistematicamente ao conceber novos produtos de atividades bancárias paralelas. Assim, conseguiram obter as avaliações mais altas possível, apesar dos riscos elevados. As agências não avaliavam os verdadeiros riscos econômicos dos produtos. (MCMILLAN, p. 95)

Diante dessa classificação irreal dos ativos, investidores ao redor do globo, fundos de pensão, autoridades internacionais, principalmente europeias, e bancos internacionais, aplicaram em ativos tóxicos, que foram classificados pelas agências em *rating* “AAA” ou “AA”, ou seja, de ativos de baixo risco. Dessa forma, como grande parte desses investidores não observavam a qualidade dos ativos que lastreavam esses títulos, muitos formavam suas assimilações, por meio da classificação dada pelas agências de classificação de risco. Assim, por meio dessa classificação manipulada, deflagrou-se a maior crise financeira e econômica dos últimos oitenta anos.

2.6 - Balanços Patrimoniais Não Computados

Como explicamos anteriormente, as atividades paralelas não eram descritas nos balanços patrimoniais que eram fiscalizados pelo Estado, desse modo existiam balanços patrimoniais remotos (*off balance*), o que dificultava as autoridades em saber se aquela instituição financeira tinha liquidez para cumprir com as suas obrigações.

2.7 - A Crise dos *Subprimes*- A Bolha Especulativa

A partir da ânsia das instituições financeiras por mais lucros e dos sucessivos erros expostos nos itens anteriores, temos a deflagração da maior crise financeira e monetária dos

adicionaram a essas notas de *ratings* ativos de todos os tipos, ações, títulos, empréstimos, etc. e subprime. Parte da crise de 2008 foi atribuída às suas opiniões com demasiadas frequências positivas nas titularizações dos *subprimes*. (tradução livre)

últimos oitenta anos. Mas para detalharmos a respeito da crise, precisamos compreender o que significa *subprime*.

O *subprime* é um termo norte-americano para classificar o tomador de empréstimo e o nível de capacidade de pagamento de suas dívidas. No caso, o *subprime* é um produto de segunda linha.

Note 6 - Subprime

Terme financier américain : les subprimes sont des prêts consentis à des emprunteurs dont la capacité de remboursement est jugée plus faible que celle d'un benchmark : le prime lending. Les emprunteurs « subprime » sont moins fiables et se voient appliquer des taux plus élevés.

En fait, les banques américaines considéraient que l'augmentation des prix de l'immobilier, réguliers depuis des années, permettraient de rembourser les prêts consentis. Or, les prix de l'immobilier stagnèrent puis s'effondrèrent. En 2007, au début de la crise, trois millions de foyers américains étaient en situation de défaut de paiement en raison de crédits distribués sans tenir compte de leurs capacités de remboursement.

L'impact financier des subprimes a surgi lorsqu'il fut mis au jour que les portefeuilles de crédits subprimes avaient été « titrisés », dotés de notation tout à fait flatteuses de la part des agences de notation les plus célèbres. Cette titrisation transformant les prêts en placements sécurisés, de nombreux investisseurs furent pris au piège de l'effondrement du marché immobilier américain créant une spirale des faillites bancaires sans précédent. (ORDONNEAU, p. 30)⁶

A partir da compreensão do que é o *subprime*, podemos começar a desenvolver como iniciou-se a crise de 2008. É válido ressaltar que o surgimento de bolhas no preço de ações, ativos imobiliários ou qualquer outro ativo, advém de uma movimentação de aumento excessivo e no desaperto monetário. Dessa forma, a bolha dos ativos imobiliários deu-se dessa maneira, no período de 2001 a 2007.

A bolha no mercado imobiliário começou a crescer quando o FED (Federal Reserve), o Banco Central dos Estados Unidos da América, após os atentados de 11 de setembro no

⁶ Nota 6 - *Subprime*

Termo financeiro americano: *subprime* são concedidos aos mutuários cuja capacidade de pagamento é considerada inferior a de um *benchmark*: empréstimos prime. Mutuários “subprime” são mais baixos e estão sujeitos a taxas mais altas.

Na verdade, os bancos dos EUA consideraram que o aumento de preço imobiliário, regular durante anos, tornaria possível reembolsar empréstimos feitos. Mas os preços dos imóveis estagnaram e depois entrou em colapso. Em 2007, no início da crise, três milhões de lares americanos estavam em falta por causa de créditos distribuídos independentemente de sua capacidade de reembolso. O impacto financeiro do *subprime* surgiu quando foi descoberto que carteiras de empréstimos *subprime* haviam sido “securitizadas”, com uma classificação muito lisonjeira das agências de classificação mais famosas. Esta securitização transforma os empréstimos em investimentos seguros, muitos investidores ficaram presos pelo colapso do mercado imobiliário americano, criando uma espiral de falências bancárias sem precedentes. (tradução livre)

World Trade Center, em Nova York, diminuiu as taxas de juros; e de setembro de 2001 a abril de 2006, o valor das casas subiram em média 75% nos EUA.⁷

Diante desse cenário de ascensão do mercado imobiliário, diversos bancos de investimentos observaram uma grande forma de ganharem dinheiro, por intermédio de operações de securitização, uma forma de atividade bancária paralela realizada pelas instituições financeiras.

A base das atividades bancárias paralelas é a concessão de empréstimos. Para criar moeda interna, primeiro é preciso oferecer crédito. As atividades bancárias, paralelas e tradicionais, divergem nisto. Os empréstimos que atuam como “matéria-prima” nas atividades bancárias paralelas foram concedidos por bancos tradicionais ou por outras instituições financeiras. Um empréstimo isolado é, em geral, um tanto arriscado, e a securitização trata dessa questão. (MCMILLAN, p. 76)

Mas o que seria a securitização? A securitização é a soma de três técnicas financeiras: agregação, diversificação e estruturação.

Assim, a securitização se refere ao seguinte: uma instituição financeira custeia uma empresa de responsabilidade limitada, chamada de *sociedade de propósito específico* (SPE). Essa SPE é uma empresa legal que não tem produção, não emprega pessoas e não oferece serviços. É um balanço patrimonial remoto que irá comprar diversos ativos, sem liquidez, do banco que a patrocinou, que a custeou, sendo que no balanço patrimonial, no lado do ativo, não irá diferir de uma instituição financeira, como, por exemplo, um banco. Mas o seu lado do passivo é diferente de um banco.

Com isso, a SPE não lança depósitos bancários, dessa forma não sofre influência de regulação estatal. O que ela faz é emitir dívidas no formato de títulos, que são lastreados em ativos, os chamados ABS (*asset-backed security*), e esse lastro está no lado ativo, no formato de empréstimo.

Dessa forma, a instituição financeira patrocinadora transformou seus empréstimos sem liquidez em valor nominal, na SPE, que transformou a dívida/empréstimo em ABS, ou seja, a instituição financeira começa a vender no mercado um título ABS que tem uma falsa liquidez, o que na verdade não tem nenhuma liquidez. Contudo, um investidor mais astuto irá ficar em dúvida se tal título é bom ou não. Com isso, a instituição financeira faz uma outra modificação financeira, chamada CDO (*collateralized debt obligation*), ou seja, a instituição financeira coloca esses ABS dentro de um novo título, um CDO, e, posteriormente, em outro

⁷ DAMAS, Roberto Dumas. **Crises Econômicas Internacionais**. São Paulo: Saraiva, 2017. p. 270.

CDO. Isso é chamado de - *trancheamento* -, dívidas transformadas em títulos, que na verdade não tem nenhum valor, mas a instituição vende para o mercado como um título bom, com liquidez, mas na realidade o título é uma dívida.

A instituição patrocinadora enfrenta esse problema com outra técnica financeira, ela estrutura o lado do passivo da SPE. A instituição patrocinadora tipicamente mantém um *tranche* (ou parcela de patrimônio líquido) e, portanto, sofre as primeiras perdas se a qualidade do empréstimo for ruim. O lado do passivo da SPE pode ser estruturado ainda mais mediante a emissão de ABS com diferentes graus de preferência ou privilégio. Em termos financeiros, isso é denominado *trancheamento*, parcelamento, ou fatiamento. A *tranche* com mais alta preferência ou privilégio é atendida primeiro; depois a com segundo nível de preferência, e assim por diante. Finalmente, as diferentes *tranches* de ABS são avaliadas por uma agência de classificação de risco de crédito, para oferecer uma avaliação independente de que a transformação foi bem-sucedida. (MCMILLAN, p. 78)

Assim, o processo de securitização é o empacotamento de dívidas transformada em título e distribuído no mercado financeiro, tornando a dívida/empréstimo em moeda, despersonalizando o credor, podendo ser negociada livremente via título. O que concede valor ao título/ativo é a qualidade do crédito. Crédito bom é aquele em que a remuneração é em linha com o índice do mercado ou abaixo do mercado, devido à alta capacidade de pagamento do emissor, ou pelo fornecimento de garantias. Já o crédito ruim é aquele em que o prêmio/retorno é proporcional ao risco.

Com essas explicações iniciais, temos base para compreender o que levou a crise de 2008.

A crise financeira internacional, que se iniciou na Islândia em 2008 e, posteriormente, atingiu os EUA e outros países, foi denominada “*crise dos subprimes*”. Entretanto, foi nos EUA aonde começou todo o caos financeiro gerado pela falta de regulamentação das instituições financeiras no mercado imobiliário. Os *subprimes*, ou *hipotecas subprimes*, configuravam empréstimos hipotecários com alto risco e com taxas variáveis que foram concedidos a pessoas e famílias que, de antemão, não teriam condições para pagar, pois não possuíam renda, não possuíam emprego e não tinham patrimônio; os financiamentos concedidos para a compra de casa, muitas vezes atrelados à emissão de cartão de crédito, a pessoas que não tinham a menor condição de adimplir com as obrigações.

A partir desses títulos de hipoteca, as instituições financeiras criaram derivativos possíveis de serem negociados no mercado financeiro e encontraram uma forma de securitizarem, transformando a dívida em títulos possíveis de serem negociados, lastreados pelas instituições financeiras criadoras e vendidos a investidores ao redor do planeta.

As agências de classificação de risco, como: Standard & Poor's, Moody's e Fitch, classificaram esses títulos como *AAA*, a mais alta, significando títulos bons. Essas agências, como explicamos anteriormente, subverteram o real valor do título, passando uma informação enganosa para o mercado financeiro mundial.

Exemplificando: uma pessoa sem condições financeiras obrigava-se não a uma, mas a várias hipotecas, sendo que não tinha condições de ter uma, tinha seis, por exemplo. Como não havia regulação que impedisse essa pessoa de adquirir várias hipotecas, conseqüentemente não se observava a saúde financeira dela. Nesse cenário, a instituição financeira toma essas dívidas e as transformam em títulos líquidos, CDO's, e as vendiam no mercado. O investidor comprava esses títulos, ranqueados em *AAA*, pensando que seriam títulos bons e líquidos, o que não era verdade.

Com isso, por situações adversas, como desemprego ou descontrole financeiro, as pessoas deixaram de pagar os empréstimos garantidos por hipotecas, e instituições financeiras que venderam os títulos deixam de ter patrimônio líquido para retornar os prêmios aos investidores.

É válido ressaltar que esses títulos tóxicos foram vendidos para o mundo inteiro, tendo, portanto, como investidores, Estados, bancos, outras instituições financeiras, fundos de investimentos e pessoas físicas.

Quando os títulos de hipoteca começaram a não serem pagos, devido à modificação do valor da taxa de juros pelo FED (Banco Central dos EUA) para controlar a inflação, começou a ocorrer um efeito dominó, começando, assim, a crise no sistema financeiro internacional.

Nos EUA, ocorreu a falência de instituições financeiras importantes, como o banco Lehman Brothers, e a seguradora American International Group (AIG), bem como a quase falência das agências de créditos imobiliários Fannie Mae e Freddie Mac. Conseqüentemente, a reação em cadeia foi atingindo vários outros setores e países, tornando, portanto, uma crise financeira global. Com isso, milhões de pessoas, só nos Estados Unidos da América, ficaram sem moradia e desempregadas.

A fim de salvar a sua economia, o governo norte-americano, por exemplo, teve que injetar dinheiro em diversas instituições financeiras para evitar suas falências e o conseqüente colapso no sistema financeiro, como, Fannie Mae, Freddie Mac, e Bank of America.

No meio desse caos houve investidores que observaram, ao longo dos anos, essa falha criada pelas instituições financeiras e lucraram apostando contra o sistema, onde investiram bilhões na queda dos ativos imobiliários.

Podemos perceber a fragilidade do sistema financeiro permitindo que instituições financeiras fizessem manobras com o dinheiro do poupador, restando ao governo norte-americano ajudar essas instituições financeiras com o dinheiro do contribuinte, que foi usado para um dos maiores resgates financeiros da história.

2.7.1 - Alternativas Após a Crise dos “Subprimes”

Diante do cenário de crise financeira mundial, no ano de 2008, onde o sistema financeiro tradicional entrou em colapso, fez surgir a criptomoeda chamada Bitcoin - estudaremos em capítulo específico -, com o intuito de libertar seus usuários da dependência do sistema financeiro tradicional, permitindo que os mesmos sejam livres para fazer transações financeiras sem a necessidade de estarem sob a influência do Estado ou de um banco para a existência da transação. Dessa forma, haverá um método mais disruptivo que irá de encontro aos métodos preconizados pelo sistema financeiro tradicional.

CAPÍTULO 3 - MOEDA

Antes de iniciarmos o estudo da criptomoeda Bitcoin, precisamos entender o que significa moeda.

Desde os tempos mais antigos, o homem, para suprir suas necessidades, sempre buscou adquirir coisas, objetos, bens. Nos tempos mais antigos, para aquisição de qualquer suprimento ou objeto, faziam pura e simplesmente a troca direta, ou seja, uma coisa pela outra, o chamado *escambo*.

Com o advento das civilizações, essa “*troca*”, realizada na forma direta, tornou-se ineficaz, precisando ser aprimorada e necessitando de algo para mensurar o real valor de cada bem, assim como demandava-se ter algo tangível que funcionaria como meio de troca/pagamento.

(...) Por meio deste instrumento, os excedentes de um grupo eram trocados pelos de outro, em função da necessidade recíproca por tais excedentes, o que posteriormente chegou a provocar problemas relativos à falta de equivalência entre os bens a serem objeto de troca. Assim, objetivando atenuar este problema, foram erigidos instrumentos que serviriam de referências para regulamentar as trocas, os chamados instrumentos de pagamento. Em função da evolução do comércio, passou-se desde a utilização de animais, sal, metais preciosos, até a utilização da moeda dotada de curso legal. (FINKELSTEIN, p. 2)

Nesse contexto, surgiu a *moeda*, uma coisa palpável, que teria como finalidade ser, ao mesmo tempo, uma referência para quantificar o valor de cada bem adquirido ou serviço prestado, tal como um meio de troca/pagamento.

A maior desvantagem da troca direta é o facto de ela depender de uma “dupla coincidência de desejos”. Um caçador que deseje trocar as suas peles por milho deverá encontrar não apenas alguém que deseje peles, mas alguém que deseje peles e que disponha de um excedente de milho para trocar. A alternativa é trocar as suas peles por um outro produto e, depois, proceder a uma série de trocas até conseguir, finalmente, obter o milho. O tempo e a energia que poderiam ser utilizados na produção são gastos num complicado sistema de trocas.

O homem descobriu bastante cedo um método muito mais conveniente. A utilização de uma mercadoria como meio de troca transforma a troca num processo triangular e elimina a principal dificuldade da troca direta. Se uma mercadoria for geralmente aceite em troca de bens e serviços, ela é moeda. Um produtor troca agora os seus bens por moeda e a moeda pode depois ser trocada pelos bens e serviços de que ele necessita. (STANLAKE, p. 433-434)

Ainda dissertando a respeito da conceituação de moeda, Nilson Holanda, em sua obra *Introdução à Economia*, aduz que:

Considera-se **moeda** qualquer coisa que, em determinada sociedade, funciona como meio de pagamento, instrumento geral de troca e medida comum de valor. Robertson diz que moeda é “tudo o que é geralmente aceito em pagamento de mercadorias ou no cumprimento de quaisquer outras obrigações comerciais”, enquanto Hart define-a como “a propriedade que pode ser utilizada por seu dono no pagamento de débitos de valor definido, com segurança e sem demora”. Boulding, por sua vez, afirma que constituem dinheiro “aqueles bens ordinariamente trocados por uma grande variedade de outros bens e que são aceitos principalmente por causa da crença em sua contínua capacidade de assim serem trocados. (HOLANDA, p. 574, 575)

Além de ser uma referência e um meio de pagamento, a **moeda** possui também uma característica essencial, primordial, a questão do **aceite**. O **aceite** é a aprovação por parte da sociedade e de sua economia de que aquela coisa é o meio e a referência para se adquirir bens e serviços. Esse **aceite** será garantido pelo Estado, contudo a aceitação da moeda não advém unicamente da imposição legal do Estado. É válido ressaltar que a aceitação da **moeda** possui muito a necessidade de ser aprovada pela comunidade a qual há a sua circulação.

A característica essencial da moeda é o facto de ela ser *geralmente aceite*. Se um meio de troca não for livremente aceite por todos, nenhum produtor se arriscará a aceitá-lo em troca dos seus produtos. Ele tem de ter confiança em que a “moeda” irá, por sua vez, ser aceite pelos vendedores dos bens que ele deseja comprar. (STANLAKE, p. 434)

Uma outra característica interessante da **moeda** é o fato desta ter um poder liberatório. Esse poder diz respeito ao fato de se poder saldar dívidas, haver a liquidação de débitos, permitir que o agente econômico se liberte de débitos auferidos em razão de manter sua subsistência, ou em consequência de sua atividade econômica, ou simplesmente devido pelo fato de gastar, despender de sua riqueza.

A moeda como nenhum outro ativo detém um poder que a distingue de quaisquer outras formas de riqueza possuídas por um agente econômico - o poder de saldar dívidas, de liquidar débitos, de livrar seu detentor de uma situação passiva. Dá-se a esta particularidade da moeda a denominação de *poder liberatório* ou *função liberatória*. (LOPES E ROSSETI, p. 22)

A **moeda** é um instrumento muito utilizado na vida cotidiana, é elemento essencial em uma civilização, é a instituição da economia de troca, é uma forma de dinheiro, sendo que a moeda passa a quitar dívidas. Atualmente, no século XXI, com o avanço da tecnologia, a moeda está no formato eletrônico e também no formato virtual (as chamadas criptomoedas).

La monnaie est l'un des instruments les plus utilisés dans notre vie quotidienne. En ce sens, elle peu être définie comme une institution caractérisant l'économie d'échange. Il est également possible de la présenter en insistant soit sur ses fonctions spécifiques, soit sur les propriétés qu'elle doit nécessairement remplir pour jouer complètement son rôle. Ces approches, non exclusives les unes des autres sont

complémentaires. Montrant la complexité du phénomène monétaire, chacun d'elles met l'accent notamment sur la manière dont celui-ci joue son rôle dans l'économie. Plus récemment, les nouvelles technologies ont fait émerger de nouveaux instruments de circulation, tels que la monnaie virtuelle, qui présente de nouveaux défis, de nature différente, au système bancaire et aux banques centrales. (DEMBIK e RUIFY, p. 7)⁸

Desse modo, a moeda, que é um elemento do nosso cotidiano, pode se apresentar de várias formas, por meio de suas funções específicas ou nas propriedades a qual se faz necessário cumprir para desempenhar plenamente o seu papel. É importante destacar que a tecnologia vem mudando a forma como entendemos as funções e propriedades da moeda, pois conseguimos novas ferramentas de circulação, a exemplo das moedas virtuais, e apresentam novos e diferentes desafios ao sistema financeiro internacional.

3.1 - Tipos de Moeda

3.1.1 - Metal/Papel - Moeda/Moeda Eletrônica

Desde os tempos mais antigos até os dias de hoje, metais como o ouro, a prata e o bronze foram matéria-prima para a cunhagem das moedas, mas, atualmente, na sua composição, há também outros metais que formam a moeda. A moeda em metal é cunhada pela autoridade oficial, o Estado.

O papel-moeda é uma outra forma de se ter a *moeda*, pois neste formato ficou mais fácil utilizar e armazenar, não se fazendo necessário usar um grande volume de moeda em metal, visto que, por exemplo: uma nota de R\$ 10,00 (dez reais) elimina a necessidade de se carregar uma enorme quantidade de moeda em metal, a fim de alcançar o valor total, (R\$ 10,00). O papel-moeda é emitido pela autoridade oficial, o Estado.

Devemos mencionar uma outra forma de moeda em papel, que é o cheque, na qual o titular preenche um valor, não sendo necessário, portanto, carregar uma grande quantidade em moeda de metal e papel-moeda.

⁸ O dinheiro é um dos instrumentos mais usados em nossas vidas cotidianas. Nesse sentido, pode ser definido como uma instituição, caracterizando a economia de troca. Também é possível apresentá-lo insistindo em suas funções específicas ou nas propriedades que ele necessariamente deve cumprir para desempenhar seu papel completo. Essas abordagens não são exclusivas uma das outras, são complementares. Mostrando a complexidade do fenômeno monetário, cada um deles coloca sua notoriedade na maneira que este joga seu papel na economia. Mais recentemente, novas tecnologias fizeram emergir novos instrumentos de circulação, como o dinheiro virtual, que apresenta novos desafios de natureza diferente para o sistema bancário e para os bancos centrais. (tradução livre)

Com o advento da tecnologia, muitos instrumentos tiveram que mudar, se adaptar ou se reinventar, um deles foi a *moeda*. O novo formato adquirido nessa era da tecnologia foi o eletrônico, onde as moedas estatais continuam sendo elas mesmas, mas no formato eletrônico, por exemplo, no cartão de crédito ou em uma transferência eletrônica; o real, o dólar, o euro, continuam sendo eles, a diferença é que a moeda não precisa ser mais palpável, ela pode se “transformar”, e essa transformação é eletrônica. Milhares de transações financeiras são realizadas diariamente ao redor do mundo, sem a necessidade de se carregar quantias de um lado para outro, facilitando e tornando mais eficaz as trocas financeiras, e elas podem ser realizadas por meio do sistema de uma instituição financeira com apenas um clique no computador, tablet ou aplicativo do celular, do relógio. Essa forma de transacionar, sem dúvida, é um fenômeno revolucionário.

3.1.2 - Moeda Virtual (Criptomoeda)

No tópico anterior, dissemos que a moeda eletrônica é um formato revolucionário. Já a *moeda virtual*, ela não é somente revolucionária como a moeda eletrônica, é mais do que isso, é disruptiva.

Mas o que seria *disrupção*? Esta ideia advinda a partir do surgimento das criptomoedas é o entendimento de mudança de paradigma, é a criação de algo novo, de algo sem precedentes.

O que é ser, na essência, disruptivo? Entendemos que ser disruptivo é romper, interromper a sequência, ou segmento natural de um processo: em termos tecnológicos, a disrupção ocorre quando uma inovação tecnológica, seja esta um produto ou serviço, interrompe uma tecnologia já existente e dominante, ou seja, em vez de a nova tecnologia ser uma evolução da precedente, ela é a interrupção e a criação de um novo sistema. (BORGES, p.121)

As criptomoedas trouxeram um novo formato no que diz respeito a forma como utilizamos o dinheiro, bem como do que entendemos por dinheiro. Na verdade, as *criptomoedas* passaram a ser a “*internet do dinheiro*”, expressão essa difundida por Andreas Antonopoulos, professor e um entusiasta do mundo cripto e da tecnologia *blockchain*.

As criptomoedas, como a etimologia da palavra diz, tem como base a criptografia. A criptografia é a utilização de códigos muito difíceis de serem “quebrados”, decodificados, tornando, portanto, o seu sistema mais eficaz e seguro.

As criptomoedas surgiram em um momento de descontentamento com a economia. Os chamados “*Cyberpunkes*”, um movimento *online* da década de 1990, que tinham como seus componentes: matemáticos, hackers, entusiastas da tecnologia e criptoanarquistas, desenvolveram as criptomoedas. Este movimento tinha o objetivo de usar a criptografia para forçar mudanças políticas e culturais. Foram eles que iniciaram o caminho para a criação dos chamados “*espaços invisíveis*” da internet. No entanto, com as crises econômicas que atingiram esse período, a sociedade moderna, o grupo passou a visar uma forma de ir de encontro ao sistema financeiro tradicional e permitir que houvesse uma maior liberdade individual, um maior poder de escolha, sendo as criptomoedas uma forma de confrontar o tradicional sistema financeiro.

(...) Cyberpunk movement, a loose association of tech-minded activists who had first gained notoriety in the 1990s with their efforts to use cryptographic privacy tools to force radical political and culture change. This effort bore some fruit: transparency crusader Julian Assange and his activist publishing organization, WikiLeaks, grew out this movement. (J. CASEY e VIGNA, p. 42)⁹
 (...) The group had got its start in the early 1990s as a loose affiliation of cryptography wizards who shared a common concern about the creeping erosion of privacy and individual disempowerment in modern society. (J. CASEY e VIGNA, p. 49)¹⁰

Esse movimento, tão engajado, teve até um documento de fundação, o qual enfatizava o uso dos métodos criptográficos fundamentais para mudar a estrutura de interferência de corporações e governos nas transações financeiras, bem como de trazer poderes de volta aos cidadãos.

The coders at the inaugural meeting were greeted by Tim May, a berded anarcho-libertarian and former Intel physicist who, when he wasn't reading or writing sci-fi, spent most of his waking hours conceiving of new cryptographic tools of rebellion. May read them his “Crypto-Anarchist Manifesto,” which opened with a play on Karl Marx's famous manifesto: “A specter is haunting the modern world, the specter of cryptoanarchy”. The essay went on to predict that “just as the technology of printing altered and reduced the power of medieval guilds an the social power structure, so too will cryptologic methods fundamentally alter the nature of corporations and government interference in economic transactions.” This, in these coders' minds was all positive. It would subvert the nexus of power they belived central banks and government agencies maintained in the service of their clients in corporate America. It would re-empower citizens.
 May's essay would become the Cyberpunks founding document.

⁹ (...) movimento Cyberpunk, uma associação de ativistas da tecnologia, que primeiro ganhou notoriedade na década de 1990 com seus esforços para usar ferramentas criptográficas de privacidade para forçar mudanças políticas e culturais radicalmente. Este esforço deu alguns frutos: o Cruzado da transparência Julian Assange e sua organização ativista de publicações WikiLeaks desenvolveu esse movimento. (tradução livre)

¹⁰ (...) O grupo começou no início dos anos 90 como uma afiliação de magos da criptografia que compartilhavam uma preocupação comum sobre a erosão da privacidade e da incapacitação individual na sociedade moderna. (tradução livre)

(...) Guided by the principle that in the digital age protecting privacy would be crucial for maintaining an open society, the Cypherpunks set their active minds to creating tools to allow people to maintain anonymity. (J. CASEY e VIGNA, p. 50-51)¹¹

Os *cypherpunkes*, então, pensaram em criar moedas virtuais que não necessitavam de autoridade central para as fabricar ou comandar, não precisariam do Estado, como acontecem com as moedas fiduciárias. As moedas virtuais seriam totalmente independentes, tendo como “lastro” a confiabilidade na rede, por parte do usuário. Um exemplo das moedas virtuais criadas nesse período são: DigiCash (1990), criada por David Chaum; Hashcash (1997), idealizada por Adam Back; B-money (1998), gerada por Wei Dei; Bitgold (1998), desenvolvida por Nick Szabo; e a RPOW (2004), pensada por Hal Finney. Mas é válido ressaltar que nenhuma dessas moedas seguiram em frente, elas tinham problemas, principalmente em sua formulação matemática. A criptomoeda de sucesso, que surgiu em 2008 após a crise financeira mundial, foi o Bitcoin. Como tal moeda é objeto deste trabalho, ela será estudada em capítulo específico.

To the Cypherpunks, the idea of an anonymous digital cash system was nothing new. It had been one of their first big ideas, but no one had yet turned it into something viable. Several had attempted to build digital cash systems, one had even got tantalizingly close, but ultimately no system had reached any kind of critical mass, and the cause had fizzled out. (J. CASEY e VIGNA, p. 42)¹²

As moedas virtuais, para alguns especialistas, são alternativas ao dinheiro estatal (moeda fiduciária). Esse entendimento surgiu, principalmente, pelo fato de ter ocorrido a crise financeira mundial de 2008, onde ocorreu a desvalorização de moedas nacionais e grandes instituições financeiras ruíram.

¹¹ Os codificadores na reunião inaugural foram recebidos por Tim May, um anarcolibertário e ex-físico da Intel que, quando ele não estava lendo ou escrevendo ficção científica, passou a maior parte de suas horas acordadas concebendo ferramentas criptográficas de rebelião. May leu para eles o seu Criptoanarquista Manifesto, que iniciou baseando-se no famoso manifesto de Karl Marx: “Um espectro está assombrando o mundo moderno, o espectro da criptografia.” O ensaio passou a prever que “assim como a tecnologia de impressão alterou e reduziu o poder das guildas medievais e a estrutura de poder social, também os métodos criptológicos alteram fundamentalmente a natureza das corporações e das interferências do governo nas transações econômicas. “Isso, nestas mentes dos codificadores, foi tudo positivo. Subverteria o nexos de poder que eles, Bancos Centrais e agências governamentais acreditavam, mantidos no serviço de seus clientes na América corporativa. Reforçaria os cidadãos. O ensaio de May se tornaria o documento fundador dos Cypherpunks.

(...) Guiados pelo princípio de que na era digital, protegendo a privacidade, seria crucial para manter uma sociedade aberta, os Cypherpunks usam suas mentes ativas para criar ferramentas que permitam as pessoas manterem o anonimato. (tradução livre)

¹² Para os Cypherpunks, a ideia de um sistema de caixa digital anônimo não era nada de novo. Foi uma das suas primeiras grandes ideias, mas ninguém tinha transformado em algo viável. Vários tentaram construir sistemas de dinheiro digital, um até chegou tentadoramente próximo, mas afinal nenhum sistema chegou a qualquer tipo de massa crítica, e a causa fracassou. (tradução livre)

Especialistas também afirmam que as criptomoedas: oferecem liberdade ao usuário, visto que este pode escolher qual criptomoeda utilizar para adquirir algum bem ou serviço; são uma forma de possuírem reserva de valor, pois o usuário pode adquiri-las como ativos digitais e também entendem que elas são uma forma de diminuir a emissão de papel-moeda, trazendo para o Estado Nacional uma grande economia de despesa anual na emissão de papel-moeda.

Assim, as criptomoedas ou *cryptocurrencies* têm como finalidade permitir a troca de bens e serviços, e também a transferência de valores monetários (dinheiro), sem a necessidade de uma autoridade central, como Estados e bancos. Mas essas não são as suas únicas finalidades, elas surgiram como uma forma disruptiva ao sistema existente, são uma transformação social, mudanças de paradigmas econômicos, políticos, culturais e sociais, é uma verdadeira revolução na era digital, que surgiu para integrar, conectar, diminuir cada vez mais “barreiras” e dinamizar as escolhas dos seres humanos ao redor do mundo.

3.2 - Funções da Moeda

A essência de moeda e suas funções já são caracterizadas desde os tempos aristotélicos. Aristóteles, em suas obras *Ética a Nicômaco e Política*, descreveu as três funções primordiais da moeda, são elas: unidade de conta, meio de pagamento e instrumento de reserva de valor.

L'essence de la monnaie, dans la tradition aristotélicienne, est appréhendée par les trois fonctions *d'unité de compte, de moyen de paiement et d'instrument de réserve de valeur*. Cette conception traditionnelle de la monnaie a traversé les siècles, résisté aux avatars des formes monétaires et constitue encore, à partir de la conception selon laquelle « money is what money does », le point d'attaque le plus fréquemment utilisé dans l'analyse économique contemporaine pour définir les fonctions de la monnaie.

Les débats ont moins porté sur la référence aux fonctions monétaires que sur l'importance respective de chacun des éléments de ce triangle fonctionnel. (DEMBIK e RUIIMY, p. 7)¹³

¹³ A essência do dinheiro, na tradição aristotélica, é aprendido pelas três funções de unidade de conta, meios de pagamento e instrumento de reserva de valor. Esta concepção de moeda tradicional passou pelos séculos, resistiu aos avatares de formas monetárias e ainda constitui, desde a concepção, segundo que “dinheiro é o que o dinheiro faz”, o ponto de ataque mais frequentemente usado na análise econômica contemporânea para definir as funções do dinheiro.

Os debates se concentraram menos na referência às funções monetárias do que nas respectivas importâncias de cada um desses elementos nesse triângulo funcional.

Dessa forma, essas três funções norteiam o estudo e o entendimento da essência de moeda, mas é importante destacar que os debates a respeito da moeda na atualidade não concentraram seus esforços na referência às funções monetárias, e sim deram ênfase na respectiva importância de cada elemento que compõe as funções da moeda.

3.2.1 - Unidade de Conta ou Medida Comum de Valor

Sabemos que, para o bom funcionamento da economia, um dos elementos essenciais é a troca de bens de serviços entre os mercados nacionais e também internacionais. Para isso, faz-se necessário existir uma medida comum de valor, ou seja, uma unidade de conta, que possibilite facilitar essa troca, como, por exemplo: o Real, o Dólar americano ou o Euro.

Dans une économie où de nombreuses marchandises doivent être échangées, il faut pour réaliser ces échanges, pouvoir apprécier la valeur des biens et services. La thèse de Walras, reprise para Denizet, démontre, de manière claire, le rôle d'étalon des valeurs. (DEMBIK e RUIFY, p. 8)¹⁴

Dessa forma, é necessário haver uma medida-padrão para se mensurar o valor. A moeda, portanto, é um padrão reconhecido no que diz respeito às trocas comerciais. Ela irá funcionar como um *numerário*.

A moeda é o padrão reconhecido para medir o valor, assim como o pé, a jarda, ou o metro são padrões reconhecidos para medir o comprimento. Essa função da moeda como medida-padrão do valor se conhece como sua função de agir como “numerário”. Eis o motivo exclusivo por que até agora usamos o dinheiro em nossa análise. A reflexão nos mostra claramente que, se se deve usar determinado bem como medida de cálculo, será muito conveniente que ele funcione igualmente como bem pelo intermédio do qual se efetua a troca. (STNIER, p. 415-416)

Havendo, portanto, uma medida-padrão, é de certo que irá facilitar as trocas comerciais, pois a ausência de um padrão monetário acarretaria num complexo sistema monetário, pois se faria necessário haver, para cada troca comercial, uma medida que avaliaria a correspondência monetária entre o bem de troca e o bem existente. A esse respeito, Nelson Holanda disserta:

(...) a moeda proporciona um denominador comum de valores, um padrão uniforme de avaliação para todos os bens que são trocados no mercado. A existência de um mercado pressupõe sempre um determinado sistema de preços relativos ou relações de troca, mediante o qual diferentes bens podem ser trocados entre si. Na ausência

¹⁴ Em uma economia onde muitos bens devem ser trocados, é necessário realizar essas trocas, para poder apreciar o valor de bens e serviços. A tese de Walras, assumida por Denizet, demonstra, de maneira clara, o papel padrão dos valores. (tradução livre)

de um padrão monetário, esse sistema seria extraordinariamente complicado, vez que, para cada mercadoria, precisaríamos ter um número de relações de troca correspondente ao número de bens existentes. A criação da moeda possibilita, no entanto, a avaliação de todos os bens em termos do número de unidades monetárias que sua venda comanda no mercado (reais ou dólares, por exemplo). (HOLANDA, p. 576)

Assim, a moeda como uma medida padrão, permite uma melhor eficiência do sistema monetário, bem como também por proporcionar uma unidade monetária única, onde os preços são expressos, viabilizará os cálculos econômicos e as arbitragens.

3.2.2 - Meio de Pagamento

A moeda na sua função como *meio de pagamento* é a mais objetiva, pois é a função que irá concretizar, será a consequência da função anterior, ou seja, para haver a troca entre bens e serviços, se fez necessário ter uma medida-padrão de valor primeiramente, em seguida irá ocorrer a troca/pagamento, que será viabilizado pela segunda função da moeda, que é *meio de troca* ou *meio de pagamento*. Esse pagamento, na verdade, será extinguir uma dívida, pois, no momento que se adquire um bem, por consequência, assume-se uma dívida, e a moeda, portanto, materializa essa ação de assunção de dívida. É importante ressaltar que a moeda permite aumentar o *poder de compra* do indivíduo. Segundo Wonnaccot e Crusius:

O *poder de compra* da moeda é medido pela quantidade de bens e serviços que uma determinada quantidade de moeda pode comprar. Em períodos inflacionários, um cruzeiro passa a comprar cada vez menos; conseqüentemente o poder de compra da moeda diminui. (WONNACCOT E CRUSIUS, p. 158)

Objetivando dissertar sobre a função da moeda (meio de pagamento), Nilson Holanda discorre também sobre a questão de a moeda ser um meio para a extinção de uma dívida.

Em primeiro lugar, a moeda funciona como meio de pagamento, vale dizer, tem a faculdade, aceita por todos, de extinguir dívidas. Pode ser utilizada para realizar quaisquer pagamentos e assegura ao seu detentor o direito de exigir da sociedade uma contrapartida de bens de valor equivalente. A moeda apresenta a vantagem de generalizar o poder de compra do consumidor, facilitando, extraordinariamente, a realização de transações comerciais e possibilitando a mais ampla especialização e divisão do trabalho. Como afirma Gudin, “a moeda transforma a dívida nascida de uma relação individual em meio de compra geral; a dívida torna-se social, estendendo-se no espaço, na pessoa, no objeto e no tempo”. (HOLANDA, p. 575)

Ainda a respeito da função *meio de pagamento*, concluímos que a moeda é um meio diretamente de troca, em face de outros bens, ou seja, permite adquirir bens ou serviços, é um equivalente geral, é consentida e aceita pela sociedade.

Dessa forma, é importante destacarmos que a moeda não corresponde somente ao metal e às cédulas em si, as quais temos em nossas carteiras, cofres e em instituições financeiras, a moeda é também aquele saldo dos depósitos bancários, é o valor agregado.

3.2.3 - Reserva de Valor

A terceira função que temos da moeda é a mesma ser reserva de valor, ou seja, uma forma de se ter um número X de capital, que varia no curso do tempo, e sua variação é inversamente ao preço, podendo, portanto, seu valor ser aumentado ou depreciado, de acordo com o tempo.

Moedas fiduciárias, como o Real, Dólar, Euro ou Yen, não podem ser considerados absolutamente como moedas, pois são suscetíveis de queda no seu poder de compra, por motivo das taxas de câmbio, as quais regem o sistema monetário internacional.

Dessa forma, têm-se como garantia o valor nominal, e não o valor real, sem necessariamente servir como meio de pagamento. Portanto, as atividades financeiras podem apresentar uma boa garantia na conservação do valor nominal.

CAPÍTULO 4 - BITCOIN

4.1 - Internet of Money (Internet do Dinheiro)

Como falamos anteriormente, no capítulo sobre a Quarta Revolução Industrial, onde está havendo um grande crescimento da Internet das Coisas, aqui, neste capítulo, vamos focar para a ideia de Internet do Dinheiro.

Esse crescimento é permitido, por meio de uma ferramenta primordial, a internet, que democratizou o acesso a informações, permitiu transpor barreiras, diminuir distâncias e conectar as pessoas ao redor do mundo. Com o uso de computadores, smartphones, tablets e relógios digitais, a otimização de experiências com o uso da internet possibilitou termos uma maior eficiência e dinâmica, permitindo, dessa forma, a conectividade intensa, que é chamada de “Internet das Coisas”, que tem como base a Inteligência Artificial (IA), ou seja, que os objetos físicos que estão conectados com a internet possam coletar e transmitir dados que otimizem as nossas experiências e controlá-los remotamente, como também utilizá-los como provedores de serviços.

Como a revolução digital, permitiu-nos termos experiências com a *Internet of Things* (Internet das Coisas), por que não utilizarmos essa mesma ideia de democratização no sistema financeiro? Por que ficarmos sujeitos a regramentos, que são pensados longe de nossas anuências? São por meio de perguntas como estas que surge o conceito de *Internet of Money* (Internet do Dinheiro).

Este conceito foi dado por Andreas M. Antonopoulos, um empreendedor tecnológico grego-britânico, que se tornou um expoente em matéria de Bitcoin. Ele afirma que não devemos entender o Bitcoin somente como uma moeda digital, pois assim estaremos limitando o entendimento e não estaremos compreendendo o seu sentido na totalidade. O Bitcoin é mais do que uma moeda, é uma tecnologia disruptiva e revolucionária que irá mudar paradigmas. É uma rede internacional de pagamentos e de trocas financeiras, totalmente descentralizado, não necessitando de bancos ou do Estado, sendo, portanto, uma revolução social e política, uma mudança total na forma de inovação financeira. É uma alteração de um sistema financeiro centralizado para um descentralizado.

Bitcoin is a digital money, but it's so much more than that. Saying bitcoin is digital money is like saying the internet is a fancy telephone. It's like saying that the internet is all about e-mail. Money is just the first application. Bitcoin is a technology, it is a currency, and it is an international network of payments and exchange that is

completely decentralized. It doesn't rely on banks. It doesn't rely on banks. It doesn't rely on governments. We have never done this before in the history of humanity. This invention is truly revolutionary. When we look back, we will see that this is a historic moment in the evolution of computer science, but it is also a social and political revolution in the making. So, let's get started (ANTONOPOULOS, 2016, p. 1)¹⁵

Dessa forma, a Internet do Dinheiro é um momento revolucionário na sociedade mundial, é poder democratizar o acesso para aqueles que não possuem entrada no sistema financeiro tradicional - nesse estudo, representado pelo Bitcoin. É válido ressaltar que existem mais de 1.500 (mil e quinhentas) moedas digitais. As criptomoedas são o dinheiro das pessoas, onde todos concordam, mas ninguém controla; não há uma autoridade central, que determina, que faz imposições, e, sim, é o consenso na rede que determina aquela criptomoeda.

4.2 - O que é o Bitcoin?

O Bitcoin é uma criptomoeda (*cryptocurrency*), criada por uma pessoa com o pseudônimo de Satoshi Nakamoto. No ano de 2008, com o advento da crise financeira mundial, Satoshi Nakamoto, que até o momento não tem sua identidade revelada, publicou em um fórum na internet o *white paper* do Bitcoin, intitulado: *Bitcoin: A Peer-to-Peer Electronic Cash System*. Dessa forma, podemos perceber a disrupção que essa iniciativa nos trouxe, pois, por meio da internet, de uma forma livre e democrática, o Bitcoin foi apresentado ao mundo, mostrando que não estava vinculado a nenhuma instituição financeira, Estado ou sistema financeiro. De uma maneira simples, seu protocolo matemático (*hash code*) está disponível publicamente na internet para qualquer pessoa que queira utilizá-lo ou aprimorá-lo, está no formato de fonte aberta (*open source*), disponível para qualquer usuário.

Bitcoin is a digital currency that came into existence in 2008 as an invention by a person called Satoshi Nakamoto. He published a paper where he posited that he found the way to create a decentralized network that could achieve consensus,

¹⁵ Bitcoin é dinheiro digital, mas é muito mais do que isso. Dizer que *bitcoin* é dinheiro digital é dizer que a internet é um telefone chique. É como dizer que a internet se resume a e-mail. Dinheiro é uma das aplicações. Bitcoin é a tecnologia, é a moeda, e é a rede internacional de pagamentos e troca, a qual é completamente descentralizada. Não conta com bancos. Não conta com governos. Nós nunca tínhamos feito isso antes na história da humanidade. Essa invenção é verdadeiramente revolucionária. Quando olhamos para trás, nós iremos ver que isso é um momento histórico na evolução da ciência da computação, mas é também uma revolução social, política em andamento. Então, vamos começar. (tradução livre)

agreement, without any central controlling authority. (ANTONOPOULOS, 2016, p.2)¹⁶

Na introdução do *paper* do Bitcoin, Satoshi Nakamoto já faz crítica ao modelo de sistema financeiro mundial, aduz sobre as falhas que o sistema tradicional possui, e a obrigação de estarmos vinculados a uma instituição financeira para fazermos nossas movimentações financeiras. Esta vinculação não irá haver no Bitcoin, não há uma autoridade central comandando as transações.

Commerce on the Internet has come to rely exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. (NAKAMOTO, p.1)¹⁷

O que Nakamoto revoluciona em seu *white paper* é a possibilidade de se ter um sistema de pagamento baseado em criptografia, onde o usuário transaciona com outro usuário sem a necessidade de uma terceira parte, uma autoridade central. Essas transações são computacionalmente impraticáveis de serem revertidas, protegendo os usuários contra fraudes. No *paper*, ele também mostra uma solução para o “gasto duplo”, um dos problemas centrais de outras criptomoedas pensadas na década de 1990, que não deram certo. Essa solução se dá por meio de uma rede distribuída *peer-to-peer*, gerando prova computacional das transações cronologicamente. Ele afirma que o sistema é seguro enquanto houver um controle coletivo das transações por toda a rede, ou seja, quanto mais “CPU’s” estiverem conectadas, mais pessoas estão verificando as transações (*nodes*), e, com isso, mais a rede vai ficando segura.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of

¹⁶ *Bitcoin* é uma moeda digital que surgiu em 2008, como uma invenção feita por uma pessoa chamada Satoshi Nakamoto. Ele publicou um trabalho, onde ele divulgou que havia encontrado um caminho para criar uma rede descentralizada a qual poderia alcançar o consenso, o acordo, sem um controle central de uma autoridade. (tradução livre)

¹⁷ O comércio na internet passou a depender exclusivamente de recursos de instituições financeiras, servindo como terceiros confiáveis para processar pagamentos eletrônicos. Enquanto o sistema funciona bem o suficiente para a maioria das transações, ele ainda sofre com as fraquezas inerentes do modelo baseado na confiança. (tradução livre)

transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes. (NAKAMOTO, p. 1)¹⁸

O Bitcoin tem natureza de um protocolo, que é um agrupamento de regras, que se comunicam por meio de computadores espalhados ao redor do mundo, que estão conectados à rede *peer-to-peer* do sistema do Bitcoin. Com isso, não há um dono do protocolo, não tem nenhuma empresa, instituição financeira ou Estado por trás do protocolo. Todos nós, usuários, somos detentores do protocolo, por isso o Bitcoin é tão disruptivo e democrático.

Bitcoin is not a company. It is not an organization. It is a standard or a protocol just like TCP/IP, or the internet. It's not owned by anyone. It operates by simple mathematical rules that everyone who participates in the network agrees on. Through this simple mechanism, through this invention of Satoshi Nakamoto, bitcoin is able to allow a completely decentralized network of computers to agree on what transactions have occurred on a network, essentially agreeing on who currently has the money. (ANTONOPOULOS, 2016, p. 2)¹⁹

Assim, o Bitcoin foi a primeira criptomoeda no formato descentralizado que deu certo, devido a ter corrigido falhas primordiais para o seu bom funcionamento, principalmente a questão do gasto duplo, que será explicado em tópico específico. Mas, antes, precisamos entender o que seria a rede *peer-to-peer*.

4.3 - Rede *Peer-To-Peer*

A rede *peer-to-peer* é entendida por criptografia de ponta a ponta, no formato de rede aberta (*open source*) e de maneira descentralizada. A criptografia é uma junção de técnicas usadas com o intuito de proteger certos dados, com objetivo de tornar o seu acesso difícil por um terceiro, que não é o destinatário.

¹⁸ O que é necessário é um sistema de pagamento eletrônico baseado em criptografia, prova em vez de confiança, permitindo que quaisquer duas partes dispostas a transacionar diretamente uns com os outros, sem a necessidade de um terceiro confiável. Transações que são computacionalmente impraticáveis de serem revertidas protegeria os vendedores de fraude, e os mecanismos rotineiros de garantia podem ser facilmente implementados para proteger os compradores. Neste trabalho, propomos uma solução para o gasto duplo usando um servidor *timestamp* distribuído *peer-to-peer* para gerar a prova computacional da ordem cronológica das transações. O sistema é seguro enquanto *nodes* honestos controlarem coletivamente mais poder de CPU do que qualquer grupo cooperante de *nodes* atacantes. (tradução livre)

¹⁹ *Bitcoin* não é uma companhia. Não é uma organização. É um padrão ou um protocolo, assim como TCP/IP, ou a internet. Não é propriedade de ninguém. É operado por simples regras matemáticas que qualquer um que participa na internet do consenso. Por meio desse simples mecanismo, por meio dessa invenção de Satoshi Nakamoto, bitcoin é capaz de permitir uma completa rede descentralizada, de computadores certificando quais transações ocorreram na rede, essencialmente confirmando com quem está o dinheiro no momento presente. (tradução livre)

No que tange ao mundo das criptomoedas, a criptografia tem o objetivo de garantir a segurança do protocolo, como também garantir o processamento das transações e proteger os usuários.

Nesse formato de rede *peer-to-peer*, cada computador conectado à rede possui uma parte do protocolo, dessa forma permitem *downloads* mais rápidos, não necessitando de uma autoridade central. Nesta rede, cada computador conectado é, ao mesmo tempo, clientes e servidores, visto que, ao fornecerem os dados, estes adquirem também os dados, formando uma imensa rede de compartilhamento, sem precisar de uma autoridade central que a comande. Ou seja, na rede há um compartilhamento de informações entre os computadores dos próprios usuários da rede, não necessitando de um terceiro para intermediar as transações na rede. É válido ressaltar que nesse tipo de rede com compartilhamento de dados podemos ter o armazenamento, o poder de processamento e a largura de banda.

Com isso, o Bitcoin possui uma rede independente, onde todas as informações estão disponíveis para os usuários, permitindo, portanto, um livre acesso à rede e extrema proteção das transações efetuadas na rede.

4.4 - Tecnologia *Blockchain*

A tecnologia *blockchain* é inovadora e tem várias utilizações. Especialmente neste trabalho, vamos estudar esta tecnologia no contexto das criptomoedas, mas especificamente no Bitcoin.

O *Blockchain* (block = bloco, chain = corrente, série, sequência), cadeia/corrente de blocos, para o Bitcoin, é como um livro-razão (*ledger*), onde estão armazenados todas as informações das transações da rede. Este registro é público e se dá por meio de blocos. As transações realizadas dentro da rede *blockchain* estão na forma cronológica, sendo que são registradas as suas origens e destinos; e também a rede é compartilhada e descentralizada salientando, portanto, o seu aspecto público.

No Bitcoin, a tecnologia *blockchain* é usada para evitar a existência do gasto duplo (explicaremos em tópico específico) e também visa manter a segurança do protocolo da rede como um todo. É com relação à solução do problema do gasto duplo, solucionado por Satoshi Nakamoto, tornando o Bitcoin a primeira criptomoeda a dar certo. Essa tecnologia é uma mudança de paradigma.

A *Blockchain* do Bitcoin é uma *ledger* que é incorruptível, é distribuída, criptografada, não é violável e também é irreversível, e tem natureza econômica. É incorruptível e inviolável, pois tem um sistema de validação, onde deve-se verificar nos novos blocos os códigos dos blocos anteriores. É distribuída, pois, como explicamos anteriormente, cada computador conectado à rede é um cliente e um servidor, recebendo e armazenando os dados, e esses dados estão espalhados ao redor do globo, sendo difícil violar a rede, pois, para ocorrer essa violação, deve-se fazer em cada computador conectado à rede. É criptografada de ponta a ponta, tornando inacessível por um terceiro, por meio de um sistema que protege os dados. É irreversível, pois, no momento que ocorre a transação e a sua respectiva validação, não é possível mais ser desfeita. E também possui natureza econômica, visto que as transações realizadas têm o objetivo de transacionar valores.

As transações na rede *Blockchain* do Bitcoin são enviadas para a rede, são recebidas, criptografadas e validadas. Todo esse sistema é baseado no chamado *consenso*. O *consenso* seria um mecanismo de decisão, que é vinculado a um formato de padrões matemáticos, os quais vinculam os usuários da rede, ou seja, as transações somente serão processadas, e sucessivamente só farão parte do sistema se a rede *Blockchain* do Bitcoin resolver os problemas matemáticos, o *proof of work* (prova de trabalho), e chegar a um consenso, validando as informações transmitidas.

A confiança, o lastro da criptomoeda se dá em sua própria rede, não necessitando de uma autoridade central para realizar a verificação, permitindo, portanto, a transação no formato *peer-to-peer*, de ponta a ponta, de A para B diretamente.

É válido destacar que no Bitcoin, em média a cada 10 minutos, um novo bloco é processado e agregado à rede *Blockchain* do Bitcoin. Cada bloco tem 1Mb, cada transação tem cerca de 250 bytes e há o processamento de 2.000 (duas mil) transações por bloco.

THE GOLDEN EIGHT

Blockchain Transformation of Financial Services

FUNCTION	BLOCKCHAIN IMPACT	STAKEHOLDER
1. Authenticating Identity and Value	Verifiable and robust identities, cryptographically secured	Rating agencies, consumer data analytics, marketing, retail banking, payment, card networks, regulators
2. Moving Value- make a payment, transfer money, and purchase goods and services.	Transfer of value in very large and very small increments without intermediary will dramatically reduce cost and speed of payments.	Retail banking, whole sale banking, payment card networks, money transfer services, telecommunications, regulators.
3. Storing Value- currencies,	Payment mechanism combined	Retail banking, brokerages,

commodities, and financial assets are stores of value. Safety deposit box, a savings account, or a checking account. Money market funds of Treasury bills.	with a reliable and safe store of value reduces need for typical financial services; bank savings and checking accounts will become obsolete.	investment banking, asset management, telecommunications, regulators.
4. Lending Value- credit card debit, mortgages, corporate bonds, municipal bonds, government bonds, asset-backed securities, and other forms of credit.	Debt can be issued, traded, and settled on the blockchain; increases efficiency, reduces friction, improves systemic risk. Consumers can use reputation to access loans from peers; significant for the worlds unbanked and for entrepreneurs.	Wholesale, commercial and retail banking, public finance (i.e., government finance), microlending, crowdfunding, regulators, credit rating agencies, credit scores software companies.
5. Exchanging Value- speculating, hedging, and arbitraging. Matching orders, clearing trades, collateral management and valuation, settlement and custody.	Blockchain takes settlement times on all transactions from days and weeks to minutes and seconds. This speed and efficiency also creates opportunities for unbanked an underbanked to participate in wealth creation.	Investment, wholesale banking, foreign exchange traders, hedge funds, pension funds, retail brokerage, clearinghouses, stock, futures, commodities exchanges; commodities brokerages, central banks, regulators.
6. Funding and Investing in Asset, Company, Start-up- capital appreciation, dividends, interest, rents, or some combination.	New models for peer-to-peer financing, recording of corporate actions such as dividends paid automatically trough smart contracts. Titles registry to automate claims to rental income and other forms of yield.	Investment banking, venture capital, legal, audit, property management, stock exchanges, crowdfunding regulators.
7. Insuring Value and Managing Risk – protect assets, homes, lives, health, business property, and business practices, derivative products.	Using reputation systems, insurers will better estimate actuarial risk, creating decentralized markets for insurance. More transparent derivatives.	Insurance, risk management, wholesale banking, brokerage, clearinghouses, regulators.
8. Accounting for Value- new corporate governance.	Distributed ledger will make audit and financial reporting real time, responsive, and transparent, will dramatically improve capacity of regulators to scrutinize financial actions within a corporation.	Audit, asset management, shareholder watchdogs, regulators.

Fonte: TAPSCOTT, Don e TAPSCOTT Alex. **Blockchain Revolution**. New York: Penguin, 2016, p. 64. (Anexo I)

4.5 - Servidor de Validação (Timestamp Server)

No *paper* de Nakamoto há a proposição do chamado *Timestamp Server*, um servidor de validação que trabalha contraindo um *hash* (algoritmo/código) de um bloco de itens, para registrar e validar publicamente na rede. O *timestamp* prova que os dados, formando um bloco, existem de acordo com a sua ordem de entrada no *hash*. Cada *timestamp* inclui o *timestamp* anterior, formando uma cadeia de blocos, ou seja, que a cada novo bloco formado há o reforço de cada *timestamp* anterior.

4.6 - O Gasto Duplo

O gasto duplo na ciência da computação é chamado de *Byzantine Genral's Problem*. Este gasto duplo seria a possibilidade de utilização da criptomoeda duas vezes na mesma transação. A solução encontrada por Nakamoto foi por meio do *proof of work* (prova de trabalho), que é uma forma de evitar a duplicidade da transação.

O *proof of work* é uma validação do trabalho. Quando uma nova transação é pedida, esta deve ir em direção à verificação SHA-256, para que o usuário gere uma prova, e este deve garantir que no próximo bloco haja toda a codificação do bloco anterior, que começa com zero bits.

Para a nossa rede de carimbos de tempo, nós vamos implementar uma prova de trabalho incrementando um número aleatório no bloco até que o valor encontrado sirva para decodificar o bloco com o número de zero bits. Uma vez que o esforço do CPU foi gasto para satisfazer a prova de trabalho, o bloco não pode ser modificado sem que o trabalho seja refeito. Como os blocos seguintes são encadeados logo após este, o trabalho para modificar o bloco inclui também todos os blocos anteriores. (NAKAMOTO, p. 3. Trad. Daniel Ribeiro)

Fernando Ulrich, em relação ao gasto duplo, explica com excelência sobre o assunto:

(...) 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 a 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 (...) (ULRICH, 2014, p. 17)

Assim, o problema do gasto duplo foi solucionado por Satoshi Nakamoto, onde ele trabalha em suas fórmulas matemáticas para que a transação seja única, à prova de fraudes, ratificando, portanto, como o formato da rede do Bitcoin é segura para a realização das transações financeiras.

im-mu-ta-ble
adjective

1. tamper-proof, something that does not change and cannot be changed.
Contemporary Example: Bitcoin's proof of work is a planetary scale,

thermodynamically guaranteed, self-evident system of immutability. (ANTONOPOULOS, 2017, vol. 2, p. 27)²⁰

É válido ressaltar que o que traz segurança à imutabilidade na rede do Bitcoin não é a tecnologia e, sim, o *proof-of-work*. Segundo Andreas M. Antonopoulos, o Bitcoin é a primeira escala (em termos matemáticos) mundial. Afirma que o Bitcoin é um “monumento digital” do *proof-of-work*, pois a transação, uma vez embutida dentro da rede *Blockchain* do Bitcoin, é segura pelo *proof-of-work* e se torna muito difícil a sua alteração.

4.7 - Transações em Bitcoin

As transações com o Bitcoin são feitas por meio de duas chaves: a chave privada e a chave pública. Para compreendermos melhor, usaremos este exemplo: (A) quer transferir para (B) Bitcoins, (A) entra na rede do bitcoin por meio de sua chave privada. No momento que faz a transferência para (B), a chave que irá aparecer na rede será a chave pública, onde qualquer usuário pode verificar, ou seja, sabe-se que (A) transferiu para (B) “N” bitcoins, mas não se sabe a identidade de (A) e nem de (B).

Nakamoto define uma moeda digital por meio de uma cadeia de assinaturas, sendo que cada proprietário/usuário irá transferir a criptomoeda para o próximo usuário, assinando, digitalmente, uma codificação com as transações precedentes, e a chave pública do seguinte usuário será acrescentada ao final da criptomoeda. Diante disso, um recebedor tem a possibilidade de verificar as assinaturas, com o intuito de averiguar a cadeia de propriedade. A maioria das vezes quem verifica é o minerador (explicaremos mais à frente, em tópico específico).

We need a way for the payee to know that previous owners did not sign any earlier transactions. For our purposes, the earliest transaction is the one that counts, so we don't care about later attempts to double-spend. The only way to confirm the absence of a transaction is to be aware of all transactions. In the mint based model, the mint was aware of all transactions and decided which arrived first. To accomplish this without a trusted party, transactions must be publicly announced [1], and we need a system for participants to agree on a single history of the order in which they were received. The payee needs proof that at the time of each

²⁰ imutável
adjetivo

1. à prova de falsificação, algo que não muda e não pode ser alterado. Exemplo Contemporâneo: A prova de trabalho do Bitcoin é uma escala planetária, termodinamicamente garantido, sistema autoevidente de imutabilidade. (tradução livre)

transaction, the majority of nodes agreed it was the first received. (NAKAMOTO, p. 2)²¹

Com isso, tendo as transações públicas na rede, não irá se fazer necessário ter um terceiro, uma autoridade central para realizar as verificações, como acontece no sistema financeiro tradicional. Qualquer pessoa com poder computacional pode fazer essa verificação.

4.8 - Funcionamento das Transações e da Rede

Para se ter o bom funcionamento da rede é necessário observar os seguintes passos: a) Cada nova transação é transmitida para todos os nós (*nodes*); b) Cada nó junta as novas transações em um bloco; c) Cada nó trabalha com o objetivo de encontrar uma prova de trabalho difícil para o bloco; d) Quando um nó encontra a prova de trabalho, ele envia o bloco para todos os nós que já estão na rede; e) Os nós que se encontram na rede somente aceitam este novo bloco se as transações que estiverem dentro dele forem válidas e não houver o gasto-duplo; f) Nós (*nodes*) expressam a sua aquiescência ao bloco quando já começam a laborar na criação de um próximo bloco da “corrente”, usando a codificação do bloco anterior.

É válido ressaltar que, dentro de cada bloco, há várias transações que formam o bloco.

4.9 - Mineração

O criador do Bitcoin, Satoshi Nakamoto, entende que o Bitcoin é o “ouro” digital. Portanto, a atividade de produção do Bitcoin, ele faz uma analogia com a atividade de mineração. Mas o que isso significa? “Minerar” significa que qualquer pessoa ao redor do mundo que tenha poder computacional (*hash power*) pode minerar, produzir Bitcoins, usando o código da rede do Bitcoin que está disponível publicamente na internet; e também possui

²¹ Precisamos de uma maneira de o beneficiário saber que os proprietários anteriores não assinaram quaisquer transações anteriores. Para nossos propósitos, a primeira transação é a única que conta, então não nos importamos com tentativas posteriores de gasto-duplo. A única maneira de confirmar a ausência de uma transação é estar ciente de todas as transações e decidir qual chega primeiro. Para conseguir isso sem uma parte confiável, as transações devem ser anunciadas publicamente [1], e precisamos para os participantes concordarem com uma única história na ordem em que forem recebidos. O beneficiário precisa de prova de que, no momento de cada transação, a maioria dos nós concordou que foi o primeiro recebido. (tradução livre)

computadores de alto desempenho que esteja com acesso à internet e estejam conectados à rede *Blockchain* do Bitcoin, funcionando vinte e quatro (24) horas por dia, sete (07) dias por semana.

O responsável por minerar Bitcoins, seja uma pessoa ou empresa, é chamado de “minerador”(miners), e este ganha por “minerar” Bitcoins, que é a criação de um novo bloco; por validar as transações na rede *Blockchain*; por meio das taxas de transações pagas pelos usuários, para que ocorra essa validação; e por contribuir com a sua força computacional para possibilitar a manutenção da rede ativa e segura. A respeito da mineração, Satoshi Nakamoto, em seu *paper*, aduz que:

(...) 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. (...) (2008, p. 4)²²

Ainda a respeito da mineração, Fernando Ulrich disserta:

(...) Esses usuários são chamados de “mineradores” porque são recompensados pelo seu trabalho com Bitcoins recém-criados. Bitcoins são criados, ou “minerados”, à medida que milhares de computadores dispersos resolvem problemas matemáticos complexos, que verificam as transações no *blockchain*. (...)
 (...) O protocolo, portanto, foi projetado de tal forma que cada minerador contribui com 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*. (2014, p. 19-20). (...)

O processamento das transações na rede do Bitcoin será executado pelo minerador, mas para tanto ele precisa receber uma remuneração que dependerá de quanto o usuário irá pagar de taxa. Normalmente, as plataformas utilizadas pelos usuários dão uma porcentagem média de taxa, mas o usuário tem o livre arbítrio de utilizar a porcentagem sugerida pela plataforma, ou entender que a taxa deva ser processada por uma porcentagem de taxa maior ou menor. É claro que quanto maior a remuneração para o minerador, mais rápido será o processamento da transação. Do contrário, essas transações com baixa remuneração irão para o chamado *Mempool*, que é o conjunto de transações que ainda não foram processadas na rede, aguardando um minerador que se disponha a validar a transação mesmo que esteja com baixa remuneração.

²² A adição estável de um montante constante de novas moedas é análoga a mineradores de ouro, que gastam recursos para adicionar ouro na circulação. No nosso caso, é o tempo da CPU e eletricidade que é gasta. (tradução livre)

As transações na rede do Bitcoin, para serem processadas, levam em média 10 minutos, mas, ratificando, vai depender da taxa de remuneração dada pelo usuário ao minerador.

Devemos observar também a questão do *Halvening*, o qual seria o corte pela metade (50%) da recompensa paga em Bitcoins aos mineradores pelo trabalho de verificação e validação das transações a cada 100 mil blocos minerados. No começo da mineração do Bitcoin, ganhavam-se 50 moedas por bloco minerado como forma de remuneração, recompensa, por utilizar sua força computacional para validar as transações. Mas a cada 4 anos, esse número decai pela metade, isso se denomina *Halvening*. Na atualidade, são 12,5 moedas como recompensa por bloco minerado. É de salientar que a medida que há a criação de novas moedas, a solução matemática se torna mais difícil.

É de salientar que as transações na rede *Blockchain* do Bitcoin são irreversíveis, pois, no momento em que são validadas, não pode mais cancelá-la ou alterá-la.

Nas transações, temos duas características importantes que devem ser destacadas: a privacidade e a segurança, pois o minerador não sabe que é A ou B, ele sabe somente que a chave privada de A transferiu uma certa quantia de Bitcoins para a chave privada de B, e que B recebeu. Portanto, somente quem é detentor da chave é que pode enviar Bitcoins.

A segunda forma, então, de o minerador auferir ganho é pela validação das transações na rede, ou seja, ganham por meio das taxas pagas pelos usuários, a fim de que as realizem e as coloquem no bloco a ser minerado.

Dessa forma, os mineradores auferem ganhos por realizarem e validarem as transações na rede e por minerarem Bitcoins (produção de moeda), mas não possuem o poder de alterar o código do Bitcoin, isso cabe aos desenvolvedores, que não ganham nenhuma remuneração.

É válido salientar que o Bitcoin tem um limite monetário (21 milhões) e não financeiro, pois sua mineração está programada até 2040.

É nesse cenário que o Bitcoin tem uma limitação, tem uma quantidade finita. Andreas M. Antonopoulos, diz que não devemos nos prender na ideia de que mineração é apenas a criação de nova moeda, não é o propósito da mineração. Para o autor, a mineração é um efeito colateral, pois, quando não houver mais Bitcoins a serem criados, a mineração ainda vai continuar, devido ao seu propósito, que é garantir a segurança, a validação para todas as transações e blocos, de acordo com as regras do consensus.

Mining doesn't work to create bitcoin. That is not the purpose of mining: that is a side effect. The way I can prove it's a side effect is that one day, there will be no new bitcoin. But guess what? There will still be mining. Even after the last satoshi (the smallest unit of bitcoin) gets mined, mining continues. It must continue because its purpose is not to create bitcoin but to provide security, to provide validation of all of the transactions and blocks according to the consensus rules. (ANTONOPOULOS, 2017, vol. 2, p. 31)²³

A mineração é mais do que uma simples ideia de criação de moeda, e sim é um dos suportes para manter a rede ativa, mesmo quando o tempo de criação de moedas terminar. As moedas que existem continuarão, e será preciso manter a sua segurança e validação das transações, e isso ocorrerá por meio da mineração. Esta situação ainda não foi definida, pois minerar custa um valor muito alto e não se sabe ao certo o custo da mineração quando não houverem mais bitcoins a serem minerados e não houver mais retorno financeiro.

(...) As *Globe and Mail* finance writer Ian McGugan pointed out earlier this year, there are at least flour glaring obstacles in bitcoin's path to glory. The most obvious is cost (...)
 (...) Nevertheless, the system needs to reward miners to ensure it is constantly maintained. An nobody knows what will happen to transaction fees when there are no bitcoins available to offer as an incentive. (...)
 (WATSON, p. 4-5)²⁴

Assim, a mineração como um suporte para manter a rede ativa ainda é uma incógnita quanto ao seu futuro, quando não houverem mais bitcoins a serem minerados, visto que o Bitcoin tem um limite monetário de 21 milhões a serem produzidos, minerados.

4.10 - Privacidade

Uma das grandes ideias de Satoshi Nakamoto, em seu *paper*, foi com relação à privacidade. Apesar de as transações serem públicas, elas, ao mesmo tempo, continuam sendo privadas, vejamos:

O modelo bancário tradicional atinge um nível de privacidade por limitar o acesso à informação apenas às partes envolvidas e ao intermediário confiável. A necessidade de anunciar todas as transações publicamente prejudica este método, mas a privacidade pode ainda ser mantida quebrando o fluxo da informação em outro local: mantendo as chaves públicas anônimas. O público pode ver que alguém está

²³ Mineração não funciona para criar Bitcoin, esse não é o propósito da mineração: isso é um efeito colateral. A maneira que eu posso provar que é um efeito colateral é que um dia não haverá novo Bitcoin, mas adivinhe? Ainda haverá mineração. Mesmo que depois que o último satoshi (a menor unidade de Bitcoin) é extraído, a mineração continua. Deve continuar porque o seu propósito não é criar Bitcoin, mas fornecer segurança, fornecer validação de todas as transações e blocos de acordo com as regras de consenso. (tradução livre)

²⁴ Como escreveu o escritor financeiro da *Global and Mail*, Ian McGugan, este ano, há pelo menos obstáculos ofuscantes no caminho do Bitcoin para a glória. O mais óbvio é o custo (...)
 (...) No entanto, o sistema precisa recompensar os mineiros para garantir taxas quando não há Bitcoins disponíveis para oferecer como um incentivo. (tradução livre)

enviando um montante de dinheiro para outra pessoa, mas sem informações ligando a transação a qualquer pessoa. Isso é parecido com o nível de informação liberado no mercado de ações, onde o tempo e o tamanho das vendas individuais, a “fita”, são tornados públicos, porém sem dizer quem são as partes envolvidas. (NAKAMOTO, p. 6. Trad. Daniel Ribeiro)

Essa grande ideia de Nakamoto propiciou de o Bitcoin dar cada vez mais certo, pois o usuário tendo duas chaves, uma privada e uma pública, permite uma maior privacidade e também permite não haver uma autoridade central para dar privacidades a essas transações, ou seja, podemos realizar transações diretamente de um para o outro, mas a rede, o público, não saberá quem transacionou e, sim, somente que houve uma transação, mas sem saber a identidade do usuário.

4.11 - Armazenamento dos Bitcoins

Os Bitcoins são guardados nas chamadas *wallets*, local este em que os usuários irão armazenar suas criptomoedas. Na atualidade há várias versões de *wallets*: *on-line*; *mobile* ou para *desktops*.

Normalmente, nas *wallets*, há a exigência de criação de um nome de usuário, senha, pin e frases para recuperar a senha, caso o usuário a esqueça ou perca. É válido ressaltar que é imprescindível o usuário salvar as suas senhas, pois sem elas não há outra forma de ter acesso às criptomoedas.

A *Wallet on-line* diz respeito a guardar a criptomoeda na conta de usuário em uma *Exchange* (corretora). Dessa forma, o usuário transfere a custódia de suas criptomoedas a uma *Exchange*. Esta não é uma forma muito aconselhável de *wallet*, pois como não há regulamentação no Brasil (iremos explicar este assunto em tópico específico), a *Exchange* pode usar a criptomoeda do usuário como bem entender, ou até sumir, como já aconteceu.

A *wallet mobile* e para *desktops* são as utilizadas com mais frequência pelos usuários, pois permite que o mesmo guarde a sua criptomoeda no celular (por meio de um aplicativo), tornando mais fácil o acesso, pois está na palma da mão, ou no computador. Essas carteiras fazem *backups* automáticos, permitindo ao usuário uma melhor experiência com suas criptomoedas. Exemplos de *wallets*: Edge, Coinbase, Xapo, entre inúmeras outras. O que o usuário deve observar é procurar em fontes confiáveis a avaliação de determinada *wallet* que quer utilizar, para assim manter o armazenamento de suas criptomoedas com segurança.

As *hard wallets* são dispositivos próprios para o armazenamento de criptomoedas, como um *pen drive* ou um *token*, é uma forma das senhas com as respectivas chaves serem guardadas no formato *off-line*.

A *paper wallet*, em nossa era digital, não é uma forma de armazenamento muito habitual em nossos tempos modernos, pois seria o fato de anotar as senhas de acesso em um papel ou agenda, e se perder não há *backup*.

4.12 - Como Obter Bitcoins

Há três formas de se conseguir Bitcoins e também outras criptomoedas. A primeira seria por meio da mineração, como explicamos anteriormente. O minerador adquire Bitcoins à medida que ele “minera” novos blocos e transmite para a rede *Blockchain* do Bitcoin. A segunda maneira seria obter por meio das *Exchanges* (corretoras), a ser explicado no tópico 4.13. A terceira maneira seria alguém que já possui a criptomoeda remeter para a sua *wallet digital* (carteira digital) de Bitcoins, ou outra criptomoeda, já explicado no tópico 4.11.

4.13 - Exchanges

As *Exchanges* são um local, uma plataforma, onde se pode realizar as transações de criptomoedas. Para utilizar essas plataformas, deve-se realizar um cadastro para a abertura de conta e transferir valores da instituição financeira a qual o usuário tem conta-corrente para a sua conta da *Exchange*, estando, portanto, apto para transacionar, comprar e vender Bitcoins ou outra criptomoeda. Cada *Exchange* possui uma exigência para cadastro. No Brasil, é exigido, por exemplo: o envio de cópia digitalizada de algum documento com foto (como RG, carteira de motorista ou passaporte), ou pede-se o nome completo com o número do CPF. Infelizmente, essa variação de exigências ocorrem, pois não há uma regulamentação no Brasil sobre as criptomoedas e o funcionamento das *Exchanges*.

É de salientar que, como no mercado de ações existe a variação das bolsas, isso também ocorre no mercado das criptomoedas. Cada *Exchange* possui seu valor/cotação para a criptomoeda, assim é possível fazer o cadastro em várias *Exchanges* e observar os valores, percebendo em qual delas está mais vantajoso comprar ou vender criptomoedas. Para usuários comuns, examinar o valor das criptomoedas em cada *Exchange* torna-se uma tarefa árdua e

cansativa, mas para profissionais do mercado financeiro esta atividade de verificação é muito frequente, possibilitando de a realizarem com mais facilidade e permitindo também a prática da chamada arbitragem financeira.

A arbitragem financeira é muito comum no mercado financeiro e seria uma forma de pesquisar diferentes valores para o mesmo ativo, possibilitando, portanto, lucrar com essa variação de cotação/valores, comprando o ativo na *Exchange* em que o valor está mais baixo e vendendo o ativo na *Exchange* em que o valor está mais elevado.

Nas *Exchanges* é possível fazer três atividades:

- a) comprar ou vender criptomoedas;
- b) trocar moedas digitais por moedas tradicionais, como: Real, Dólar, Euro ou Libra Esterlina.
- c) trocar uma moeda digital por outra moeda digital, como, por exemplo: trocar Bitcoins por Ethereum.

Não nos esqueçamos que hoje, no mercado, existem mais de 1.500 criptomoedas.

Hoje, no Brasil, temos as *Exchanges*: Foxbit, Mercado do Bitcoin, Coinbene, entre outras; e no exterior: Poloniex e Bittrex, entre outras.

4.14 - Divisão do Bitcoin

Apesar do ideal de descentralização e consenso, idealizado por Satoshi Nakamoto, nos últimos dois anos houveram divisões na rede *Blockchain* do Bitcoin, devido a desentendimentos entre mineradores e desenvolvedores. Mas, antes de explicarmos sobre as divisões na rede, precisamos entender uma nomenclatura utilizada para essa divisão, que para a ciência da computação é chamado de *fork*.

Fork significa divisão, é quando ocorre uma fragmentação de um projeto de *software* já existente, sendo que pode ser integralmente diferente do original, ou ser apenas um aprimoramento, uma implementação do original, feito por um programador ou por um grupo de desenvolvedores.

Há o *hard fork* e o *soft fork*. O *soft fork* ocorre quando antes condições válidas se tornam inválidas, causando mudança no protocolo, mas a cadeia de blocos permanece a

mesma. Já no *hard fork* é ao contrário, condições antes inválidas se tornam válidas, originando novas possibilidades, expandindo o código e permitindo a geração de duas moedas.

No ano de 2015, houve uma proposta dos desenvolvedores, chamada de BIP 148 (*Bitcoin Improvement Proposal*) - USAF (*User Activated Soft Fork*), que objetivava um melhoramento na rede, por meio da adesão do denominado *Segwit* (*Segregated Witness*), que significa um procedimento de diminuição de transação. Nesse cenário do BIP 148, houveram dois acordos: o Acordo de Hong Kong, em fevereiro de 2016, e o Acordo de Nova York, em maio de 2017.

No primeiro acordo, o de Hong Kong, foi definido pelos desenvolvedores um projeto de aprimoramento na rede, por meio de uma ampliação do bloco de transações para 2Mb, via um *hard fork*, a ser realizado em 31/07/2017. Mas a maioria dos mineradores não aceitaram o *Segwit*.

No segundo acordo, o de Nova York, foi apresentado pelo mineradores o *Segwit 2X*, uma data-limite para a ocorrência do *hard fork*, que objetivava o aumento do bloco para 2Mb em outubro/novembro de 2017. Nesta proposta, os mineradores queriam um aprimoramento do protocolo do Bitcoin, como também propuseram a simplificação da verificação e da mineração. Este acordo foi ratificado por um grupo que possui mais de oitenta por cento (80%) do poder de mineração da rede *Blockchain* do Bitcoin.

Como não houve acordo entre desenvolvedores e mineradores, no dia 1º de agosto de 2017, ocorreu o *hard fork* na rede do Bitcoin, onde houve a divisão na rede, originando assim uma nova moeda: a *Bitcoin Cash*. Esta nova criptomoeda propiciou a duplicidade, pois os usuários que já possuíam Bitcoins tinham a mesma quantidade duplicada na rede do *Bitcoin Cash*.

No que tange ao *Segwit 2X*, proposta esta realizada pelos mineradores, não ocorreu no mês de novembro/2017. Os mineradores renunciaram com a ideia de irem adiante com a proposta.

É válido ressaltar que dois meses após a criação do *Bitcoin Cash*, em 24 de outubro de 2017, houve outra cisão na rede *Blockchain* do Bitcoin, originando uma nova criptomoeda, a *Bitcoin Gold*.

4.15 - Bitcoin Para Além da Ideia de Moeda

Não devemos entender o Bitcoin apenas no seu conceito de moeda, a qual podemos fazer transações financeiras, fazer compras. O Bitcoin é mais do que isso, é uma tecnologia disruptiva e libertária, que veio para integrar pessoas e dar uma nova abordagem ao sistema financeiro mundial, com democratização e facilitação no acesso, não havendo necessidade de intermediação de uma instituição financeira ou de um Estado.

O Bitcoin é uma invenção que trouxe um novo formato de rede, baseado no consenso, é o dinheiro do povo (*Money of the People*), como Andreas Antonopoulos afirma. Entende-se o Bitcoin como uma rede descentralizada, onde todos os *nodes* são iguais, tendo o seu protocolo neutro. Portanto, esse fundamento de neutralidade é a base da internet em termos gerais, ou seja, há a inovação sem a necessidade de permissão.

Bitcoin creates a completely flat and decentralized network where every node is equal, where protocol is neutral to the transactions, and it pushes innovations to the edge of the network, allowing exactly the same phenomenon we saw on the internet: innovation without permission. (ANOTONOPOULOS, 2016, p. 5)²⁵

Bitcoin is not just money for the internet. Yes, it's perfect money for the internet. It's instant, it's safe, it's free. Yes, it is money for the internet, but it's so much more. Bitcoin is the internet of money, currency is only the first application. If you grasp that, you can look beyond the price, you can look beyond the volatility, you can look beyond the fad. As its core, bitcoin is a revolutionary technology that will change the world forever. (ANTONOPOULOS, 2016, p. 8)²⁶

O Bitcoin como uma criptomoeda libertária está livre das políticas econômicas dos bancos e dos governos, não está sujeito a nenhuma regra concernente às instituições privadas e públicas. Está sujeito, obviamente, somente à regra matemática, que é a sua base, e varia, como em um mercado de ações, devido somente à confiança na rede, no sistema, e não a políticas ou determinantes externos.

(...) With its roots in the anti-establishment cypherpunk movement, which advocates the use of cryptography to protect individual privacy and liberty, the bitcoin revolution has true believers who see the world's original cryptocurrency as an ideal replacement for fiat currencies, or government-backed money, which is

²⁵ Bitcoin criou uma completa rede linear e descentralizada, onde todas as conexões são iguais, onde o protocolo das transações é neutro, e isso empurrou a inovação para a fronteira da rede, permitindo exatamente o mesmo fenômeno que nós vimos na internet: inovação sem permissão. (tradução livre)

²⁶ Bitcoin não é somente dinheiro para a internet. Sim, é dinheiro para a internet, mas é muito mais do que isso. Bitcoin é a internet do dinheiro. Moeda é somente a primeira aplicação. Se você entender isso, você pode olhar para além do preço, você pode olhar para além da volatilidade, você pode olhar para além da novidade. Bitcoin é uma revolução tecnológica que irá mudar o mundo para sempre. (tradução livre)

controlled by corporate middleman and always at risk of being inflated or deflated by fiscal or monetary mismanagement. (WATSON, p. 3)²⁷

Bitcoin, como Andreas Antonopoulos diz, é o dinheiro do povo, pois permite o seu acesso por qualquer pessoa, em qualquer parte do mundo, em países como no Afeganistão, onde mulheres não podem ter acesso a uma conta bancária. O Bitcoin tornou uma mudança de paradigmas. Mulheres com acesso à internet podem adquirir Bitcoins e realizar compras ou transações financeiras, pois na rede Bitcoin não se identifica a pessoa ou o gênero. Em países africanos, utilizar criptomoedas, como o Bitcoin, tornou-se uma das maneiras de se proteger mais contra roubos e assaltos, bem como se proteger da “montanha-russa” que são algumas economias africanas.

Bitcoin é se libertar das amarras e do controle dos bancos e governos, é se livrar da dominação bancária, iniciada pela família Médici de Florença, umas das famílias precursoras da forma de sistema financeiro mundial; é ser disruptivo, é ter poder de escolha, é permitir que a tecnologia lhe auxilie no seu dia a dia de uma forma revolucionária.

At its core, this technology is a form of social organization that promises to shift the control of money and information away from the powerful elites and deliver it to the people to whom it belongs, putting them back in charge of their assets and talents. (VIGNE & CASEY, p. 6)²⁸

Bitcoin permite uma igual e tecnológica disrupção, permitindo uma economia mais eficiente, criando mais riqueza global, pois a junção de tecnologia e dinheiro possibilita uma quebra de paradigmas mais intensa.

Former US. treasury secretary Larry Summers has grasped this. “If you think about what a modern economy is all about, it basically involves ever more exchange,” he told us. “And exchange, unless it can be literally simultaneous, always has real issues of trust. So, what the breakthrough in communications and computer science represented in bitcoin does is to support deeper exchange at lower price. And that matters both within countries for the traditionally excluded and it also matters across international borders. (VIGNE & CASEY, p. 8)²⁹

²⁷ (...) Com suas raízes no movimento *Cyberpunk anti-establishment*, que defende o uso de criptografia para proteger privacidade e liberdade individual, a revolução do Bitcoin tem adeptos que veem o mundo original das criptomoedas como um substituto ideal para as moedas fiduciárias, ou dinheiro apoiado pelo governo, que é controlado por intermediário, que sempre corre o risco de ser inflacionado ou deflacionado pela má administração fiscal ou monetária. (tradução livre)

²⁸ Em essência, essa tecnologia é uma forma de organização social que promete deslocar o controle do dinheiro e da informação para longe das poderosas elites e entregá-lo para as pessoas a quem pertence, colocando-os de volta no comando de seus bens e talentos. (tradução livre)

²⁹ O ex-secretário do Tesouro dos EUA, Larry Summers, compreendeu isso. “Se você pensa sobre o que é uma economia moderna, basicamente envolve mais troca.”, ele nos disse. “E troca, a menos que possa ser literalmente simultânea, sempre tem problemas reais de confiança”. Então, o que o avanço em comunicações e ciência da computação representa no Bitcoin, é apoiar uma troca mais profunda a preço mais baixo. E isso

Nas palavras do ex-secretário do Tesouro Norte-Americano, Larry Summers, ele disserta sobre a confiança (*“in real issues of trust”*), ele fala a respeito do dilema da confiança em transacionar com algum estranho, e esse foi um dos problemas solucionados pela família de banqueiros de Florença, a família Médici. No que tange aos “tradicionalistas excluídos”, Summers diz respeito aos mais de 2,5 bilhões de excluídos do sistema financeiro global, em continentes como África e América, e países como o Afeganistão. (VIGNE & CASEY, p.8)

Dessa forma, o Bitcoin veio para dar acesso às pessoas excluídas do sistema financeiro, dar liberdade e livrar as pessoas da tirania da centralização. O Bitcoin não é só uma questão de moeda, que tem o seu preço variável, não é só alta e baixa de valores, é retornar o poder financeiro para o povo, é democratizar o acesso, é revolucionar o que entendemos por sistema financeiro.

At its core, cryptocurrency is not about the ups and downs of the digital currency market; it's not even about a new unit of exchange to replace the dollar or the euro or the yen. It's about freeing people from the tyranny of centralized trust. It speaks to the tantalizing prospect that we can take power away from the center-away from banks, governments, lawyers, and tribal leaders of Afghanistan- and transfer it to the periphery, to We, the People. (VIGNE & CASEY, p. 8)³⁰

Assim, Bitcoin é uma revolução no sistema financeiro, que permite a escolha, o livre arbítrio, a descentralização, a confiança na rede, a quebra do antigo pensamento, a disrupção, é a possibilidade de trazer a integração para o mundo nunca vista anteriormente.

4.16 - Bitcoin Ameaça ao Sistema Financeiro Tradicional?

Esta é uma pergunta que estudiosos, tecnólogos e banqueiros fazem quando observam o avanço das criptomoedas, especialmente o Bitcoin.

Para alguns, o avanço das criptomoedas é o fim dos bancos e da centralização, e uma real ameaça para o sistema financeiro tradicional. Para outros é uma bolha, que logo irá estourar; outros afirmam que não é ameaça alguma, pois o sistema bancário é sólido e as criptomoedas são somente mais uma inovação tecnológica, a qual não possui solidez.

importa tanto para dentro do país, para os tradicionalmente excluídos, e também é importante para as fronteiras internacionais. (tradução livre)

³⁰ Em essência, criptomoedas não é sobre os altos e baixos do mercado de moeda digital, não é também sobre uma unidade de troca para substituir o dólar, o euro ou o iene. É sobre libertar as pessoas da tirania, da confiança centralizada. Ela fala da perspectiva tentadora de poder que podemos ter longe dos bancos, governos, advogados e líderes tribais do Afeganistão, e transferir para a periferia, para nós, o povo. (tradução livre)

A esse respeito, Thomas Watson disserta:

As things stand, bitcoin doesn't pose a major threat to the global economy, so central bankers are not losing sleep over the enthusiasm for it. But investors should be very concerned with the impact of irrational exuberance on bitcoin demand since it has a nasty habit of evaporating. (WATSON, p. 3)³¹

Como Thomas Watson explicou, Bitcoin não é uma ameaça principal para a economia global, os bancos centrais não estão muito eufóricos com o entusiasmo dos investidores, mas adverte que os investidores devem estar atentos aos impactos da euforia em comprar Bitcoin.

Já Andreas Antonopoulos, afirma que:

I predict, over the next 15 to 20 years, we'll see a great infrastructure inversion happen in finance. First, the banks will resist. Then, the banks will adopt. The banks will run their systems alongside blockchain and bitcoin systems, and finally they will run all traditional banking as an application on top of a decentralized trusted ledger. Because, while it is very hard to do decentralized trusted ledger that's connected to all of these legacy banking systems, simulating legacy banking on top of a decentralized ledger, on top of bitcoin, an open global blockchain, is trivial. (ANTONOPOULOS, p. 62)³²

Neste cenário, Andreas Antonopoulos afirma que haverá nos próximos quinze (15) ou vinte (20) anos uma mudança significativa na infraestrutura do sistema, conta a trajetória afirmando que os bancos irão primeiro resistir, posteriormente irão adotar a tecnologia e seus sistemas serão adaptados ao *Blockchain* e ao sistema do Bitcoin.

Portanto, o Bitcoin é uma alternativa ao dinheiro estatal, não estando sujeito às políticas monetárias dos países.

Diante dos pensamentos diversos, entendemos que o Bitcoin é uma inovação tecnológica que irá andar, paralelamente, com o sistema financeiro tradicional por ora, pois ainda necessita de várias adaptações que o sistema tradicional já tem, a principal delas é a aceitação pelas pessoas. A partir dessa aceitação, sucessivamente terão modificações,

³¹ Como as coisas estão, o Bitcoin não representa uma grande ameaça para o mercado global, assim os bancos centrais não estão perdendo o entusiasmo por isso. Mas os investidores devem estar muito preocupados com o impacto irracional da exuberância que o Bitcoin demanda, uma vez que tem um péssimo hábito de evaporação. (tradução livre)

³² Eu prevejo que nos próximos 15 a 20 anos veremos uma ótima inversão na infraestrutura das finanças. Primeiro, os bancos resistirão. Depois os bancos irão adotar. Os bancos administrarão seus sistemas ao lado dos sistemas do Blockchain e do Bitcoin, e finalmente eles vão executar os sistemas tradicionais bancários como uma aplicação no topo de uma razão confiável descentralizada. Porque, enquanto é muito difícil conectar esse sistema descentralizado distribuído com o sistema bancário tradicional, simulando bancos em cima de um *ledger* descentralizado, em cima do Bitcoin, um Blockchain global aberto e trivial.

adaptação dos bancos, ou nem a existência de bancos, talvez, regulação por parte do Estado, difusão no mercado consumidor da moeda, adaptação das próprias pessoas na utilização das criptomoedas, por exemplo.

Assim, precisamos aguardar como o mercado e o sistema irão se comportar, mas afirmamos que criptomoedas e o mercado financeiro tradicional vão caminhar em paralelo, permitindo ao consumidor, ao usuário, a escolha, se quiser ficar atrelado à moeda fiduciária do Estado, como Real, Dólar, Euro, Libra Esterlina ou utilizar as mais de mil e quinhentas (1.500) moedas digitais disponíveis no mercado.

4.17 - Altcoins

Como Satoshi Nakamoto definiu o Bitcoin como o “ouro digital”, dando uma relevância maior para a sua invenção, as outras criptomoedas são denominadas de *altcoins*. São altcoins por não serem Bitcoin.

It’s really easy to explain what an altcoin is. Technically speaking, it’s any coin that isn’t bitcoin. Since bitcoin was the first to hit the scene and build a mainstream following, it’s as conventional as this space can get. The rest of the coins that make up the cryptosphere are referred to as altcoins. Yes that includes ethereum and XRP. They got the name because they provide alternative services, functions, and usability features that bitcoin either lacks or chooses not to offer. From an investing perspective, they also provide choices for crypto enthusiasts outside of bitcoin. (DEROUSSEAU, p. 166)³³

As altcoins, apesar de serem desenvolvidas na tecnologia *Blockchain*, suas utilizações, funcionalidades e investimentos são diferentes das do Bitcoin. O Ethereum, por exemplo, a segunda criptomoeda mais comercializada, tem como função “rodar” *Smart Contracts*, que são Contratos Inteligentes, criptografados e seguros.

Nesse universo das criptomoedas, a concorrência é muito elevada, cada uma tem seus objetivos específicos, mas se convergem quando buscam na tecnologia *Blockchain* superarem no tempo de realização de uma transação e terem os seus preços mais baixos que o Bitcoin, assim os usuários podem investir mais em altcoins e aumentar o seu volume comercializado frente ao Bitcoin.

³³ É muito fácil explicar o que é um Altcoin. Tecnicamente falando, é qualquer moeda que não seja Bitcoin. Já que o Bitcoin foi o primeiro a entrar em cena e construir um *mainstream*, é tão convencional quanto esse espaço pode chegar. O resto das moedas que compõem a criptoesfera é referido como Altcoins. Sim, isso inclui Ethereum e XRP. Eles pegaram o nome porque eles fornecem serviços, funções e recursos de usabilidade alternativos que o Bitcoin não tem ou escolhe não oferecer. De uma perspectiva de investimento, eles também fornecem opções para entusiastas de criptografia fora do Bitcoin. (tradução livre)

4.18 - O que Determina o Preço do Bitcoin

Nesse tópico iremos estudar como é determinado o preço do Bitcoin, a partir do estudo de Sukmawati Sukamulja e Cornelia Olivia Sikora, publicado no “*Journal of Indonesian Economy and Business*”.

As mention before, cryptocurrrencies or bitcoin are a new financial instrument and they have become an alternative investment with diversification benefits (Brière, Oosterlinck & Szafarz, 2013). Since becoming an investment alternative, it has developed a typical characteristic of investments; the price of bitcoins tends to increase or decrease significantly in the short-term. The price volatility has attracted the attention of the academic and industrial fields. That is why so much research has been published since the rise in bitcoin’s price. (p. 54)³⁴

Como dissertado na pesquisa, as criptomoedas, em geral, são um novo instrumento de investimento, oportunizando a diversificação do portfólio do investidor. Sendo, portanto, uma novidade de investimento, o preço tende a subir ou decair no curto prazo, dessa forma a volatilidade no preço tem atraído atenções de estudiosos e investidores.

A partir dessa pesquisa, é observado que o Bitcoin não pode ser explicado pelas teorias econômicas usuais, como: fluxo de caixa futuro, paridade de poder de compra e paridade da taxa de juros descoberta, devido ao fato de que características naturais de fornecimento e demanda de uma moeda fiduciária não existem no mercado do Bitcoin e das criptomoedas em geral, pois o Bitcoin não é emitido por um Banco Central e, conseqüentemente, por nenhum Estado.

According to Kristoufek (2013), bitcoin’s price cannot be explained by standard economic theories like future cash flow, purchasing power parity and uncovered interest rate parity, because several futures of a normal currency’s supply and demand do not exist in the bitcoin market. (SUKAMULJA E SIKORA. p. 54)³⁵

A pesquisa mostra que há o pensamento de alguns estudiosos, que o preço do Bitcoin é separado da real economia e dos fundamentos da macroeconomia que determinam o preço,

³⁴ Como mencionado anteriormente, as criptomoedas ou Bitcoin são um novo instrumento financeiro e eles se tornaram um investimento alternativo com benefícios diversificados. (BRIÈRE, OOSTERLINCK & SZAFARZ, 2013). Desde que se tornaram um investimento alternativo, tem se desenvolvido uma típica característica de investimentos; o preço do Bitcoin tende a valorizar e desvalorizar significativamente em um curto espaço de tempo. A volatilidade do preço tem atraído a atenção dos campos acadêmicos e industrial. É por isso que tanta pesquisa publicada desde o aumento do Bitcoin. (tradução livre)

³⁵ De acordo com Kristoufek (2013), o preço do Bitcoin não pode ser explicado pelas teorias econômicas padrão como fluxo de caixa futuro, paridade de poder de compra e paridade de taxas de juros descoberto, porque vários futuros de uma oferta e demanda da moeda fiduciária não existem no mercado de Bitcoin. (tradução livre)

pois o Bitcoin é uma inovação tecnológica, disruptiva, que veio com o intuito de quebrar com paradigmas. Portanto, o que irá determinar, afetar o preço para eles do Bitcoin é a atratividade para os investidores.

Bitcoin's price is separated from de real economy and there are no macroeconomic fundamentals that determine bitcon's price formation. Similarly, Ciaian, Rajcaniova, and Kancs (2014) also found that bitcoin's price is not driven by macroeconomics factors. Both of these researchers found that the one thing that does affect bitcoin's price is its attractiveness for investors. (SUKAMULJA E SIKORA, p. 54)³⁶

Contudo, há outros estudiosos, e as pesquisadoras tendem a esse pensamento de que o mercado tradicional de bolsa de valores influenciam no preço do Bitcoin, observemos:

In contrast, van Wijk (2013) found that the role of global financial development, which can be measured by looking at the stock exchange indices, exchange rates, and oil prices, can also affect bitcoin's price. Stock exchange indices represent the general macroeconomic situation and the state of financial development, because those stock exchange indices contain or represent the performance of the big companies in those countries. Research from Zhu, Dickinson & Li (2017) and Wang, Xue, & Liu (2016) found that macroeconomic indicators represented by DJIA have a negative effect on bitcoin's price.

H1: Macroeconomic indicators, namely the stock exchange indices, negatively influence bitcoin's price fluctuations.

H2: The supply and demand of bitcoins negatively influence bitcoin's price fluctuations.

H3: Gold's price negatively influences bitcoin's price fluctuations. (SUKAMULJA E SIKORA. p.54)³⁷

De acordo com as pesquisas de Sukamulja e Sikora, o mercado especulativo também influencia no preço do Bitcoin, pois quando a demanda aumenta, o preço aumenta, visto que a produção de Bitcoins é limitada, bem como a flutuação do preço é influenciado pela adoção da criptomoeda cada vez mais pelos usuários, quando estes utilizam o Bitcoin como investimento ou forma de pagamento.

³⁶ O preço do Bitcoin é separado da economia real e não há fundamentos macroeconômicos que determinam a formação de preço do Bitcoin. Da mesma forma, Ciaian, Rajcaniova e Kancs (2014) também descobriram que o Bitcoin não é impulsionado por fatores macroeconômicos. Ambos os pesquisadores descobriram que a única coisa que afeta o preço do Bitcoin é a sua atratividade para investidores. (tradução livre)

³⁷ Em contraste, van Wijk (2013) descobriu que o papel das finanças no desenvolvimento financeiro global, o qual pode ser medido observando os índices das bolsas de valores, taxas de câmbio e preços do petróleo, podem também afetar o preço do Bitcoin. Os índices das bolsas de valores representam a situação macroeconômica geral e o estado de desenvolvimento financeiro, porque esses índices de bolsa de valores contêm ou representam a performance das grandes empresas naqueles países. A pesquisa de Zhu, Dickinson & Li (2017) e Wang, Xue & Liu (2016) constatou que os indicadores macroeconômicos representados pela DJIA tiveram um efeito negativo no preço do Bitcoin.

H1: Indicadores macroeconômicos, nomeadamente os índices das bolsas de valores, influenciam negativamente as flutuações do preço do Bitcoin. (tradução livre)

O outro fator entendido por Sukamulja e Sikora em sua pesquisa é o fato de o ouro influenciar no preço do Bitcoin.

De acordo com a pesquisa que embasamos neste tópico, percebemos que, de acordo com o histórico de preço do Bitcoin, várias pessoas ao redor do globo ficam entusiasmadas com o ganho que podem obter com a aquisição da criptomoeda, sendo um fator determinante para a volatilidade do preço, visto que a criptomoeda Bitcoin tem um limite monetário de vinte e um (21) milhões. Portanto, a demanda influencia no preço, a demanda e a limitação atrai a especulação, um outro fator determinante do preço. Um outro fator que a pesquisa observa é que a volatilidade do preço do Bitcoin está ligada ao preço do ouro. Portanto, de uma certa forma, alia-se ao pensamento de Satoshi Nakamoto, de que o Bitcoin é o “ouro” digital, pois, para investidores, o ouro é um investimento seguro. Quando há crises financeiras, quem possui uma boa reserva de ouro consegue passar pela crise sem grandes perdas, pois esta matéria-prima, ao longo da história financeira da humanidade, sempre foi um “porto seguro” no que se refere a investimento e reserva de valor, tanto é que economias de países no passado tinham sua moeda fiduciária lastreada em suas reservas de ouro.

4.19 - Confiança no Bitcoin

Há discussões sobre se o Bitcoin é uma criptomoeda confiável. Entendemos que irá depender do perfil do investidor. É comum que a grande maioria dos investidores de Bitcoin sejam os entusiastas da tecnologia, principalmente jovens, os chamados *Millenials*. Para estes, a tecnologia é uma ferramenta importante em suas vidas, o que os proporciona a utilizarem no mundo financeiro.

4.20 - Bitcoin: Pode ser uma Rede de Pagamento?

Sobre esta visão de rede de pagamento, podemos analisar a partir do seguinte aspecto: com a evolução da tecnologia cada vez mais rápida, o Bitcoin pode, sim, se tornar uma rede de pagamento, irá depender, principalmente, da regulamentação de cada país, do desenvolvimento de sua rede *Blockchain* e da aceitação, pois, se compararmos as transações realizadas com os meios de pagamentos atuais, por exemplo, cartão de crédito, enquanto a cada 10 minutos se valida uma transação na rede *Blockchain* do Bitcoin, Visa e Mastercard, a

exemplo, validam em seus sistemas várias transações por minuto, portanto, é necessário, para que o Bitcoin se torne uma rede de pagamento, uma melhor eficácia de sua tecnologia.

4.21 - Acessibilidade do Bitcoin

O Bitcoin é uma criptomoeda que é dividida em oito casas decimais, portanto é possível comprar frações de Bitcoins, não sendo preciso adquirir um Bitcoin. Por exemplo, se um Bitcoin está valendo R\$ 20.000,00 (vinte mil reais), o usuário não é obrigado a adquirir Bitcoin por esse valor, se ele quiser somente investir R\$ 1.000,00 (mil reais), ou menos, é possível, devido à possibilidade de fracionamento do Bitcoin.

4.22 - Como o Bitcoin Vira “Dinheiro”?

Há duas maneiras de o Bitcoin se tornar “dinheiro”. A primeira diz respeito ao usuário vender seus Bitcoins em uma *Exchange* e esta fazer a transferência do valor na moeda do país para a conta bancária do usuário.

A segunda refere-se ao fato de o usuário utilizar os caixas eletrônicos (ATM) de criptomoedas, espalhados pelo mundo, e sacar em moeda nacional.

4.23 - É Possível Comprarmos no Comércio Utilizando Bitcoins?

Como falamos em tópico específico sobre MOEDA, onde uma de suas principais características é a aceitação, podemos afirmar que somente é possível comprarmos no comércio utilizando Bitcoins se houver a aceitação, e esta já é uma realidade em nossos dias. Por exemplo, grandes empresas como a Amazon, já aceita o pagamento da compra em Bitcoins, portanto, há diversos setores ao redor do mundo que já aceitam o Bitcoin como meio de pagamento.

4.24 - Bitcoin X Libra

Em 18 de junho de 2019, o Facebook anunciou a sua própria criptomoeda, em parceria com gigantes da tecnologia do mercado financeiro e do mercado varejista, como:

Mastercard, Visa, eBay, Spotify e Uber. Com o advento desta criptomoeda, o Facebook tem o objetivo de criar um sistema seguro, escalável, confiável e com credibilidade, baseado na tecnologia *Blockchain*.

A LIBRA se propõe a apresentar três diferenciais: o primeiro se refere ao fato de ser construída em uma segura, escalável e confiável *Blockchain*; a segunda diz respeito a estar baseada em uma reserva de ativos, os quais são desenhados para lhe dar um valor intrínseco; e o terceiro concerne de que a LIBRA será governada por uma associação, a *Libra Association*, a qual está encarregada de evoluir o ecossistema da criptomoeda.

(...) Libra is made up of three parts that will work together to create a more inclusive financial system:

- 1- It is built on a secure, scalable, and reliable **blockchain**;
- 2- It is **backed by a reserve** of assets designed to give it intrinsic value;
- 3- It is **governed by the independent Libra Association** tasked with evolving the ecosystem. (WHITE PAPER-LIBRA)³⁸

Percebemos que este formato de criptomoeda lançada pelo Facebook, que tem o intuito de entregar aos usuários a verdadeira internet do dinheiro, é diferente do ideal pensado pelos *cypherpunks*, bem como difere bastante do formato que o Bitcoin é proposto.

A Libra irá ter um fundo, uma reserva, onde os associados irão depositar uma quantia X de valor, e o montante destes valores depositados, portanto, será o que indicará o valor intrínseco, o lastro da criptomoeda.

A outra peculiaridade da Libra é o fato de haver uma associação, a *Libra Association*, que terá como membros, associados de renome, como: Facebook/Calibra, Mastercard, PayPal, Spotify, Uber, a qual irá comandar todas as diretrizes da moeda, bem como supervisionará a *Libra Blockchain* (sistema) e a *Libra Reserve* (fundo de reserva).

É de se observar que o caráter libertário e descentralizado idealizado nos primórdios dos ideais das criptomoedas não irá ocorrer, visto que o controle de lastro, câmbio e produção da criptomoeda será centralizado na *Libra Association*, a qual comandará e indicará todas as diretrizes a serem seguidas.

Uma outra característica é o fato de que para se ter a confiabilidade na criptomoeda, será necessário haver um fundo com uma reserva de valor, o qual indicará quanto vale a

³⁸ Libra é constituída de três partes que irão trabalhar juntas para criar um sistema financeiro mais inclusivo:

- 1- É construída em uma segura, escalável e confiável *blockchain*;
- 2- É apoiada por uma reserva de ativos, desenhados para darem valor intrínseco;
- 3- É governada pela independente Libra Association, que está encarregada de evoluir com o ecossistema.

criptomoeda. Diferentemente do que ocorre no Bitcoin, a confiabilidade advém da rede, da utilização pelos usuários, e conseqüentemente o valor é cotado.

Assim, a Libra propõe um formato que não difere muito do que é uma moeda fiduciária governada pelo Estado, pois o controle e as diretrizes virão em vez do Estado, virão de instituições privadas, portanto ocorrerá a centralização do comando, formato este o qual não é o ideal das criptomoedas, que é a descentralização. Portanto, o Bitcoin, que é a principal criptomoeda da atualidade, segue o formato da descentralização, baseado em uma rede *peer-to-peer* e na tecnologia *Blockchain*.

CAPÍTULO 5 - BITCOIN E SEUS ASPECTOS LEGAIS

Com o avanço da tecnologia e o advento das criptomoedas no mundo financeiro, dúvidas ainda pairam quando se refere aos seus aspectos legais. O entendimento do Direito Civil (*Civil Law*) ainda é variável e incipiente. Como as criptomoedas são algo muito novo, o Direito ainda está em busca de entender o que é, como deve ser a legislação, quais medidas adotar na regulação, qual o entendimento dos bancos centrais, a aceitação pelas pessoas, aceitação pelo mercado, entre outros questionamentos que vamos estudar ao longo deste capítulo.

The scholarly essays addressing the civil law definition of cryptocurrencies present a range of views. The question is an important one, as the answer will dictate the legal framework applicable to contracts involving cryptocurrency and how cryptocurrency can be protect as an asset. (BRITO, p. 114)³⁹

Como dissertado na referência acima, precisamos definir qual é o entendimento sobre Bitcoin, para então serem definidos outros aspectos de regulação, para assim haver uma concreta legislação que ampare os usuários, as *Exchanges* e o próprio mercado.

Inicialmente, precisamos desenvolver qual é a natureza jurídica do Bitcoin.

a) Natureza jurídica de moeda

Como explicamos no capítulo específico sobre Moeda, observamos que é o instrumento mais utilizado na vida cotidiana, sendo na civilização um elemento primordial na economia de troca. Contudo, esta possui várias facetas. Moeda pode ser dinheiro, riqueza, reserva de valor, elemento de troca.

N. Gregory Mankiw, em seu livro de Introdução à Economia, no capítulo concernente à *moeda*, ele, de início, já faz a indagação *o que é moeda?* Sabemos que, no capítulo 3, já desenvolvemos a ideia de Moeda, mas é interessante destacarmos o pensamento deste autor a respeito do assunto.

O que é moeda? Esta pode parecer uma pergunta estranha. Quando você lê que o bilionário Bill Gates tem muito dinheiro, sabe o que isso significa: ele é tão rico que

³⁹ Os ensaios acadêmicos que tratam da definição da lei civil das criptomoedas apresentam várias definições. A questão é muito importante, pois a resposta vai ditar o quadro jurídico aplicável aos contratos envolvendo as criptomoedas e como as criptomoedas podem ser protegidas como um ativo. (tradução livre)

pode comprar quase tudo que ele quiser. Nesse sentido, o termo *dinheiro* é usado para significar *riqueza*.

(...)

Os economistas, contudo, usam a palavra de um modo mais específico: *moeda* é o conjunto de ativos na economia que as pessoas usam regularmente para comprar bens e serviços de outras pessoas. O dinheiro em sua carteira é moeda porque você pode usá-lo para comprar uma refeição num restaurante ou uma camisa em uma loja de roupas. No entanto, se você fosse dono da maior parte da Microsoft Corporation, como é o caso de Bill Gates, você seria rico, mas esse ativo não é considerado uma forma de moeda. Você não poderia comprar uma refeição ou uma camisa com essa riqueza sem antes obter algum tipo de dinheiro. De acordo com a definição dos economistas, a moeda inclui apenas aqueles poucos tipos de riqueza que são regularmente aceitos por vendedores em troca de bens e serviços. (2015, p. 592)

De acordo com Mankiw, e com o que já estudamos, a aceitação é uma característica muito importante para a moeda. Dessa forma, para as criptomoedas serem “moeda” precisam de aceitação, e estas serem de uma maneira ou de outra transformadas em dinheiro, pois são um tipo de riqueza. É de destacar que esta aceitação pelo mercado ainda está em processo, pois estamos acostumados a entender que “moeda” é aquilo que damos valor, que confiamos, auferimos valor, além de que possui liquidez e garantia, e é administrada e auferida pelo Estado soberano, algo que as criptomoedas não são.

Contudo, afirmar que o Bitcoin é uma moeda, apesar de que na maioria dos casos é sua função principal, é algo que ainda não podemos ratificar, pois depende de fatores importantes como liquidez e aceitação.

Um outro fator importante para se afirmar que Bitcoin é moeda é a necessidade de ser reconhecido pelo Estado, haver uma legislação específica que o ratifique como moeda, e até o presente momento não temos essa ratificação pelo Estado brasileiro.

Uma moeda, para que assim seja considerada dentro de um sistema legal, há de convir que os caracteres de “curso legal” e “poder libertário”, nenhum dos quais o Bitcoin lança mão sobre. O curso legal é o atributo da moeda que tem o seu lastro na Lei do país em que ele se expressa, enquanto que, dotada de poder liberatório, a moeda deve ser aceita obrigatoriamente por qualquer um dentro do território nacional daquele país.

O curso legal do Real, por exemplo, foi instituído pela Lei 9.069, de 29 de junho de 1995, que determinou que “a partir de 1º de julho de 1994, a Unidade do Sistema Monetário Nacional passa a ser o REAL (art. 2º da Lei 8.880, de 27 de maio de 1994 (LGL/1994/46)), que terá curso legal em todo o território nacional.

O mesmo não se dá com o Bitcoin. Em razão de não ser reconhecido como moeda no Brasil, ninguém pode forçar outrem a quitar dívida por meio de transferência de Bitcoin. Eis a razão pela qual uma moeda, para assim ser reconhecida, tem de prover garantia aos seus usuários de que ela será aceita quando efetuarem suas transações. (MEIRELES, SILVEIRA E FILHO, 2019)

Portanto, entendemos que Bitcoin é uma riqueza que precisa ser convertida, afim de que possa auferir valor, sendo que deve haver liquidez, aceitação e ratificação pelo Estado, para que seja compreendido como moeda.

b) Natureza jurídica de ativo

Entendemos que esta é a melhor classificação no momento para o Bitcoin, este ser considerado um ativo, uma reserva de valor, visto que um ativo é a somatória de bens, de valores, ou créditos pertencentes a uma pessoa ou a uma empresa.

Diante deste nosso entendimento de que Bitcoin é um ativo, no caso um ativo monetário, é preciso entendermos alguns tipos de ativos existentes: ativo de capital (*capital assets*); ativo monetário (*current assets*); ativo financeiro (*financial assets*) e ativo tóxico (*toxic assets*).

O primeiro (ativo de capital) refere-se a um ativo o qual algo, como terra, imóveis ou máquinas, são utilizados por algum negócio, e estes irão dar como resultado algum bem ou serviço, havendo, portanto, um ganho de capital.

O segundo (ativo monetário) diz respeito à riqueza que se tem ou é devido, ou algo que pode ser convertido em dinheiro, a exemplo de: matéria-prima, bens que foram produzidos, mas não foram vendidos, ao próprio dinheiro ou seus equivalentes, como as criptomoedas, em específico o Bitcoin, recebíveis, inventários.

O terceiro (ativo financeiro) tange aquele ativo que possui um valor inerente, específico, como, por exemplo: as ações, títulos e depósitos bancários, mas é válido ressaltar que não possuem aspecto físico.

O quarto (ativo tóxico) concerne àquele ativo que apresenta um elevado risco, tendo o seu valor já com queda, ou com a possibilidade de queda. Um exemplo o qual estudamos neste trabalho são os *subprimes*.

c) Natureza jurídica de commodities

A respeito de se pensar o Bitcoin como uma *commoditie*, entendemos que é um entendimento um tanto forçado, mas há defensores desta ideia. Igualar o Bitcoin, ou criptomoedas em geral, a um minério, soja, petróleo, é uma maneira equivocada de se pensar,

pois aqueles derivam de matéria-prima encontrada na natureza e são comercializadas em massa e no estado bruto, totalmente contrárias ao que é o Bitcoin, as criptomoedas, as quais são provenientes de um código matemático e não são comercializadas em massa. Portanto, entender as criptomoedas como *commodities* é algo fora de cogitação.

Dessa forma, a concepção de que o Bitcoin é uma *commoditie* é algo um pouco forçado, apesar de, em alguns países, como na Indonésia, ele ser tratado como uma *commoditie*.

d) Natureza jurídica de bem imaterial

Bens imateriais são aqueles que são bens, os quais possuem ou não valor monetário. A exemplo temos: liberdade, ideias ou invenções.

Esta concepção surgiu pelo fato de que o Bitcoin e as criptomoedas, especificamente seus códigos-fonte e software, poderiam ser protegidos.

(...) Immaterial goods are goods that are not things and yet have monetary or non-monetary value. Examples of immaterial goods are freedom, ideas or inventions.
 (...) This conclusion flows from the understanding that crypto currencies are not original personal creations, and thus, according to section 2 (2) of the Copyright Act, they cannot be protected. Only the source code and software of a cryptocurrency might be protected by the copyright law, but not the currency unit (or a part of a currency unit) evolving out of the source code. (...) (BRITO, p. 116)⁴⁰

Entendemos que é uma ideia equivocada haver a cogitação de que o Bitcoin possa ter natureza jurídica de bem imaterial, devido ao fato de que a criptomoeda é algo que pode ser contável, e bem imaterial é algo incontável.

e) Natureza jurídica de valor mobiliário

Em nosso ordenamento jurídico, o legislador deixou muito amplo o que seria valor mobiliário, o rol do art. 2º da Lei 6385, de 07 de dezembro de 1976, nos informa quais seriam os tipos de valores mobiliários, vejamos:

⁴⁰ (...) Bens imateriais são bens que não são coisas, no entanto, têm valor monetário ou não têm valor monetário. Exemplo de bens imateriais são liberdade, ideias ou invenções. (...) (tradução livre)
 (...) Esta conclusão decorre do entendimento de que as criptomoedas não são criações pessoais originais, e assim, de acordo com a seção 2 da Lei de Direitos Autorais, eles não podem ser protegidos. Apenas o código-fonte e o software da criptomoeda talvez poderia ser protegido pela lei de direitos autorais, mas não a unidade de moeda (ou a parte de uma unidade monetária) envolvendo o código-fonte. (tradução livre)

Art. 2º São valores mobiliários sujeitos ao regime desta Lei: (Redação dada pela Lei nº 10.303, de 31.10.2001)

I - as ações, debêntures e bônus de subscrição; (Redação dada pela Lei nº 10.303, de 31.10.2001)

II - os cupons, direitos, recibos de subscrição e certificados de desdobramento relativos aos valores mobiliários referidos no inciso II; (Redação dada pela Lei nº 10.303, de 31.10.2001)

III - os certificados de depósito de valores mobiliários; (Redação dada pela Lei nº 10.303, de 31.10.2001)

IV - as cédulas de debêntures; (Inciso incluído pela Lei nº 10.303, de 31.10.2001)

V - as cotas de fundos de investimento em valores mobiliários ou de clubes de investimento em quaisquer ativos; (Inciso incluído pela Lei nº 10.303, de 31.10.2001)

VI - as notas comerciais; (Inciso incluído pela Lei nº 10.303, de 31.10.2001)

VII - os contratos futuros, de opções e outros derivativos, cujos ativos subjacentes sejam valores mobiliários; (Inciso incluído pela Lei nº 10.303, de 31.10.2001)

VIII - outros contratos derivativos, independentemente dos ativos subjacentes; e (Inciso incluído pela Lei nº 10.303, de 31.10.2001)

IX - quando ofertados publicamente, quaisquer outros títulos ou contratos de investimento coletivo, que gerem direito de participação, de parceria ou de remuneração, inclusive resultante de prestação de serviços, cujos rendimentos advêm do esforço do empreendedor ou de terceiros.

A partir do rol informado em lei, percebemos que o Bitcoin não se insere, pois sua constituição não advém de uma pessoa jurídica formalmente constituída, diferentemente do que ocorre com os valores mobiliários que contam na lei, e os mesmos são instrumentos ofertados por terceiro para que se tenha investidores que apliquem o seu dinheiro, com o intuito de obter lucro, por meio do papel do negócio ofertado por terceiro ao público.

O Bitcoin, apesar de ser um instrumento de investimento, ofertado ao público, para que se obtenha lucro, não devemos compará-lo como um valor mobiliário, visto que não deriva de uma pessoa jurídica, ou seja, sua emissão não advém de um negócio de um terceiro. Na verdade, o Bitcoin provém de um código aberto, disponível na internet, tornando-se acessível a qualquer pessoa ao redor do globo, diferentemente do que ocorre com os valores mobiliários, pois está vinculado a uma pessoa jurídica, a qual está sobre a supervisão do Estado. Já o Bitcoin é supervisionado por todos, devido ao seu caráter descentralizado.

Assim, diante do exposto, não devemos entender a natureza jurídica do Bitcoin como sendo a de um valor mobiliário.

5.1 - A Questão da Regulação

No Brasil, a questão da regulação das criptomoedas ainda é incipiente. Mas você pode se perguntar: se as criptomoedas são uma tecnologia distribuída e descentralizada, por que o Estado vai intervir? Entendemos que deve haver uma mínima regulação neste mercado, pois é preciso haver diretrizes, visto que, se deixarmos a tecnologia se autorregular, ou seja, o “código” ser lei, pode ser algo incontrolável e ser danoso para a sociedade. Portanto, direcionamentos mínimos de regulação pelo Estado, compreendemos que se faz necessário.

Podemos elencar algumas questões importantes no cenário brasileiro no que se refere à falta de regulamentação por parte do Estado.

a) Documentos exigidos pelas Exchanges

As *Exchanges* no Brasil, para se inscrever, cada uma pede um modo de solicitação: umas pedem a anexação de um documento com foto, mais CPF; outras não exigem nenhuma confirmação de dados, apenas a inscrição de um nome e senha. Portanto, para que esses dados? O que irão fazer com esses dados? Como proteger o usuário de utilização indevida de seus dados pelas *Exchanges*? São perguntas como essas que, por carência de regulação, ficamos sem saber de respostas.

b) Fechamento de Exchange e a não garantia de criptomoedas depositadas

No caso de falência, ou mesmo fechamento arbitrário por parte do(s) dono(s), como resgatar as criptomoedas custodiadas nas *Exchanges*? No mercado financeiro tradicional há a exigência do Estado para o banco, a questão do Fundo Garantidor, ou seja, que é a garantia, por CPF, de retorno financeiro de um banco para o cliente em caso de falência da instituição financeira, a garantia é no valor de R\$ 250.000,00 (duzentos e cinquenta mil reais). Ou seja, não importa o valor de quanto a pessoa tem depositado no banco, o valor de retorno por CPF será de somente de R\$ 250.000,00 (duzentos e cinquenta mil reais). Dessa forma, como o

usuário, que deixa as suas criptomoedas custodiadas na Exchange, fica no caso de falência ou fechamento arbitrário? Não há nenhuma lei que obriga a devolução de um valor por CPF, ou seja, não há um Fundo Garantidor para o usuário de criptomoedas.

c) Fiscalização de lavagem de dinheiro

Não há nenhum método, nem por parte das *Exchanges* e nem por parte do Estado, que possa impedir a ocorrência de lavagem de dinheiro no âmbito das criptomoedas. Entendemos que, se o Estado usar algum meio de fiscalização, a rede pode continuar descentralizada. Mas como? O Estado irá usar método, ainda em pesquisa, para de alguma forma fazer parte da *Blockchain* de uma criptomoeda, mas claro que essa fiscalização deve ser regulamentada para que não haja abuso por parte do Estado e a rede continue distribuída, descentralizada e a base do consensus entre as partes atuantes na rede.

d) Invasão cibernética

Como o Estado irá atuar para identificar e responsabilizar os responsáveis por eventuais ataques cibernéticos na rede? Apesar de a rede do *Blockchain* ser *peer-to-peer* e descentralizada, há uma maior dificuldade para que *hackers* invadam o seu sistema, mas a mesma não está imune a tal ataque. Pois, para que um *hacker* invada a rede *Blockchain*, ele precisa se conectar com todos os computadores conectados à rede, o que torna o seu “ataque” mais difícil.

e) Partilha de bens e Sucessão

No caso da partilha de bens por divórcio ou falecimento, como fica a divisão pela partilha e herança de Bitcoins? O cônjuge deve informar o seu patrimônio em criptomoedas? E no caso de falecimento, a Exchange ou a plataforma em que o usuário depositava suas criptomoedas, devem informar o valor deixado?

f) Declaração de Imposto de Renda

O usuário deve informar ao Estado quanto possui em criptomoedas?

A partir da Instrução Normativa da Receita Federal nº 1888, de 03 de maio de 2019, a qual estudaremos mais à frente, será necessário fazer a declaração das criptomoedas adquiridas a partir de um valor determinado pela Receita Federal, sob pena de sofrer alguma sanção, bem como as *Exchanges* passarão a ser de cunho obrigatório a prestação de informações no que se refere a operações efetuadas com criptoativos.

g) Fraudes e Pirâmides Financeiras

Com a falta de regulação, os usuários do sistema das criptomoedas estão mais sujeitos a caírem em fraudes, como, por exemplo, a vítima deixava as suas criptomoedas sob custódia de uma *Exchange* e simplesmente o dono desta sumia com o dinheiro. Ou em pirâmides financeiras, esta se refere ao fato de que quanto mais pessoas fizerem parte de um grupo “X”, a quantidade de pessoas será o quanto irá haver de retorno para os participantes. Ou em esquemas Ponzi, que diz respeito ao fato de a vítima fazer um depósito inicial em troca de um retorno de um valor “X” garantido.

No Brasil, os casos ocorridos, em grande parte, os criminosos entregavam às vítimas uma ideia de, a partir de um depósito inicial, um retorno alto e significativo em pouco espaço de tempo. Ou simplesmente ludibriavam a vítima para que as mesmas depositassem um valor e deixassem sob a custódia da pessoa jurídica, e assim o dono fugia com o dinheiro, ou utilizava o valor, e quando a vítima necessitava do resgate, o dono não tinha liquidez para o pagamento.

Desse modo, a inexistência de regulação no Brasil para as criptomoedas, infelizmente permite que pessoas sejam vítimas de golpes e fraudes, o que denigre a imagem e impede o avanço e a evolução desse sistema disruptivo.

5.2 - A Regulação

Primeiramente, para facilitar a compreensão, vamos entender a etimologia da palavra regulação, a qual é o ato ou efeito de regular. Portanto, regular algo conforme as leis, a praxe, a natureza.

No sentido jurídico, Marçal Justen Filho, disserta:

A regulação econômico-social consiste na atividade estatal de intervenção indireta sobre a conduta dos sujeitos públicos e privados, de modo permanente e sistemático, para implementar as políticas de governo e a realização dos direitos fundamentais. (FILHO, p. 677)

Portanto, o ato de regular é a intervenção indireta do Estado na ações dos entes públicos e privados em seus ramos de atividades, sendo que esta regulação será permanente e sistemática.

A regulação é uma atividade exclusiva do Estado, concernente a todas as esferas federativas, a qual possui como característica natureza normativa, objetivando atuar como uma forma repressiva e promocional, a fim de mudar e guiar as práticas de condutas dos sujeitos públicos e privados.

A regulação se caracteriza pela organização de meios materiais e humanos com a criação de estruturas administrativas especializadas, visando a desempenho contínuo e racional. A regulação consiste não apenas na produção de normas e atos decisórios, mas na produção *ordenada* de normas e atos decisórios. (FILHO, p. 678)

A partir deste entendimento, a regulação é uma forma de ordenamento de conduta para os sujeitos envolvidos em uma determinada situação, sendo um norte para as suas tomadas de decisões particulares, sendo que estas não podem ser nem aquém e nem além do que determina a lei. Se levarmos estes conceitos para a esfera econômica, o Estado não atua como sujeito de atividade empresarial, mas intervém de modo significativo e enfático, com o objetivo de o mercado não se autorregular e criar modelos de negócios que podem ser catastróficos para a economia. O Estado terá sua atuação como observador e interventor quando for preciso, a fim de proteger sua economia e o seus cidadãos de práticas indevidas dos agentes financeiros.

Como assinala Carlos Ari Sundfeld:

A regulação é - isso, sim - característica de certo modelo econômico, aquele em que o Estado não assume diretamente o exercício de atividade empresarial, mas intervém enfaticamente no mercado utilizando instrumentos de autoridade. Assim, a regulação não é própria de certa família jurídica, mas sim de uma opção de política econômica. (FILHO, p. 680)

Em nosso ordenamento jurídico, a competência regulatória compete aos diversos entes da federação, e os critérios de regulação estão descritos constitucionalmente.

A produção da regulação compete ao regulador praticar atividades vinculadas e adotar tendências de escolha discricionária. Mas é válido salientar que o Estado não deve

realizar uma regulação fora da realidade e do conhecimento técnico do assunto a ser regulado, deve-se basear a regulação em critérios objetivos

(...) Justamente por isso, a validade da regulação depende da observância de um procedimento adequado a identificar os problemas, a avaliar as consequências das soluções cabíveis, a permitir a ampla discussão das propostas e a demonstrar que a escolha adotada é a mais satisfatória. (FILHO, p. 683)

Observando estes critérios, o ordenamento jurídico não aceita comportamento imprudente, desatencioso, e reprova qualquer dano causado por ações culposas dos sujeitos envolvidos. Com isso, principalmente no âmbito dos particulares, o Estado abomina condutas danosas, provenientes da inexistência de observância de atos adequados por parte dos sujeitos privados.

Recai sobre todo agente estatal um dever de diligência especial. O sujeito investido em competências estatais tem o dever jurídico de cercar-se de todas as precauções para evitar atuação imprecisa, defeituosa ou inadequada. (FILHO, p. 684)

Uma outra questão é que a regulação é um planejamento estatal, ou seja, o Estado deve observar o contexto atual, os possíveis problemas e os desdobramentos futuros do que se pretende regular, sendo, portanto, o planejamento um ato vinculante do Estado, conforme previsto em nossa Constituição Federal de 1988.

A natureza contínua e permanente da regulação estatal compreende uma função de planejamento. O Estado tem o dever jurídico de avaliar a situação contemporânea, identificar os problemas previsíveis do futuro e estimar as providências cabíveis e adequadas a serem adotadas. O planejamento deve traduzir-se em projetos de atuação concreta, visando a interferir sobre a realidade e orientar as providências futuras.

(...)

A titularidade da competência pública para decidir não compreende o poder jurídico para decidir impetuosamente, impensadamente ou defeituosamente. Justamente por isso, o art. 174 da CF/1988 estabelece que “Como agente normativo e regulador da atividade econômica, o Estado exercerá, na forma da lei, as funções de fiscalização, incentivo e planejamento, sendo este determinante para o setor público e indicativo para o setor privado. (FILHO, p. 685)

É válido salientar que tanto o planejamento quanto a regulação estatal, estão subordinados a um dever de observar o princípio da prevenção ou precaução, que tem o objetivo de exigir que a atuação estatal e privada seja dotada de todo o cuidado possível. Contudo, este princípio é norteado pela proporcionalidade, visto que é difícil mapear todas as alternativas possíveis. É notadamente impossível que elimine de forma absoluta a possibilidade de dano.

Um outro aspecto relevante que é necessário comentar diz respeito ao requisito de *Análise de Impacto Regulatório*. Esta análise objetiva avaliar os custos, benefícios e os efeitos da regulação pretendida, bem como coletar a maior quantidade de informações para embasar a decisão tomada pelo agente regulador. Havendo a ausência dessa análise, demonstra que o agente regulador faltou em refletir e ponderar sobre os atos necessários. Dessa forma, sua decisão não foi tomada com consciência, e sim teve um formato subjetivo, sem fundamento técnico-científico, podendo acarretar em um defeito insanável, tornando a regulação, a norma ineficaz, prejudicial à sociedade, pois não houve uma avaliação minuciosa dos possíveis impactos da regulação.

Portanto, o Estado precisa intervir indiretamente nas atividades dos sujeitos que manejam com as criptomoedas, a fim de proteger usuários, intermediários e a própria rede.

No Brasil, o legislador não acompanha o mesmo ritmo que a inovação exige, e, com essa inércia, permite que haja uma lacuna dentro do ordenamento jurídico, acarretando insegurança jurídica e ensejando, assim, a inúmeras interpretações.

A esse respeito, disserta Maria Eugênia Finkelstein:

Ocorre, no entanto, que a Internet e o comércio eletrônico ainda não apresentam regulação satisfatória, de forma que não se tem certeza da forma de solução de conflitos, caso estes se apresentem. Assim sendo, estamos diante de uma criação tecnológica que permite o desenvolvimento de sistemas ainda mais sofisticados, havendo a necessidade imediata de os juristas, juízes e legisladores orientarem-se pelos pareceres e laudos de especialistas em informática, quando a elaboração de leis ou do julgamento de lides. (FINKELSTEIN, 2016, p. 55)

Um fator relevante à regulamentação do Bitcoin, em âmbito do Direito Nacional, seria a questão das leis serem baseadas na *territorialidade*, o que difere por completo dos aspectos de transnacionalidade do Bitcoin e do próprio comércio eletrônico, pois é necessário ter uma lei que proteja o usuário brasileiro em qualquer transação com Bitcoin nacional ou internacional. Este é, portanto, um dos desafios da regulamentação do Bitcoin.

No Direito Brasileiro, bem como em quase todos os países de tradição civilista, temos que as leis encontram-se calcadas na territorialidade, o que se contrapõe diretamente ao caráter transnacional da Internet. (FINKELSTEIN, 2016, p. 55)

Assim, vamos analisar as ações que estão sendo encaminhadas por autoridades estatais brasileiras, devido à inexistência de regulação em nosso país.

5.3 - Projeto de Lei 2.303/2015

O Projeto de Lei 2.303/2015 - Banco Central Regular Moedas Digitais, está tramitando na Câmara dos Deputados, estando em fase de audiências públicas.

A seguir, mostramos o interior teor do Projeto de Lei:

PROJETO DE LEI Nº, DE 2015 (Do Sr. Aureo)

Dispõe sobre a inclusão das moedas virtuais e programas de milhagem aéreas na definição de “arranjos de pagamento” sob a supervisão do Banco Central.

O Congresso Nacional decreta:

Art. 1º Modifique-se o inciso I do art. 9º da Lei 12.865, de 09 de outubro de 2013:

“Art. 9º

I - disciplinar os arranjos de pagamento; incluindo aqueles baseados em moedas virtuais e programas de milhagens aéreas;”

Art. 2º Acrescente-se o seguinte § 4º ao art.11 da Lei 9.613, de 03 de março de 1998:

“Art. 11

§ 4º As operações mencionadas no inciso I incluem aquelas que envolvem moedas virtuais e programas de milhagens aéreas”

Art. 3º - “Aplicam-se às operações conduzidas no mercado virtual de moedas, no que couber, as disposições da Lei nº 8.078, de 11 de setembro de 1990, e suas alterações.

Art. 4º - Esta Lei entra em vigor na data de sua publicação”.

JUSTIFICAÇÃO

As chamadas “moedas virtuais” ganham cada vez mais destaque nas operações financeiras atuais.

Apesar de não haver ainda uma regulamentação nem nacional e nem internacional sobre a matéria, há uma preocupação crescente com os efeitos das transações realizadas por meios destes instrumentos.

O assunto mereceu um relatório especial do Banco Central Europeu (BCE), em outubro de 2012⁴¹, que foi atualizado em fevereiro de 2015⁴². Apesar de concluir pela desnecessidade da introdução imediata de uma regulação mais ativa sobre as moedas virtuais, tal relatório aponta um conjunto de riscos que devem ser devidamente monitorados. Colocaremos a seguir um quadro com cada uma das principais conclusões do relatório e um comentário.

⁴¹ Virtual currency Schemes. European Central Bank. October, 2012 <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>. Acesso em:

⁴² Virtual Currency Schemes – a further analysis. February, 2015. <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>

Quadro I

Riscos Apontados pelo Relatório sobre Moedas Virtuais do BCE	Comentário
“Não impõe um risco sobre a estabilidade de preços, conquanto a criação de moeda permaneça em um nível baixo” (tradução livre) ⁴³ .	Como bem ressalvado, o efeito das moedas virtuais sobre a estabilidade de preços ainda traz preocupações enquanto estes mecanismos não cresceram em relação à economia. Assumindo ser inevitável que eles realmente continuem crescendo junto ao incremento do uso da internet, cabe monitorar a partir de que ponto esta premissa deixará de ser verdadeira.
“tendem a ser inerentemente instáveis, mas não têm o condão de comprometer a estabilidade financeira do país dada a sua conexão limitada com a economia real, seu baixo volume negociado e a falta de aceitação tão ampla entre os usuários” (tradução livre) ⁴⁴ .	Mais uma vez, o Relatório do BCE faz a devida ressalva de que a desnecessidade de regulação imediata depende da (ainda) baixa amplitude de adoção dessas moedas virtuais. Com o crescimento da internet impulsionando as moedas virtuais, haverá um natural incremento de pontos de conexão com a economia real, podendo passar a ameaçar a estabilidade financeira. De qualquer forma, o Relatório indica que tais esquemas são inerentemente instáveis, com elevada volatilidade da sua relação de troca com a moeda local.
“não é regulado no presente momento e não é supervisionado ou fiscalizado de perto por qualquer autoridade pública ainda que a participação nesses esquemas exponha os usuários a riscos de crédito, liquidez, operacionais e legais” (tradução livre) ⁴⁵ .	Aqui a preocupação é menos sistêmica e mais de direito do consumidor. Os usuários desses mecanismos estão inadvertidamente expostos a riscos financeiros significativos e sem proteção legal alguma.
“podem representar um desafio às autoridades públicas, dada a incerteza legal por trás destes esquemas que podem ser utilizados por criminosos fraudadores e pessoas que lavam dinheiro para realizar suas operações ilegais” (tradução livre) ⁴⁶ .	As moedas virtuais facilitam atividades criminosas, especialmente lavagem de dinheiro.
“podem ter um efeito negativo sobre a reputação dos Bancos Centrais, assumindo que o uso de tais sistemas cresce consideravelmente e	Um esquema que pode ser entendido como uma “pirâmide” que acaba desmoronando pode ser interpretado como uma

⁴³ “do not pose a risk to price stability, provided that money creation continues to stay at a low level”

⁴⁴ “tend to be inherently unstable, but cannot jeopardise financial stability owing to their limited connection with the real economy, their low volume traded and a lack of wide user acceptance”.

⁴⁵ “are currently not regulated and are not closely supervised or overseen by any public authority, even though participation in these schemes exposes users to credit, liquidity, operational and legal risks”;

⁴⁶ “could represent a challenge for public authorities, given the legal uncertainty surrounding these schemes, as they can be used by criminals, fraudsters and money launderers to perform their illegal activities”;

que no caso de um incidente atrair a cobertura da imprensa, o público pode perceber o incidente como sendo causado, em parte, pelo fato de o Banco Central não estar fazendo o seu trabalho” (tradução livre). ⁴⁷	“barbearagem” do Banco Central minando a sua credibilidade.
“recaem sob a responsabilidade dos Bancos Centrais na medida que o seu funcionamento tem características compartilhadas com os sistemas de pagamento, o que implica a necessidade de exame de pelo menos alguns dos seus desenvolvimentos e a provisão de uma avaliação inicial” (tradução livre) ⁴⁸ .	Constitui um reconhecimento de que as moedas virtuais constituem sistemas de pagamento e como tal devem ser monitoradas de perto.

Sobressai-se nesta análise das moedas virtuais o que é considerado o maior caso de “sucesso” que é o Bitcoin. Conforme o relatório do ECB de 2012: “Desenhado e implementado pelo programador japonês Satoshi Nakamoto em 2009, o esquema é baseado em uma rede *peer-to-peer* similar ao Bit Torrent, o famoso protocolo de compartilhamento de arquivos como filmes, jogos e música na internet. O Bitcoin opera globalmente e pode ser usado como moeda para todos os tipos de transação (para ambos bens, e serviços virtuais e reais), competindo portanto com as moedas oficiais como o euro e o dólar... Embora o Bitcoin seja um esquema de moeda virtual, possui algumas inovações que a tornam mais similar à moeda convencional” (tradução livre).⁴⁹

O mais importante para nós, no entanto, são os riscos potenciais apontados no relatório para o Bitcoin:

“De tempos em tempos, o Bitcoin é cercado por controvérsias. Algumas vezes ressalta-se o seu potencial para se tornar uma alternativa monetária ao tráfico de drogas e lavagem de dinheiro, como resultado do elevado grau de anonimato. Em outras ocasiões, os usuários têm reclamado ter sofrido um roubo substancial de Bitcoins através de um “cavalo de troia” que ganhou acesso ao seu computador. A Fundação Fronteira Eletrônica, que é uma organização que busca defender a liberdade no mundo digital, decidiu não mais aceitar doações em Bitcoins. Entre as razões dadas, eles consideram “que a Bitcoin gera preocupações legais ainda não testadas relacionadas às lei de ativos financeiros, como o “*Stamp Payment Act*” (legislação que proíbe qualquer pagamento abaixo em moeda, nota ou cheque abaixo de \$ 1), de evasão de tributos, de proteção do consumidor e lavagem de dinheiro, entre outros”. (tradução livre)⁵⁰

⁴⁷ “could have a negative impact on the reputation of central banks, assuming the use of such systems grows considerably and in the event that an incident attracts press coverage, since the public may perceive the incident as being caused, in part, by a central bank not doing its job properly;”

⁴⁸ “do indeed fall within central banks’ responsibility as a result of characteristics shared with payment systems, which give rise to the need for at least an examination of developments and the provision of an initial assessment.”

⁴⁹ “Designed and implemented by the Japanese programmer Satoshi Nakamoto in 2009, the scheme is based on a peer-to-peer network similar to BitTorrent, the famous protocol for sharing files, such as films, games and music, over the internet. It operates at a global level and can be used as a currency for all kinds of transactions (for both virtual and real goods and services), thereby competing with official currencies like the euro or US dollar..... Although Bitcoin is a virtual currency scheme, it has certain innovations that make its use more similar to conventional money”.

⁵⁰ “From time to time, Bitcoin is surrounded by controversy. Sometimes it is linked to its potential for becoming a suitable monetary alternative for drug dealing and money laundering, as a result of the high degree of anonymity. 9 On other occasions, users have claimed to have suffered a substantial theft of Bitcoins through a

O Relatório do BCE também possui um box específico (box 1) para os programas de milhagem. O efeito de tais programas, enquanto uma “moeda paralela”, não pode ser subestimado. O Relatório cita matéria do “The Economist” de 2005 que mostra que tais programas, já naquela época, atingiam valores significativos, inclusive ultrapassando a quantidade de dólares em circulação. O Relatório inclui os programas de milhagem como um tipo específico de “moeda virtual”.

Em certa medida, acreditamos que tanto o Banco Central como o Conselho de Controle de Atividades Financeiras (Coaf) e os órgãos do consumidor já tem competência para fiscalizar e regular moedas virtuais. No entanto, entendemos que as legislações que conferem tais atribuições podem ser mais transparentes em relação a tais atribuições, o que evita desnecessários questionamentos judiciais.

Sendo assim, endereçamos no projeto de lei proposto três questões relacionadas às moedas virtuais, uma em cada artigo: i) regulação prudencial pelo Banco Central, ii) lavagem de dinheiro e outras atividades ilegais e iii) defesa do consumidor. Deixamos claro no art. 1º que os “arranjos de pagamento” citados no inciso I do art. 9º da Lei 12.865, de 09 de outubro de 2013, inclui “aqueles baseados em moedas virtuais e programas de milhagens aéreas”. Ademais, deixamos claro no art. 2º que as operações que envolvem moedas virtuais estão incluídas na fiscalização do Coaf. Por fim, não deixamos margem a dúvida de que a legislação de defesa do consumidor se aplica ao mundo das moedas virtuais no art. 3º.

Contamos com o apoio dos nobres pares para a aprovação desta importante medida para reduzir os riscos das moedas virtuais contra a estabilidade financeira da economia, diminuir a possibilidade delas financiarem atividades ilegais, além de proteger o consumidor contra eventuais abusos.

Sala das Sessões, em ? de ? de 2015.

Deputado AUREO

Esse projeto de lei está desde 2015 em fase de audiências públicas, com isso a falta de regulamentação deixa o mercado de criptomoedas aguardando definições de procedimentos das autoridades.

5.4 - Projeto de Lei Nº 2.060/2019

O Projeto de Lei nº 2.060/2019 foi apresentado no mês de abril de 2019, do Deputado Aureo Ribeiro, do Rio de Janeiro, com o objetivo de dispor sobre o regime jurídico dos criptoativos. Este projeto está em fase de tramitação pela Câmara dos Deputados.

Neste projeto de lei, há a descrição no artigo 1º, de quais são os tipos de criptoativos: a) os criptoativos que são usados como meio de pagamento; b) os que são reserva de valor; c) os que são utilidade e valor mobiliário. Neste projeto não está somente em estudo quais são os

Trojan that gained access to their computer. 10 The Electronic Frontier Foundation, which is an organization that seeks to defend freedom in the digital world, decided not to accept donations in Bitcoins anymore. Among the reasons given, they considered that “Bitcoin raises untested legal concerns related to securities law, the Stamp Payment Act, tax evasion, consumer protection and money laundering, among others”

tipos de criptoativos, mas também o entendimento de aumento de pena para aqueles que cometem crime de “pirâmide financeira”, e também para os crimes que dizem respeito ao uso fraudulento de criptoativos.

PROJETO DE LEI ?, DE 2019
(Do Sr. Aureo Ribeiro)

Dispõe sobre o regime jurídico de Criptoativos.

O CONGRESSO NACIONAL decreta:

Capítulo I - Disposições Preliminares

Art. 1º - Esta lei dispõe sobre Criptoativos, que englobam ativos utilizados como meio de pagamento, reserva de valor, utilidade e valor mobiliário, e sobre o aumento de pena para o crime de “pirâmide financeira”, bem como para crimes relacionados ao uso fraudulento de Criptoativos.

Capítulo II - Definições

Art. 2º - Para a finalidade desta lei e daquelas por ela modificadas, entende-se por criptoativos:

I – Unidades de valor criptografadas mediante a combinação de chaves públicas e privadas de assinatura por meio digital, geradas por um sistema público ou privado e descentralizado de registro, digitalmente transferíveis e que não sejam ou representem moeda de curso legal no Brasil ou em qualquer outro país;

II – Unidades virtuais representativas de bens, serviços ou direitos, criptografados mediante a combinação de chaves públicas e privadas de assinatura por meio digital, registrados em sistema público ou privado e descentralizado de registro, digitalmente transferíveis, que não seja ou representem moeda de curso legal no Brasil ou em qualquer outro país;

III – Tokens Virtuais que conferem ao seu titular acesso ao sistema de registro que originou o respectivo token de utilidade no âmbito de uma determinada plataforma, projeto ou serviço para a criação de novos registros em referido sistema e que não se enquadram no conceito de valor mobiliário disposto no art. 2º da Lei no 6.385, de 7 de dezembro de 1976;

Parágrafo único. Considera-se intermediador de Criptoativos a pessoa jurídica prestadora de serviços de intermediação, negociação, pós- negociação e custódia de Criptoativos.

Capítulo III - Das operações com Criptoativos

Art. 3º - É reconhecida a emissão e circulação de Criptoativos, observado o disposto na legislação em vigor.

Art. 4º - A emissão de Criptoativos, sob o escopo desta Lei, poderá ser realizada por pessoas jurídicas de direito público ou privado, estabelecidas no Brasil, desde que a finalidade à qual serve a emissão dos Criptoativos seja compatível com as suas atividades ou com seus mercados de atuação.

§ 1º - Observado o disposto neste artigo, é livre a emissão de criptoativos de utilidade, bem como de outros tipos de criptoativos que, por sua natureza ou pela natureza dos bens, serviços e/ou direitos subjacentes, não estejam sujeitos à regulação específica.

§ 2º - A emissão de criptoativos que, por sua natureza ou pela natureza dos bens, serviços ou direitos subjacentes, estejam sujeitos à regulação específica a ela devem se submeter.

Capítulo IV - Disposições Finais

Art. 5º - O § 1º do art. 2º da Lei 6.385, de 7 de dezembro de 1976, passa a vigorar acrescida do seguinte inciso III:

“Art. 2º

.....

§ 1º

.....

III – Criptoativos, ainda que tenham os seus valores correspondentes ao valor de cotas de pessoas jurídicas”. (NR)

Art. 6º - O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), passa a vigorar acrescido do seguinte artigo 292-A:

“Art. 292-A - Organizar, gerir, ofertar carteiras, intermediar operações de compra e venda de Criptoativos com o objetivo de pirâmide financeira, evasão de divisas, sonegação fiscal, realização de operações fraudulentas ou prática de outros crimes contra o Sistema Financeiro, independentemente da obtenção de benefício econômico:

Pena - detenção, de um a seis meses, ou multa.”

Art. 7º - A Lei nº 1.521, de 26 de dezembro de 1951, passa a vigorar acrescida do seguinte artigo 2º-A:

“Art. 2º-A - Constitui crime da mesma natureza obter ou tentar obter ganhos ilícitos em detrimento de uma coletividade de pessoas, ainda que indetermináveis, mediante especulações ou processos fraudulentos (“bola de neve”, “cadeias”, “pichardismo”, “pirâmides” e quaisquer outros equivalentes)”.

Pena - reclusão, de um a cinco anos, e multa.

Art. 8º - A Lei nº 6.385, de 7 de dezembro de 1976, passa a vigorar acrescida do seguinte artigo 28-A:

“Art. 28-A - A Comissão de Valores Mobiliários pode dispensar o registro de atividades regulamentadas nos termos da Lei, com a finalidade de instituir ambiente de testes de novas tecnologias e inovações em produtos e serviços no mercado de valores mobiliários.

Parágrafo único. A Comissão de Valores Mobiliários pode dispensar o registro previsto no caput deste artigo dentro de limites e restrições preestabelecidos, observando:

I – os riscos e benefícios de cada autorização; e

II – o estímulo a iniciativas inovadoras ou de médio ou pequeno porte que visem conferir maior eficiência, segurança e ampliação do acesso ao mercado de valores mobiliários.”

Art. 9º. Fica revogado o inciso IX do artigo 2º da Lei no 1.521, de 26 de dezembro de 1951.

Art. 10 - Essa Lei entra em vigor na data de sua publicação.

JUSTIFICAÇÃO

O projeto de lei em questão tem como finalidade criar um ambiente em que os elementos positivos da tecnologia do Blockchain sirvam a fomentar a higidez e transparência do Sistema Financeiro Nacional e, ao mesmo tempo, às necessidades da economia e aos anseios da população.

Os benefícios da regulação para utilização das Criptomoedas e Tokens Virtuais são diversos. Essencialmente segura, a tecnologia, quando fomentada em ambiente regulado, constitui elemento instrumental à redução de fraudes nas relações comerciais, dada a imutabilidade de sua cadeia de blocos de dados. Serve, ademais, por seu caráter público, ao combate à lavagem de dinheiro e à corrupção, utilidade que se mostra premente no atual contexto brasileiro.

O esforço regulatório está presente em todos os países e deve estar também em um nível supranacional, visto que o alcance dos Estados sobre tais operações é limitado. Porém, justamente para permitir uma coordenação mais ampla e eficaz, não pode a regulação interna ser desmedida a ponto de tolher transações entre agentes nacionais e entre agentes nacionais e estrangeiros. O aspecto “sem fronteiras” é intrínseco às trocas de

Criptomoedas e Tokens Virtuais, pelo que as regulações nacionais que incidem sobre tais operações não podem ser restritivas e congelar tal potencialidade ao tentar adequá-las aos moldes de investimentos e ativos financeiros tradicionais.

Sala das Sessões, em de de 2019
Dep. AUREO RIBEIRO (Solidariedade/RJ)

A justificativa para a criação deste projeto é a de se permitir a confluência dos interesses dos cidadãos em utilizar a tecnologia *blockchain*, em face de haver uma regulamentação que ampare essa utilização e permita uma maior evolução no cenário econômico, permitindo a aceitação pelo Sistema Financeiro Nacional das criptomoedas.

A regulamentação entende que não deve ser limitativas a ponto de paralisar o potencial econômico e tecnológico advindo do âmbito dos criptoativos, bem como não se pode pensar em um formato de regulação que se aproxime muito das que são utilizadas para regular o sistema financeiro tradicional em nosso país, dado o caráter inovador e econômico que tal tecnologia propicia.

5.5 - Instrução Normativa da Receita Federal

A Receita Federal instrui que deve-se declarar no Imposto de Renda quem movimentou mais de R\$ 30.000,00 (trinta mil reais) ao mês em moedas digitais, devendo, portanto, recolher a porcentagem de 15% em tributo.

Dessa forma, apesar de as criptomoedas não serem consideradas como moeda para a Receita Federal, e ao mesmo tempo não haver regulamentação, esta entende que deve-se

equiparar as criptomoedas a ativos financeiros, e com isso devem ser declaradas pelo valor de aquisição no Imposto de Renda.

Nesta Instrução Normativa, a Receita Federal inclui a obrigatoriedade de envio de informações mensais pelas *Exchanges* e pelas pessoas físicas a partir de agosto de 2019, instruções para procedimentos das *Exchanges* para com os usuários. Outra novidade é a inclusão de penalidades em caso de descumprimento das ações que devem tomar as pessoas físicas e jurídicas, apresentadas na Instrução Normativa.

O inteiro teor da instrução normativa está no Anexo II, ao final do trabalho.

5.6 - Comunicados do Banco Central

Em 2014, o Banco Central emitiu o Comunicado 25.306, datado de 19 de fevereiro, o qual avisava sobre os riscos da aquisição de “moedas virtuais” e das transações feitas com elas, bem como informava a diferença entre moeda eletrônica (são as moedas nacionais, que são transacionadas e armazenadas em dispositivos ou sistemas móveis) e moeda virtual (moedas que não são emitidas por nenhum Estado Nacional), e que não havia nenhuma autoridade governamental responsável por sua gestão, regulação e comercialização.

Já no ano de 2017, o Banco Central do Brasil novamente emitiu um Comunicado (nº 31.379), datado de 16 de novembro, alertando a respeito dos riscos provenientes de operação de guarda e negociação das moedas virtuais.

Dessa forma, o Banco Central do Brasil, instituição que emite moedas e que demanda diretrizes sobre o Sistema Financeiro Nacional, emitiu suas considerações a respeito das criptomoedas, informando à sociedade os potenciais riscos de aquisição e utilização.

5.7 - Nota da Comissão de Valores Mobiliários (CVM)

A Comissão de Valores Mobiliários (CVM), é uma autarquia federal que regula o mercado financeiro. No mercado de ações existe o chamado IPO, do termo em inglês (*Initial Public Offering*), que diz respeito à oferta pública de ações a ser negociada em bolsa de valores. Usando a analogia do mercado tradicional de ações, quando há uma oferta pública de criptomoedas, normalmente para arrecadar fundos para o desenvolvimento do projeto, chama-se ICO, do inglês, (*Initial Coin Offering*), oferta pública de criptomoedas. Em contrapartida,

há a emissão dos chamados *tokens* ou *coins*. A respeito desse assunto, ICO, a autarquia emitiu uma nota no dia 11 de outubro de 2017, alertando sobre suas preocupações. (Anexo III)

No mês seguinte do mesmo ano, em 16 de novembro de 2017, a CVM emite novamente uma nota a respeito do ICO. Já nesta nota, ela detalha o que seria um ICO, suas modalidades e informa sobre outros aspectos relacionados ao ICO. (Anexo III)

No dia 07 de março de 2018, novamente a autarquia emite uma nota, cujo o tema é novamente o ICO, mas neste comunicado, em específico, ela não ratifica e nem faz recomendações sobre esta prática. Também informa ao investidor as atenções que este deve ter em relação aos riscos de fazer investimentos em ICO. (Anexo III)

A partir deste comunicado, a CVM emite ao investidor as precauções o qual deve adotar e que tal atividade de ICO não é regulada no país. Portanto, para a autarquia, as mesmas são práticas irregulares.

Assim, podemos perceber que instituições importantes do Estado brasileiro emitiram suas considerações e diretrizes para as criptomoedas, mas é válido ressaltar que, como não há uma regulação a respeito do assunto, principalmente no que concerne ao âmbito da Receita Federal, haverá uma obrigação de declarar a Receita a partir de agosto de 2019, mas a diretriz desse órgão é questionável, devido ao não reconhecimento das criptomoedas pelo Estado brasileiro, ocasionando, portanto, uma confusão de diretrizes emitidas pelas instituições.

5.8 - Meios de Regulação

Apesar das notas e comunicados das instituições federais, as quais destacamos no tópico anterior, no âmbito das criptomoedas não há uma regulação no país a respeito. Dessa forma, a partir do estudo de Primavera de Filippi e Aaron Wright, no livro “Blockchain and the Law - The Rule of Code”, apresentaremos as possibilidades de regulação no que concerne ao âmbito das criptomoedas, pois, como os autores afirmam, a necessidade de uma *lex cryptographica* e a tecnologia *Blockchain* apresentam uma desafio para os reguladores. Mas, apesar do sistema da tecnologia *Blockchain* ser desenhada para ignorar a lei, para se ter acesso a ela é necessário intermediários, e assim intermediários podem ser regulados.

5.8.1 - Regulação do Usuário Final

A regulação do usuário final é uma forma mais direta possível a ser utilizada pelos governos, mas entendemos que não é a mais lógica, pois estes se utilizam da rede, a qual é fornecida por algum intermediário, ou plataforma que o conecta à rede. A rede *blockchain* é baseada na transparência, pois todas as transações na rede são mostradas, mas a identificação do usuário não é feita, ou seja, o usuário é apenas uma chave, uma numeração, um código na rede.

(...) bringing actions against end users provides an incomplete solution because of the difficulty of locating and bringing actions against individuals. (DE FILIPPI, p. 176)⁵¹

Contudo, se o usuário utilizar plataformas ilegais e praticar atos ilícitos na rede, aí sim, entendemos que o Estado deva intervir, utilizando seu poder de polícia em atos considerados ilegais.

Instead of holding individuals directly responsible for the use of a blockchain-based system, governments also could hold end users vicariously liable for interacting with undesirable blockchain-based applications. (DE FILIPPI, p. 176)⁵²

É válido ressaltar que, apesar de toda tecnologia de anonimato na rede, as partes envolvidas em transações na rede *Blockchain* não estão imunes às pressão dos Estados, pois este consegue identificar os usuários por meio de sofisticados sistemas de mineração de dados e análise de *big data*.

5.8.2 - Regulação nos Provedores de Internet

Nessa possibilidade de regulação, podemos observar que o Estado pode controlar os usuários por meio dos provedores de internet, ou seja, o Estado tem uma grande habilidade em usar os ISPs, termos em inglês para *Internet Service Provider*, como ferramenta de controle.

⁵¹ (...) trazer ações contra usuários finais fornece uma solução incompleta por causa da dificuldade de localizar e promover ações contra indivíduos. (tradução livre)

⁵² Em vez de responsabilizar diretamente os indivíduos pelo uso de um sistema baseado em *blockchain*, os governos também poderiam segurar os usuários finais indiretamente responsáveis por seus interesses em aplicações indesejadas baseadas em *blockchain*.

O ISP permite a conectividade da internet, permite que todos os sujeitos que utilizam a rede *Blockchain* tenham acesso a mesma, permitindo o suporte da rede, a manutenção do *consensus* na rede.

A blockchain based network fundamentally depends on Internet connectivity and operates on top of the TCP/IP protocol. This protocol relays information between nodes supporting the network and helps nodes reach consensus as to whether they should record new data or code to the shared database. (DE FILIPPI, p. 177)⁵³

Dessa forma, regulando os provedores de internet no que diz respeito às criptomoedas, pode ser uma forma de se encontrar uma regulação da rede descentralizada e anônima, pois, a partir do conhecimento do ISP, o Estado pode chegar na identificação do usuário da rede *blockchain*.

The inherent transparency of blockchains means that ISPs can discern which computers are connected to a blockchain-based network (through their IP address or hostname) and, in some cases, even analyze the data being recorded to a blockchain. As blockchain technology spreads, governments could require that ISPs operating within their borders block data coming from and directed to a particular blockchain or - more granularly - to discriminate among transactions performed within a particular blockchain based application depending on their respective source or destination. (DE FILIPPI, p. 177)⁵⁴

Assim, apesar da possibilidade de identificação do usuário, por meio do ISP, há usuários mais habilidosos no que diz respeito ao uso da internet, e conseguem por meio de criptografia mascararem suas utilizações, continuando, portanto, anônimos e protegidos da verificação da identidade pelo ISP.

5.8.3 - Regulação dos Intermediários de Informação

Neste contexto de regulação, há a possibilidade de regular os intermediários de informação, como, por exemplo, plataformas de busca, como o Google, ou redes sociais,

⁵³ Uma rede baseada em *blockchain* depende fundamentalmente da conectividade da internet e da operação sobre o protocolo TCP/IP. Este protocolo retransmite informações entre os nós que suportam a rede e ajuda os nós a chegar a um consenso sobre se eles devem registrar novos dados ou códigos no banco de dados compartilhado. (tradução livre)

⁵⁴ A transparência inerente a *blockchain* significa que ISPs podem identificar qual computador está conectado à rede *blockchain* (por meio de seu endereço de IP ou seu nome de identificação), e, em alguns casos, analisa os dados gravados em uma *blockchain*. Como a tecnologia *blockchain* se espalha, governos poderiam exigir que os ISPs operassem junto com seus blocos vindos e direcionados para uma *blockchain* particular ou mais gradualmente, discriminando entre as transações realizadas dentro de uma aplicação baseada em *blockchain*, dependendo de suas respectivas fontes ou destino. (tradução livre)

como, Facebook e Twitter. Esse formato seria obrigar essas plataformas a não apresentarem links que indiquem as redes *Blockchains* para o usuário.

Beyond transportation layers, governments also retain the power to apply regulations on information intermediaries- such as search engines and social networks- requiring that they purposefully avoid indexing or distributing links to undesirable or illegal blockchain-based applications. (DE FILIPPI, p. 178)⁵⁵

Dessa forma, o Estado não permitiria uma maior facilidade ao usuário para acessar a rede *blockchain*, tornando esse acesso mais difícil e trabalhoso para o usuário.

5.8.4 - Regulação de Intermediários Específicos

No mundo das criptomoedas, novos negócios e serviços surgem a cada dia e, com isso, aumenta o desafio da regulação, pois estes intermediários específicos atuam diretamente na rede *Blockchain*. Um exemplo de intermediários são as *Exchanges* e as *wallets*, e, portanto, estes intermediários podem ser regulados.

É válido ressaltar que não são todas as plataformas que rodam por completo na rede *Blockchain*, ou seja, há aquelas em que somente fazem leitura de informações na rede *Blockchain*, e outras plataformas que dependem parcialmente de suas operações serem realizadas na rede. Vejamos:

For example, large companies backed by venture capital are providing “wallet” services that make it easier for people to create accounts to send and receive blockchain-based digital currencies like bitcoin and ether. Centralized exchanges also are developing, enabling people to convert digital currency into dollars, euros, or other fiat currencies. (DE FILIPPI, p. 179)⁵⁶

Então, observamos que nem todas as plataformas utilizam a rede *Blockchain* por completo. Desse modo, a futura regulação deve observar as diferenças que existem de utilização da rede por aquelas.

⁵⁵ Além das camadas de transporte, os governos também mantêm o poder de aplicar regulamentos sobre intermediários de informação - tais como motores de busca e redes sociais -, exigindo que evitem intencionalmente a indexação ou distribuição de links para aplicativos baseados em *blockchains* indesejáveis ou ilegais. (tradução livre)

⁵⁶ Por exemplo, grandes empresas apoiadas por capital de risco estão fornecendo serviços de “carteira” que facilitam para as pessoas a criação de contas para envio e recebimento de moedas digitais baseadas em *blockchain*, como o Bitcoin e o Ether. As trocas centralizadas também estão em desenvolvimento, permitindo que as pessoas convertam moeda digital em dólares, euros ou outras moedas fiduciárias. (tradução livre)

Entendemos que a regulação nesses intermediários específicos é acertada, pois estes conectam o usuário à rede. Sendo assim, essa ligação deve ser bem dirimida pela futura regulamentação, pois, como citamos anteriormente: a) documentos exigidos pelas *Exchanges*; b) Fechamento de *Exchanges* e a não garantia do valor depositado, e possíveis outras exigências e inseguranças, como, por exemplo, o fim de uma determinada “wallet”, podem ser solucionadas. Desse modo, regular alguns procedimentos e mecanismos das plataformas irá trazer mais segurança e confiabilidade para o mercado.

Nos Estados Unidos da América, no ano de 2013, por exemplo, foi exigido que as *Exchanges*, para funcionarem, deviam possuir uma licença e implementar um sistema de *compliance* que combatesse a lavagem de dinheiro.

In mid-2013, the U.S government provided a preliminary answer, issuing regulatory guidance informing digital currency exchanges that they could not lawfully operate in the United States if they failed to obtain necessary licenses and implement anti-money laundering (AML) compliance programs. (DE FILIPPI, p. 179)⁵⁷

A regulação desses intermediários específicos é acertada, contudo há um obstáculo de grande relevância neste assunto. Quando falamos dessas plataformas, elas não atuam somente em um determinado país, elas atuam globalmente, e, com isso, como regular? Criar cada país sua própria regulação? Ou criar uma regulação única? E a soberania dos Estados? Estas indagações ainda são complexas no âmbito das criptomoedas, pois precisam de um amadurecimento por parte dos reguladores, a fim de que haja respostas e soluções para estes questionamentos.

5.8.5 - Regulação de Mineradores

Uma possível regulação no âmbito dos mineradores entendemos ser bem-acertada, pois estes fornecem a sua força computacional, “mineram” os Bitcoins e as criptomoedas em geral e validam as transações na rede *Blockchain* do Bitcoin ou de outra criptomoeda. Desse modo, estes lucram ao produzirem (minerar) a criptomoeda, e também ao validarem as transações.

Blockchain rely on miners or other transaction processors to facilitate the transmission of digital currencies, the storage of data, and the execution of smart

⁵⁷ Em meados de 2013, o governo dos EUA forneceu uma resposta preliminar, emitindo orientação regulamentar informando que as *Exchanges* de moedas digitais, que elas não poderiam operar ilegalmente nos Estados Unidos se não conseguissem obter a licença necessária e implementasse um programa de *compliance* ante lavagem de dinheiro. (tradução livre)

contracts. These miners receive block rewards and fees for their efforts. (DE FILIPPI, p. 180)⁵⁸

Diante desta oportunidade de lucro, o que se tem observado, ao longo dos anos, é que há uma “centralização” dos mineradores, ou seja, está havendo a criação de “pools” de mineração, possibilitando haver monopólios de mineração. Atualmente, há quatro “pools” de mineração que controlam mais de cinquenta (50) por cento (%) da rede *Blockchain* do Bitcoin.

Over the last few years, mining on popular blockchain networks like Bitcoin and Ethereum has increasingly consolidated into large, centralized mining pools that aggregate the computational resources of multiple machines to increase the probability of receiving a block reward. Today, the degree of centralization is stark—four mining pools together control over 50 percent of the Bitcoin blockchain, and two mining pools combined control more than 50 percent of the Ethereum blockchain. These mining pools could work together or collude to fork a blockchain. (DE FILIPPI, p. 180)⁵⁹

Este máximo controle por parte de um grupo específico é algo que o regulador deve observar bem atentamente, pois isto influencia no bom funcionamento do mercado. Monopólios como estes no mercado financeiro tradicional é regulado, pois visa bloquear este excessivo controle e a conseqüente manipulação do mercado.

Como citado ao final da citação acima, de que esses *pools* de mineração podem trabalhar juntos ou colidirem em um *fork* da rede, e estas situações ocorrem, como explicamos em tópico específico, houve o *fork* da rede *Blockchain* do Bitcoin, originando duas novas criptomoedas: a Bitcoin Gold e a Bitcoin Cash. As possibilidades de *fork* é algo que o regulador deverá também observar com bastante cuidado.

Diante deste cenário de regulação do minerador e dos *pools* de mineração, é válido ressaltar que o Estado, os regulamentando, este tem o poder de influenciar na operação da rede *Blockchain*, bem como interferir diretamente nos procedimentos da rede, como, por exemplo, em caso de descumprimento da lei, os governos podem forçar os *pools* de mineração há implementarem protocolos específicos de mudança.

⁵⁸ *Blockchain* depende dos mineradores ou outros processadores de transações para facilitar a transmissão de moedas digitais, o armazenamento de dados e a execução de contratos inteligentes. Esses mineradores recebem recompensas de blocos e taxas por seus esforços. (tradução livre)

⁵⁹ Nos últimos anos, a mineração em redes populares de *Blockchain*, como Bitcoin e o Ethereum, se consolidaram cada vez mais em grandes e centralizados *pools* de mineração para aumentar a probabilidade de receber uma recompensa de bloco. Hoje, o grau de centralização é gritante, quatro *pools* de mineração em conjunto controlam 50% da *Blockchain* do Bitcoin, e dois *pools* de mineração juntos controlam mais de 50 por cento da *Blockchain* do Ethereum. Esses *pools* de mineração poderiam trabalhar em conjunto ou conspirarem para um *fork* da *Blockchain*. (tradução livre)

O Estado também pode interferir promovendo benefícios, aquelas plataformas que estão cumprindo com as determinações legais, ou taxar, ou penalizar os mineradores que processam transações ilegais.

Como observamos no tópico anterior, regular os mineradores e os *pools* de mineração também possuem o obstáculo de que atuam globalmente, e novamente questionamos: como regular?

Even if governments regulate the activity of miners in a handful of countries, these regulations could lack effectiveness because of a blockchain's global and decentralized nature. (DE FILIPPI, p. 181)⁶⁰

Sabemos que mudar uma rede *Blockchain* é necessário que haja um consenso na rede. Desse modo, uma regulação específica só de um país pode acarretar em uma ineficácia da lei, pois, caso grande parte dos mineradores não pertençam àquele país que regulou, a rede irá continuar funcionando sem modificações ou até haver um *fork*, não tendo, portanto, a regulamentação, nenhuma relevância e impacto.

Changing a blockchain's underlying protocol and operation requires that the network reach a consensus, and if a sufficient number of miners or mining pools reside in jurisdiction not affected by these regulations, the blockchain-based network could fork or continue to operate as if these regulation did not exist. (DE FILIPPI, p. 181)⁶¹

Uma outra preocupação é o fato de os mineradores não possuírem a capacidade de distinguirem quando uma transação é lícita ou ilícita, pois todas as operações dentro da rede *Blockchain* possuem o mesmo padrão. Os mineradores têm a capacidade de distinguirem quando uma transação está criptografada ou tecnicamente válida, contudo, para saberem se a transação é legal ou não, os mesmos precisam de mais informações, e estas somente podem ser informadas pelo Estado, por meio do ISP, ou de uma profunda inspeção.

Of equal concern is the fact that miners may be unable to differentiate between valid and invalid uses of a blockchain-based network, especially when the network facilitates both lawful and unlawful activity. Unlike an ISP, which can to some extent monitor traffic on the Internet by using techniques such as deep packet inspection, miners may lack the capability to identify lawful or unlawful transactions flowing through a blockchain-based network. While miners have the ability to discern whether a transaction is cryptographically or technically valid, they

⁶⁰ Mesmo que os governos regulem a atividade dos mineradores em vários países, essa regulação pode não ter eficácia por causa da natureza global e descentralizada da *Blockchain*. (tradução livre)

⁶¹ Mudar o protocolo e operações subjacentes de uma *Blockchain* requer que a rede chegue a um consenso, e se um número suficiente de mineiros ou *pools* de mineração residem em uma mesma jurisdição que não são afetados por essas regulações, poderiam realizar um *fork* ou continuar a operar como se essas regulamentações não existissem. (tradução livre)

may not be able to comprehend the purpose of such transactions without additional contextual information. (DE FILIPPI, p. 181)⁶²

Assim, regular os mineradores é uma proposição acertada, contudo há obstáculos a serem transpostos, principalmente no que diz respeito à atuação global destes, dificultando, portanto, qual forma de regulação adotar. Além do mais, a possível regulação não deve ter muita interferência do Estado, esta deve ser específica, pois, do contrário, irá perder-se o caráter descentralizado da rede *Blockchain*, e, com isso, todo o ideal de disrupção inerente a esta tecnologia.

5.8.6 - Regulação do Código Base

Sabemos que a rede *Blockchain* do Bitcoin tem como base o Código, uma proposição de regulação visa regulamentar esta parte fundamental, a essência da tecnologia *Blockchain*. Dessa forma, Estados perceberam que esta é uma poderosa ferramenta de imposição de regulação.

Code has long been recognized as powerful tool to enforce legal rules. Because technological systems like the Internet lack inherent natural properties attributable to physical spaces, they depend on code for their form and to shape the boundaries of what users can and cannot do. (DE FILIPPI, p. 181)⁶³

O Código é a base de qualquer tecnologia e aplicação. Desse modo, encontrar uma forma de regulá-lo seria uma grande vitória para o Estado, contudo esta deve também ser vista de uma forma específica, pois, do contrário, irá tirar completamente a liberdade dos desenvolvedores no processo de criação de novas aplicações e tecnologias, pois uma possível regulação irá interferir diretamente em como o sistema é usado e como este funciona.

Because blockchains rely on code to define their operation, governments could choose to regulate how developers create blockchain-based applications and smart

⁶² De igual preocupação é o fato de mineradores, talvez, podem ser incapazes de diferenciar entre usos válidos e inválidos de uma rede *Blockchain*, especialmente quando a rede facilita atividades lícitas e ilícitas. Ao contrário de um ISP, que pode até certo ponto monitorar o tráfego na internet usando técnicas, como a inspeção profunda de pacotes, os mineradores podem não ter a capacidade para identificar transações legais ou ilegais que fluem em uma rede *Blockchain*. Enquanto os mineradores têm a capacidade de discernir se a transação é criptograficamente ou tecnicamente válida, eles podem não ser capazes de compreender o objetivo de tais transações sem informação contextual. (tradução livre)

⁶³ O código há muito é reconhecido como uma ferramenta poderosa para impor regras legais. Porque sistemas tecnológicos, como a internet, carecem de recursos naturais atribuíveis a espaços físicos, eles dependem do código para a sua forma e moldar os limites do que os usuários podem e não podem fazer. (tradução livre)

contracts so as to influence how these systems are used and how these systems develop. (DE FILIPPI, p. 181)⁶⁴

O Estado interferindo de forma mais contundente pode exigir que sistemas possam ser implementados no Código a ser desenvolvido, a fim de que possa controlar de forma bem direta, podendo, por exemplo, desabilitar sistemas autônomos de *smart contracts* ou suspender a rede *Blockchain* que vá de encontro com os preceitos estatais.

For instance, new laws could mandate that software developers introduce specific features- such as a government backdoor-directly into a blockchain's underlying protocol, giving the government the power to disable autonomous smart contracts or suspend a blockchain-based application that fails to comply with the law. (DE FILIPPI, p. 181)⁶⁵

Esta interferência extrema do Estado no Código discordamos plenamente, pois o caráter de descentralização e de anonimidade será completamente mitigado, o que não é o objetivo dessa nova tecnologia. Portanto, defendemos a ideia de que a regulação estatal deva ser a mínima possível, a qual não comprometa o bom funcionamento das novas tecnologias. A regulação do código deve dirimir alguns aspectos específicos de utilização e criação, para que não haja nenhum formato de tecnologia ilegal, a ponto de prejudicar a rede e os usuários. Mas é válido ressaltar o obstáculo do alcance global do Código. Portanto, uma lei estipulada em um país pode não ser seguida no outro, e assim o Estado não pode forçar os sujeitos que implementam esse código a adotarem a regulação para além de suas fronteiras.

Even if governments require that blockchain developers introduce specific features into their code, they cannot force users or other private actors to adopt these features outside of their jurisdictional boundaries. If restrictions imposed by a government are too harsh, inefficient, or unfair, miners supporting a blockchain-based network could reject these rules, refusing to install software incorporating such rules or refusing to process transactions or smart contract code mandated by these laws. (DE FILIPPI, p. 183)⁶⁶

⁶⁴ Porque *Blockchains* dependem do código para definir sua operação, os governos poderiam optar por regulamentar como os desenvolvedores criam a *Blockchain* de aplicações e contratos inteligentes, de modo a influenciar a forma como estes sistemas são usados e como estes sistemas se desenvolvem. (tradução livre)

⁶⁵ Por exemplo, novas leis podem exigir que os desenvolvedores de software introduzam características específicas - como um *backdoor* do governo - diretamente de um protocolo subjacente ao *Blockchain*, dando ao governo o poder de desativar um contrato inteligente autônomo ou suspender uma aplicação *Blockchain* que não cumpra a lei. (tradução livre)

⁶⁶ Mesmo se os governos exigirem que os desenvolvedores de *Blockchain* introduzam características específicas em seu código, eles não podem forçar usuários ou outros atores a adotarem esses recursos fora de suas fronteiras jurisdicionais. Se as restrições impostas por um governo são muito duras, ineficientes ou injustas, mineradores que apoiam uma rede baseada em *Blockchain* poderiam rejeitar essas regras, recusando-se a instalar software, incorporando tais regras ou recusando-se a processar transações ou código de contrato inteligente mandatado por estas leis. (tradução livre)

Um outro obstáculo no que diz respeito à regulação do Código é o fato de que, dado o anonimato na rede *Blockchain*, para o Estado se torna um desafio ter de identificar os desenvolvedores do Código, e também há o desafio de os desenvolvedores não aderirem a ideia de se identificarem e registrarem o seu software na data-base do Estado. Com isso, não se pode haver a imposição do governo para aqueles que não fazem parte de sua jurisdição.

Um outro fator importante é com relação que, mesmo que tenha uma regulação em uma dada jurisdição, ainda assim pode-se usar técnicas de anonimato dentro do sistema *Blockchain*, não sendo, portanto, rastreável a sua verdadeira identidade.

Assim, percebemos que regular o Código não é uma tarefa fácil para as autoridades reguladoras, visto que trata-se de uma importante ferramenta da tecnologia *Blockchain*, a qual o seu formato objetiva manter o anonimato e a descentralização.

5.8.7 - Regulação de Hardware

Nesse formato de possível regulação de hardware, o Estado irá interferir nos equipamentos necessários ao funcionamento da rede *Blockchain*, ou seja, poderá implementar software de inspeção e controle naqueles em que utilizarem esses equipamentos para a conexão com a rede *Blockchain* e exigirem uma licença dos equipamentos antes que estes sejam lançados para venda no mercado.

Essa forma de regulação é, no mínimo, inapropriada, pois as empresas produtoras dos equipamentos seriam obrigadas a instalarem mecanismos de controle do Estado perante os seus cidadãos, permitindo ao governo saber de cada passo dado pelo utilizador dos equipamentos dentro da rede.

Introducing similar access control mechanisms into a blockchain-enabled device could reduce the benefits of relying on blockchain technology in the first place. Indeed, these would not only limit the distinctive features of the technology - in terms of autonomy, tamper resistance, and resiliency - but would also potentially make the technology more vulnerable to exploitation by both governmental and nongovernmental authorities. (DE FILIPPI, p. 184)⁶⁷

⁶⁷ Introduzindo mecanismos similares de controle de acesso dentro de um dispositivo ativado em uma rede *Blockchain* poderia reduzir os benefícios de confiar na tecnologia *Blockchain* em primeiro lugar. Com efeito, estes não só limitariam as características distintivas da tecnologia - em termos de autonomia, resistência à adulteração e resiliência -, mas também potencialmente poderia tornar a tecnologia mais vulnerável à exploração por autoridades governamentais e não governamentais. (tradução livre)

Regulando os hardwares, o governo irá ter controle de todas as ações dos usuários da rede, havendo, assim, uma centralização, o qual é o oposto do que é baseado a tecnologia *Blockchain*, que é a descentralização, o anonimato e a ideia de consensus.

5.8.8 - Regulação do Mercado que Utiliza o Sistema *Blockchain*

Nessa possibilidade de regulação do mercado que utiliza o sistema *Blockchain*, entendemos que é uma das possíveis regulações mais acertadas, visto que, como ocorre no mercado tradicional, há a regulação do mercado, não permitindo que este se autorregule. Dessa forma, voltando-se para o ambiente das criptomoedas, em especial o Bitcoin, tema deste trabalho, o Estado irá intervir no mercado, podendo influenciar no comportamento dos sujeitos que suportam, usam ou implementam aplicações na rede *Blockchain*.

Nesse formato, o Estado irá observar cada transação e seu custo, pois cada interação com a rede é uma transação econômica; e cada usuário, minerador, *Exchange*, ou seja, cada participante da rede é um sujeito econômico. Dessa forma, as características de regulação do mercado que utiliza o sistema *Blockchain* são muito parecidos com as características de regulação do mercado tradicional. Portanto, o Estado irá modificar uma dinâmica de mercado, o qual poderá afetar o comportamento na rede dos sujeitos participantes.

These characteristic make regulating a blockchain similar to regulating a traditional market. Just as a government can influence the price of goods or services to dissuade or encourage certain behaviors - as it does by taxing cigarettes or providing subsidies to the producers of certain goods - changing the market dynamics of a blockchain-based network could also affect the behavior of all parties relying on this shared network. (DE FILIPPI, p. 185)⁶⁸

Regulando o mercado que utiliza o sistema *Blockchain*, o Estado impacta em como os sujeitos interagem com a rede, e com isso explora a dinâmica do mercado e incentiva o sistema a respeitar a lei, tornando economicamente conveniente para os sujeitos participantes. Portanto, para que essa regulação seja efetiva, os governos devem ter a habilidade de mudarem a dinâmica do mercado do sistema *Blockchain*.

⁶⁸ Essas características fazem a regulação de uma Blockchain semelhante a regulação de um mercado tradicional. Assim como um governo pode influenciar o preço de bens ou serviços para dissuadir ou encorajar certos comportamentos - como faz taxando cigarros ou fornecendo subsídios aos produtores de certas mercadorias -, mudar a dinâmica do mercado de uma rede baseada em Blockchain também poderia afetar o comportamento de todas as partes que dependem dessa rede compartilhada. (tradução livre)

Um forma de atuarem na mudança da dinâmica do mercado do sistema *Blockchain*, a tarefa é um pouco difícil, seria a possibilidade de o Estado adquirir a maioria do poder de mineração da rede. Nesse caso, se o governo conseguir o maior controle no processamento de transações dentro da rede *Blockchain*, eles podem dar um passo bem significativo, que é o fato de implementarem protocolos de mudança na rede, o qual a afetaria economicamente e estruturalmente.

Governments also could influence the price of executing transactions on a blockchain by manipulating the value of the blockchain's native digital currency on the secondary market. (DE FILIPPI, p. 186)⁶⁹

Esta interferência do Estado ocorreria no mesmo formato quando estes manejam a economia para a proteger de uma inflação, ou quando os governos querem intervir na taxa de câmbio de diferentes moedas fiduciárias. Contudo, os governos não possuem a capacidade de participar de políticas monetárias tradicionais com um *Blockchain*, ou de inserir mais moeda no sistema, a fim de que possa estimular a inflação, portanto não poderá ocorrer interferência em um mercado aberto, comprando ou vendendo uma criptomoeda com o objetivo de aumentar ou diminuir o seu preço.

Atualmente, o que ocorre costumeiramente no mercado tradicional é o fato de o Estado buscar influenciar nas taxas de câmbio das diferentes moedas fiduciárias, os quais eles não têm controle, sem aumentar a inflação dentro de seus países, pois comprando e mantendo uma reserva de moeda estrangeira, o governo pode aumentar o valor da moeda estrangeira em relação a sua própria, fomentando o aumento da competitividade de suas exportações, objetivando reduzir a importação de bens de outros países. Tal ação, o Estado ainda se vê em uma esfera de incapacidade no que diz respeito ao mundo das criptomoedas, visto que tais manejos na economia de uma rede *blockchain* não seria possível fazê-los até o momento.

Havendo uma futura regulação no mercado das criptomoedas, ações tomadas pelo Estado, as quais citamos anteriormente, ou outras, aí sim poderiam ser efetivadas. Governos poderiam comprar ou manter reservas de criptomoedas, com isso teriam a possibilidade de aumentarem o preço de mercado da moeda, dessa forma aumentaria o custo de armazenamento de dados, executaria transações, ou implementaria, ou executaria o código de contratos inteligentes que são baseados em uma rede *Blockchain*, podendo assim, também,

⁶⁹ Os governos podem influenciar o preço da execução de transações em uma Blockchain manipulando o valor da moeda digital baseada em Blockchain no mercado secundário. (tradução livre)

influenciar até como os participantes da rede que interagem entre si, e, com isso, ao mesmo tempo, influenciariam na dinâmica do mercado da rede *Blockchain*.

Essas interferências do Estado tem o objetivo de influenciar o uso geral da tecnologia *Blockchain*, contudo, essa forma de abordagem poderia ser uma forma de os governos realizarem pressão sobre os mineradores ou aos outros sujeitos que apoiam, dão suporte à rede *Blockchain*, para que façam alterações no protocolo da rede. Um exemplo seria se os Estados aumentassem os custos das transações do Bitcoin; estes poderiam exercer uma pressão para que os sujeitos participantes fizessem alterações necessárias para interromper ou restringir atividades ilegais.

Indeed, if miners or other intermediaries knew that the government had such power, the threat of government intervention could, in and of itself, create a strong deterrent effect. The mere fact of knowing that a government could change the payoff structures related to the creation and deployment of blockchain based systems may ultimately shape the evolution of blockchain-based protocol and dissuade individuals from engaging in unlawful activity. (DE FILIPPI, p. 187)⁷⁰

Assim, os Estados com uma futura regulação do mercado que utiliza o sistema *Blockchain* podem criar estratégias de controle, as quais tem a possibilidade de mudar significativamente o objetivo da tecnologia. Esta regulação entendemos que deve ser realizada para que o mercado não se autorregule, o qual pode criar situações que fujam do controle e prejudiquem a rede de forma geral, mas esta regulação deve ser realizada de forma moderada, onde o Estado pode ter um controle, contudo, sem permitir que ocorra a perda da característica primordial da tecnologia *Blockchain*, que é a descentralização da rede, por isso que esta é distribuída.

5.8.9 - Regulação por Meio de Normas Sociais

Nessa sugestão de possível regulação da rede *Blockchain* por meio das normas sociais, esta é baseada na ideia de consenso da rede. Como os mineradores e os outros sujeitos que suportam a rede possuem a autoridade de promoverem “leis” dentro da rede, esses agentes atuam coletivamente em ações que influenciam no ecossistema da *Blockchain*.

⁷⁰ De fato, se mineradores ou outros intermediários soubessem que o governo tinha tal poder, a ameaça do governo poderia, em si, criar um forte efeito dissuasivo. O simples fato de saber que um governo poderia mudar as estruturas de pagamento relacionadas com a criação e desdobramento de um sistema baseado em Blockchain pode finalmente moldar a evolução do protocolo baseado em Blockchain e dissuadir os indivíduos de engajar-se em atividade ilegal. (tradução livre)

Blockchains rely on distributed consensus to operate, and therefore miners and other parties supporting these decentralized data structures have the authority to ensure the application of legal or community rules. In a sense, miners and other transaction processors act as judges, with the power to enforce the rules or values of a blockchain-based network. Network nodes can take action to halt unlawful activity when enough of them agree on a course of action. These parties can collectively decide to intervene to remedy a harm by implementing necessary changes to the protocol to censor or reverse particular transactions or unwind autonomous code. DE FILIPPI, p. 187)⁷¹

É válido ressaltar que o Bitcoin permanece com a sua característica de imutabilidade, a sua *Blockchain* não foi alterada, houveram *forks*, formando assim outra rede para o Bitcoin Cash e o Bitcoin Gold, mas a rede do Bitcoin permanece inalterada.

Assim, as autoridades reguladoras norteariam a sua regulação nas normas sociais, ou seja, nas normas presentes na rede pela sua comunidade, a fim de influenciar nas decisões da comunidade. Dessa forma, circundando-a poderia haver uma regulação indireta nas operações da rede.

⁷¹ *Blockchains* dependem de consenso distribuído para operar e, portanto, mineradores e outras partes que suportam estas estruturas de dados descentralizadas têm autoridade para garantir a aplicação de regras legais ou comunitárias. Em um sentido, os mineradores e outros processadores de transações atuam como juízes, com o poder para - impor regras ou valores de uma rede baseada em *Blockchain*. Nós da rede podem tomar medidas para interromper a atividade ilegal quando eles concordam em um curso de ação. Essas partes podem decidir coletivamente intervir para remediar um dano, implementando mudanças necessárias ao protocolo para censurar ou reverter determinadas transações ou desenrolar autônomo código. (tradução livre)

CONCLUSÃO

No século XXI, o qual o mundo está cada vez mais tecnológico, inúmeras inovações têm surgido em diversos setores. A Quarta Revolução Industrial, ou Revolução 4.0, trouxe à sociedade atual a oportunidade de reconhecer que o futuro será baseado na tecnologia, que a revolução digital é a mudança de paradigmas de nossos tempos modernos, onde sistemas ciberfísicos, internet das coisas e a inteligência artificial irão permitir a interação e a conectividade com os seres humanos, e as criptomoedas são uma realidade dessa revolução digital, pois estas vieram para desafiar o sistema financeiro tradicional.

Quando falamos em sistema financeiro tradicional, nos vêm logo a mente bolsa de valores, instituições financeiras, políticas econômicas do Estado, moedas fiduciárias, bancos centrais, ações, fundos de investimentos, *commodities*, controle centralizado. Foi a partir desse conjunto tradicionalista e centralizado do mercado financeiro mundial que, no ano de 2008, foi estabelecido a maior crise financeira global, após a Grande Depressão de 1929. As instituições financeiras, principalmente nos EUA, realizaram durante décadas uma configuração de investimentos tóxicos, que espalharam esses ativos para o mercado mundial, jamais visto na história financeira mundial. Em contrapartida, o Estado Liberal, que preconiza o Estado-mínimo, permitiu uma regulação ínfima sobre estas instituições financeiras. Sabe-se que esta forma de mercado está em um círculo vicioso, pois as instituições financeiras sempre buscam uma alternativa para ousarem e lucrarem cada vez mais. Nos EUA, há a expressão “muito grande para quebrar”, é baseado nesse pensamento que grandes bancos ousam em suas atividades, pois sabem que, se falharem, no final, o dinheiro do contribuinte irá ajudá-los, pois o Estado norte-americano não irá permitir que “quebrem”, que vão à falência, pois são instituições muito grandes e complexas, importantes para a economia nacional.

É nesse contexto de dependência do sistema financeiro tradicional por parte dos pequenos poupadores, que alavancou a concepção das criptomoedas, em especial o Bitcoin. Satoshi Nakamoto, em seu *white paper*, permitiu que o ideal libertário, que já vinha sendo desenvolvido há muito tempo, mas não havia chegado em uma definição concreta de sistema/código, fosse possível vir à tona e permitir uma disrupção no sistema financeiro.

As criptomoedas, sem dúvida, vieram para desafiar o sistema financeiro tradicional, permitindo a nós, o Povo, fazermos nossas próprias escolhas, sem depender de um poder centralizador, sem depender de um Estado ou instituição financeira.

A revolução digital, a qual está inserida as criptomoedas, é o futuro, e entendemos que estas devem andar em paralelo com o sistema financeiro tradicional, pois acreditamos que, em um futuro não muito longínquo, as criptomoedas serão mais aceitas e estarão mais presentes no cotidiano dos cidadãos nos quatro cantos do planeta.

É visando essa entrada mais eficiente das criptomoedas no mercado, que vindo para a nossa realidade brasileira, o Estado deve olhar para essa inovação tecnológica não como uma ameaça, e sim como um parceiro, para o desenvolvimento de sua economia, e, com isso, dever realizar uma regulação mínima, a fim de que não retire a característica primordial da tecnologia, que é a descentralização.

A regulação mínima do Estado deve propor guias no âmbito do procedimento e atividades dos intermediários que conectam os usuários à rede *Blockchain* do Bitcoin, e principalmente permitir aos usuários das criptomoedas garantias de que sua riqueza em criptomoeda não se evapore, visto que o Bitcoin entendemos ser um ativo com propriedades de moeda. Portanto, o Estado brasileiro deve propor uma forma de proteção, a fim de que, cada vez mais, a partir do livre arbítrio, mais cidadãos possam aderir ao mundo das criptomoedas.

Assim, finalizamos este trabalho com o ideal de que possamos transmitir um conhecimento a respeito do Bitcoin, e que essa criptomoeda possa fazer mudanças positivas no sistema financeiro, mas, fundamentalmente, que possa transformar a percepção do sistema financeiro e a realidade da maior quantidade de cidadãos, pois o Bitcoin não é só um ativo em si, é uma mudança de pensamento, de ações, de paradigmas, que pode profundamente mudar a realidade social e financeira de inúmeras pessoas ao redor do globo.

REFERÊNCIAS BIBLIOGRÁFICAS

BORGES, Ana Beatriz dos Santos. **Bitcoin: internet do dinheiro e o direito**. Revista de Direito Bancário e do Mercado de Capitais, vol. 81, ano 2. p. 119-139. São Paulo: Ed. RT, jul./set. 2018.

BRITO, Jerry. **The Law of Bitcoin**. Indiana: Universe, 2105.

CONWAY, Edward. **50 Ideias de Economia que Você Precisa Conhecer**. Tradução Marcello Borges, 1ª ed. São Paulo: Planeta, 2015.

DEROUSSEAU, Ryan. **The Everything Guide to Investing in Cryptocurrency**.

DE FILIPPI, Primavera e WRIGHT, Aaron. **Blockchain and the Law: The Rule of Code**. United States of America: Harvard University Press, 2018.

FILHO, Marçal Justen. **Curso de Direito Administrativo**, 9ª ed. rev., atual e ampl. São Paulo: Editora Revista dos Tribunais, 2013.

FINKELSTEIN, Maria Eugênia. **Manual de Direito Empresarial**, 8ª ed. rev., ampl. e ref. São Paulo: Atlas, 2016.

HOLANDA, Nilson. **Introdução à Economia: Da Teoria à Prática e Da Visão Micro à Macroperspectiva**, 8ª ed. rev. e ampl. Petrópolis, RJ: Vozes, 2002.

[REVOLUÇÃO]. Disponível em: <https://www.significados.com.br/revolucao/>. Acesso em 05/06/2019.

[LIBERALISMO ECONÔMICO]. Disponível em: <https://www.todamateria.com.br/liberalismo-economico/>. Acesso em 20/06/2019.

[PROVA DE TRABALHO]. Disponível em: https://pt.wikipedia.org/wiki/Prova_de_trabalho. Acesso em 02/07/2019.

[PROJETO DE LEI]. Disponível em: <https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/especiais/55a-legislatura/banco-central-regular-moedas-virtuais>. Acesso em 21/07/2019.

[INSTRUÇÃO NORMATIVA]. Disponível em: <http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?visao=anotado&idAto=10059>. Acesso em 21/07/2019.

[COMUNICADO BANCO CENTRAL]. Disponível em: <https://www3.bcb.gov.br/normativo/detalharNormativo.do?method=detalharNormativo&N=14009277>. Acesso em 21/07/2019.

[COMUNICADO BANCO CENTRAL]. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=comunicado&numero=31379>. Acesso em 21/07/2019.

[NOTA DA CVM]. Disponível em: <http://www.cvm.gov.br/noticias/arquivos/2017/20171011-1.html>. Acesso em 21/07/2019.

[NOTA DA CVM]. Disponível em: <http://www.cvm.gov.br/noticias/arquivos/2017/20171116-1.html>. Acesso em 21/07/2019.

[NOTA DA CVM]. Disponível em: <http://www.cvm.gov.br/noticias/arquivos/2018/20180307-1.html>. Acesso em 21/07/2019.

[4ª REVOLUÇÃO INDUSTRIAL]. Disponível em: <https://www.bbc.com/portuguese/geral-37658309>. Acesso em 16/08/2019.

HUBERMAN, Leo. **História da Riqueza do Homem**. Tradução de Waltensir Dutra. Atualização e revisão técnica: Marcia Guerra, 22ª ed. rev. e ampl., reimpr. Rio de Janeiro: LTC, 2017.

LOBO, Carlos Augusto da Silveira. **Os Valores Mobiliários**. Revista dos Tribunais, vol. 36/2007, p. 27-42, abr./jun. 2007.

LOPES, João do Carmo. **Economia Monetária**/João do Carmo Lopes, José Paschoal Rosetti, 6ª ed. rev., ampl. e atual.- São Paulo: Atlas, 1996.

MCMILLAN, Jonathan. **O Fim dos Bancos: Moeda, Crédito e a Revolução Digital**. Tradução: Afonso Celso da Cunha Serra, 1ª ed. São Paulo: Portifolio-Penguin, 2018.

MEIRELES, Edilton, SILVEIRA, Everton Caldas, FILHO, Ruy Nestor Bastos Mello. **A Natureza Jurídica do Bitcoin no Sistema Legal Brasileiro**. Revista dos Tribunais, vol. 1004/2019, p. 147-167, jun./2019; e Revista dos Tribunais, vol. 1007/2019, p. 371-392, set./2019.

Disponível em: <https://www.revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0ad82d9a0000016cc5514db040977227&docguid=I52cf6e407d1211e9a116010000000000&hitguid=I52cf6e407d1211e9a116010000000000&spos=3&epos=3&td=5&context=27&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1>. Acesso em 24/08/2019.

NAKAMOTO, Satoshi. **Bitcoin: A peer-to-peer Electronic Cash System.**

Trad. Daniel
Ribeiro

NAJJARIAN, Ilene Patrícia de Noronha. **Fintech: Novo Desafio Regulatório.** Revista dos Tribunais, vol. 74/2016, p. 33-49, out/dez. 2016.

ORDONNEAU, Pascal. **Monnaies Cryptées et Blockchain : La Confiance Est-elle un Algorithme?.** Paris: Franel Éditions, 2017.

PERASSO, Valeria. **O Que é a 4ª Revolução Industrial - E Como Deve Afetar Nossas Vidas,** 2016. Disponível em: <https://www.bbc.com/portuguese/geral-37658309>. Acesso em 16/08/2019.

ROVAI, Armando Luiz. **Atualidades do Direito Empresarial Brasileiro.** Belo Horizonte: D'Plácido, 2019.

SCHWAB, Klaus. **A Quarta Revolução Industrial.** Tradução Daniel Moreira Miranda. São Paulo: Edipro, 2016.

SCHUMPETER, Joseph A. **Fundamentos do Pensamento Econômico.** Rio de Janeiro: Zahar Editores, 1968.

SMITH, Adam. **A Riqueza das Nações: Uma investigação sobre a natureza e as causas da riqueza das nações/Adam Smith.** Tradução Getulio Schanoski Jr. São Paulo: Madras, 2018.

STANLAKE, George Frederik. **Introdução à Economia**. Lisboa: Fundação Calouste Gulbenkian, 1993

STONIER, Alfred e Hague, Douglas. **Teoria Econômica**. Tradução Cássio Fonseca. Rio de Janeiro: Zahar Editora, 1970.

SUKAMULJA, Sukmawati e Sikora, Cornelia Olivia. **The New Era of Financial Innovation: The determinants of bitcoin's price**. Journal of Indonesian Economy and Business, vol. 33, nº 1, 2018, 46-64.

ULRICH, Fernando. **Bitcoin - A Moeda na Era Digital**. São Paulo: Instituto Ludwig von Mises Brasil, 2014.

VIGNA, Paul e CASEY, Michael J. **The Age of Cryptocurrency: how bitcoin and digital money are challenging the global economic order**. Nova York: St. Martins Press, 2015.

WATSON, Thomas. **The Real Value of Bitcoin**. Ivey Business Journal: Improving Practice of Management. Canadá. jan./feb. 2018.

WHITE PAPER, **An introduction to Libra**.

WONACOTT, Paul e WONACOTT, Ronald. **Introdução à Economia**. Coordenadores da edição em português: Yeda Rorato Crusius & Carlos Augusto Crusius. Tradução, revisão e adaptação: Nuno Renan Lopes de Figueiredo Pinto *et al.* São Paulo: McGraw-Hill do Brasil, 1985.

ANEXO I

OS OITO DE OURO

Transformação da Blockchain no Sistema Financeiro

FUNÇÕES	IMPACTO DA BLOCKCHAIN	PARTES INTERESSADAS
1. Autenticando a identidade e valor.	Identidades verificáveis e robustas identidades protegidas criptograficamente.	Agências de rating, análise de dados do consumidor, marketing, banco de varejo, redes de cartões de pagamento, reguladores.
2. Movendo o valor - faça um pagamento, uma transferência de dinheiro, e compre bens e serviços.	Transferência de valor em incrementos muito grandes e muito pequenos sem intermediários reduzirá drasticamente o custo e a velocidade dos pagamentos.	Bancos de varejo, banco de atacado, rede de cartões de pagamento, serviços de transferência de dinheiro, telecomunicações, reguladores.
3. Valor de armazenamento - moedas, commodities, e ativos financeiros são lojas de valor. Cofre, poupança, ou uma conta de verificação. Fundos do mercado monetário ou Título do Tesouro.	Mecanismo de pagamento combinado com uma loja confiável e segura de valor reduz a necessidade de típicos serviços financeiros; poupanças bancárias e contas-correntes vão se tornar obsoletas.	Banco de varejo, corretoras, investimento bancário, gestão de ativos, telecomunicações, reguladores.
4. Valor do Empréstimo - débito do cartão de crédito, hipotecas, títulos municipais, títulos do governo, títulos lastreados em ativos e outras formas de crédito.	A dívida pode ser emitida, negociada e estabelecida na blockchain; aumenta a eficiência, reduz o atrito, melhora o risco sistêmico. Os consumidores podem usar a reputação para acessar empréstimos de pares; significativo para o mundo sem banco e para empreendedores.	Atacado, banco comercial e de varejo, finanças públicas (finanças do governo), microempréstimo, crowdfunding, reguladores, agências de notação de crédito, empresas de software de pontuação de crédito.
5. Troca de Valor - especulação, cobertura e arbitragem. Ordens correspondentes, operações de compensações, gestão de garantias, liquidação de valorização e custódia.	Blockchain leva tempos de liquidação em todas as transações de dias e semanas para minutos e segundos. Esta velocidade e eficiência também cria oportunidades para os não bancarizados e sub-bancários para participar na criação de riqueza.	Investimento, banco de atacado, comerciantes de câmbio, fundos de hedge, fundos de pensão, corretagem de varejo, câmaras de compensação, bolsa, futuros, troca de commodities; corretagem de commodities, bancos centrais, reguladores.
6. Financiamento e Investimento em um Ativo, Companhia ou Start-up - valorização do capital, dividendos, interesse, aluguéis, ou alguma combinação.	Novos modelos de financiamento peer-to-peer, registro de ações corporativas, como dividendos pagos automaticamente por meio de contratos inteligentes. Títulos de registro para autorizar reivindicações de renda e outras formas de rendimento.	Investimento bancário, venture capital, legal, auditoria, gestão de propriedade, bolsa de valores, crowdfunding, reguladores.
7. Assegurando valor e gerenciando riscos - proteger ativos, casas, vidas, saúde, propriedade de negócio, produtos derivados.	Utilizando sistemas de reputação, assegura-se uma melhor estimativa do risco atuarial, criando mercados descentralizados para o seguro. Derivativos mais transparentes.	Seguro, gerenciamento de riscos, banco de atacado, corretagem, câmaras de compensação, reguladores.
8. Contabilizando o valor - nova	O livro-razão distribuído tornará	Auditoria, gestão de ativos,

governança corporativa.	o relatório de auditoria e financeiro em tempo real, ágil e transparente, melhorará drasticamente a capacidade dos reguladores de examinar as ações financeiras dentro de uma corporação.	guardiões dos acionistas, reguladores.
-------------------------	---	--

ANEXO II: INSTRUÇÃO NORMATIVA RFB Nº 1888, de 03 DE MAIO DE 2019.

INSTRUÇÃO NORMATIVA RFB Nº 1888, DE 03 DE MAIO DE 2019

(Publicado(a) no DOU de 07/05/2019, seção 1, página 14)

Institui e disciplina a obrigatoriedade de prestação de informações relativas às operações realizadas com criptoativos à Secretaria Especial da Receita Federal do Brasil (RFB).

Histórico de alterações

(Alterado(a) pelo(a) Instrução Normativa RFB nº 1899, de 10 de julho de 2019).

O SECRETÁRIO ESPECIAL DA RECEITA FEDERAL DO BRASIL, no uso da atribuição que lhe confere o inciso III do art. 327 do Regimento Interno da Secretaria Especial da Receita Federal do Brasil, aprovado pela Portaria MF nº 430, de 9 de outubro de 2017, e tendo em vista o disposto no art. 113 da Lei nº 5.172, de 25 de outubro de 1966, no art. 16 da Lei nº 9.779, de 19 de janeiro de 1999, e no art. 57 da Medida Provisória nº 2.158-35, de 24 de agosto de 2001, resolve:

CAPÍTULO I DISPOSIÇÕES GERAIS

Art. 1º Esta Instrução Normativa institui e disciplina a obrigatoriedade de prestação de informações relativas às operações realizadas com criptoativos à Secretaria Especial da Receita Federal do Brasil (RFB).

Art. 2º As informações a que se refere o art. 1º deverão ser prestadas com a utilização do sistema Coleta Nacional, disponibilizado por meio do Centro Virtual de Atendimento (e-CAC) da RFB, em leiaute a ser definido em Ato Declaratório Executivo (ADE) da Coordenação-Geral de Programação e Estudos (Copes), a ser publicado no prazo de até 60 (sessenta) dias, contado a partir da data de publicação desta Instrução Normativa.

Parágrafo Único. A Copes deverá também editar e divulgar o manual de orientação do sistema Coleta Nacional no prazo a que se refere o caput.

~~Art. 3º O conjunto de informações enviado de forma eletrônica deverá ser assinado digitalmente pela pessoa física, pelo representante legal da pessoa jurídica ou pelo procurador, constituído nos termos da Instrução Normativa RFB nº 1.751, de 16 de outubro de 2017, mediante o uso de certificado digital válido, emitido por entidade credenciada pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).~~

Art. 3º O conjunto de informações enviado de forma eletrônica deverá ser assinado digitalmente mediante o uso de certificado digital válido, emitido por entidade credenciada pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), sempre que for exigido no portal e-CAC da RFB. (Redação dada pelo(a) Instrução Normativa RFB nº 1899, de 10 de julho de 2019)

Art. 4º Para os efeitos desta Instrução Normativa e para fins de conversão de valores em Reais, o valor expresso em moeda estrangeira deve ser convertido:

I - em dólar dos Estados Unidos da América; e

II - em moeda nacional.

Parágrafo Único. A conversão de que trata o caput será feita pela cotação do dólar dos Estados Unidos da América fixada, para venda, pelo Banco Central do Brasil (BCB) para a data da operação ou saldo, extraída do boletim de fechamento PTAX divulgado pelo BCB.

CAPÍTULO II DAS DEFINIÇÕES

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.

CAPÍTULO III

DA OBRIGATORIEDADE DE PRESTAÇÃO DE 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.

§ 1º No caso previsto no inciso II do caput, as informações deverão ser prestadas sempre que o valor mensal das operações, isolado ou conjuntamente, ultrapassar R\$ 30.000,00 (trinta mil reais).

§ 2º A obrigatoriedade de prestar informações aplica-se à pessoa física ou jurídica que realizar quaisquer das operações com criptoativos relacionadas a seguir:

I - compra e venda;

II - permuta;

III - doação;

IV - transferência de criptoativo para a Exchange;

V - retirada de criptoativo da Exchange;

VI - cessão temporária (aluguel);

VII - dação em pagamento;

VIII - emissão; e

IX - outras operações que impliquem em transferência de criptoativos.

CAPÍTULO IV

DAS INFORMAÇÕES SOBRE OPERAÇÕES COM CRIPTOATIVOS

Art. 7º Deverão ser informados para cada operação:

I - nos casos previstos no inciso I e na alínea “b” do inciso II do caput do art. 6º:

a) a data da operação;

b) o tipo da operação, conforme o § 2º do art. 6º;

c) os titulares da operação;

d) os criptoativos usados na operação;

e) a quantidade de criptoativos negociados, em unidades, até a décima casa decimal;

f) o valor da operação, em reais, excluídas as taxas de serviço cobradas para a execução da operação, quando houver;

g) o valor das taxas de serviços cobradas para a execução da operação, em reais, quando houver; e

~~h) o endereço da wallet de remessa e de recebimento, se houver; e (Revogado(a) pelo(a) Instrução Normativa RFB nº 1899, de 10 de julho de 2019)~~

II - no caso previsto na alínea “a” do inciso II do art. 6º:

a) a identificação da Exchange;

b) a data da operação;

c) o tipo de operação, conforme o § 2º do art. 6º;

d) os criptoativos usados na operação;

e) a quantidade de criptoativos negociados, em unidades, até a décima casa decimal;

f) o valor da operação, em reais, excluídas as taxas de serviço cobradas para a execução da operação, quando houver;

g) o valor das taxas de serviços cobradas para a execução da operação, em reais, quando houver; e

~~h) o endereço da wallet de remessa e de recebimento, se houver. (Revogado(a) pelo(a) Instrução Normativa RFB nº 1899, de 10 de julho de 2019)~~

~~Parágrafo único. Das informações a que se refere este artigo devem constar a identificação dos titulares das operações e incluir nome, nacionalidade, domicílio fiscal, endereço, número de inscrição no Cadastro de Pessoas Físicas (CPF) ou no~~

~~Cadastro Nacional da Pessoa Jurídica (CNPJ) ou Número de Identificação Fiscal (NIF) no exterior, quando houver, nome empresarial e demais informações cadastrais.~~

§ 1º Em relação aos titulares da operação, devem constar das informações a que se refere este artigo: (Redação dada pelo(a) Instrução Normativa RFB nº 1899, de 10 de julho de 2019)

I - o nome da pessoa física ou jurídica; (Incluído(a) pelo(a) Instrução Normativa RFB nº 1899, de 10 de julho de 2019)

II - o endereço; (Incluído(a) pelo(a) Instrução Normativa RFB nº 1899, de 10 de julho de 2019)

III - o domicílio fiscal; (Incluído(a) pelo(a) Instrução Normativa RFB nº 1899, de 10 de julho de 2019)

IV - o número de inscrição no Cadastro de Pessoas Físicas (CPF) ou no Cadastro Nacional da Pessoa Jurídica (CNPJ), conforme o caso, ou o Número de Identificação Fiscal (NIF) no exterior, quando houver, no caso de residentes ou domiciliados no exterior; e (Incluído(a) pelo(a) Instrução Normativa RFB nº 1899, de 10 de julho de 2019)

V - as demais informações cadastrais. (Incluído(a) pelo(a) Instrução Normativa RFB nº 1899, de 10 de julho de 2019)

§ 2º Caso os titulares das operações sejam residentes ou domiciliados no Brasil, a prestação da informação relativa ao número de inscrição no CPF ou no CNPJ, conforme o caso, é obrigatória a partir da data da entrega do primeiro conjunto de informações, prevista no § 1º do art. 8º. (Incluído(a) pelo(a) Instrução Normativa RFB nº 1899, de 10 de julho de 2019)

§ 3º Caso os titulares das operações sejam residentes ou domiciliados no exterior, a prestação das informações relativas ao país do domicílio fiscal, endereço e NIF no exterior é obrigatória a partir da entrega de informações a ser efetuada em janeiro de 2020, referentes às operações realizadas em dezembro de 2019. (Incluído(a) pelo(a) Instrução Normativa RFB nº 1899, de 10 de julho de 2019)

§ 4º A entrega das informações relativas ao endereço da wallet de remessa e de recebimento, se houver, é obrigatória apenas na hipótese de recebimento de intimação efetuada no curso de procedimento fiscal. (Incluído(a) pelo(a) Instrução Normativa RFB nº 1899, de 10 de julho de 2019)

CAPÍTULO V

DO PRAZO PARA PRESTAÇÃO DAS INFORMAÇÕES

Art. 8º As informações deverão ser transmitidas à RFB mensalmente até as 23h59min59s (vinte e três horas, cinquenta e nove minutos e cinquenta e nove segundos), horário de Brasília, do último dia útil do:

I - mês-calendário subsequente àquele em que ocorreu o conjunto de operações realizadas com criptoativos, quanto às obrigações previstas no art. 7º;

II - mês de janeiro do ano-calendário subsequente, quanto à obrigação prevista no art. 9º.

§ 1º O primeiro conjunto de informações a ser entregue em setembro de 2019 será referente às operações realizadas em agosto de 2019.

§ 2º A transmissão das informações não dispensa o declarante da obrigação de guardar os documentos e manter os sistemas de onde elas foram extraídas.

Art. 9º A Exchange de criptoativos domiciliada para fins tributários no Brasil a que se refere o inciso I do caput do art. 6º deverá prestar também, relativamente a cada usuário de seus serviços, as seguintes informações relativas a 31 de dezembro de cada ano:

I - o saldo de moedas fiduciárias, em reais;

II - o saldo de cada espécie de criptoativos, em unidade dos respectivos criptoativos; e

III - o custo, em reais, de obtenção de cada espécie de criptoativo, declarado pelo usuário de seus serviços, se houver.

Parágrafo único. As informações de que trata este artigo deverão ser incluídas no conjunto de informações prestadas nos termos do art. 7º.

CAPÍTULO VI DAS PENALIDADES

Art. 10. A pessoa física ou jurídica que deixar de prestar as informações a que estiver obrigada, nos termos do art. 6º, ou que prestá-las fora dos prazos fixados no art. 8º, ou que omitir informações ou prestar informações inexatas, incompletas ou incorretas, ficará sujeita às seguintes multas, conforme o caso:

I - pela prestação extemporânea:

a) R\$ 500,00 (quinhentos reais) por mês ou fração de mês, se o declarante for pessoa jurídica em início de atividade, imune ou isenta, optante pelo Regime Especial Unificado de Arrecadação de Tributos e Contribuições devidos pelas Microempresas e Empresas de Pequeno Porte (Simples Nacional), instituído pela Lei Complementar nº 123, de 14 de dezembro de 2006, ou que na última declaração apresentada tenha apurado o Imposto sobre a Renda da Pessoa Jurídica (IRPJ) com base no lucro presumido;

b) R\$ 1.500,00 (mil e quinhentos reais) por mês ou fração de mês, se o declarante for pessoa jurídica não incluída na alínea “a”; ou

c) R\$ 100,00 (cem reais) por mês ou fração, se pessoa física;

II - pela prestação com informações inexatas, incompletas ou incorretas ou com omissão de informação:

a) 3% (três por cento) do valor da operação a que se refere a informação omitida, inexata, incorreta ou incompleta, não inferior a R\$ 100,00 (cem reais), se o declarante for pessoa jurídica; ou

b) 1,5% (um inteiro e cinco décimos por cento) do valor da operação a que se refere a informação omitida, inexata, incorreta ou incompleta, se o declarante for pessoa física; e

III - pelo não cumprimento à intimação da RFB para cumprir obrigação acessória ou para prestar esclarecimentos nos prazos estipulados pela autoridade fiscal, o valor de R\$ 500,00 (quinhentos reais) por mês-calendário;

§ 1º A multa prevista na alínea “a” do inciso II do caput será reduzida em 70% (setenta por cento) se o declarante for pessoa jurídica optante pelo Simples Nacional.

§ 2º A multa prevista na alínea “b” do inciso I do caput será aplicada também, em caso de apresentação das informações fora do prazo previsto no art. 8º, à pessoa jurídica que na última declaração tenha utilizado mais de uma forma de apuração do lucro ou tenha realizado operação de reorganização societária.

§ 3º A multa prevista no inciso I do caput será reduzida à metade nos casos em que a obrigação acessória for cumprida antes de qualquer procedimento de ofício.

Art. 11. Sem prejuízo da aplicação da multa prevista no inciso II do caput do art. 10, poderá ser formalizada comunicação ao Ministério Público Federal, quando houver indícios da ocorrência dos crimes previstos no art. 1º da Lei nº 9.613, de 3 de março de 1998.

CAPÍTULO VII DA RETIFICAÇÃO DAS INFORMAÇÕES

Art. 12. Caso a pessoa física ou jurídica constate que as informações prestadas contêm erros, inexatidões ou omissões, poderá corrigi-los ou supri-las, conforme o caso, mediante apresentação de retificação, observado o disposto nos arts. 2º e 3º.

Parágrafo Único. Não incidirá multa relativamente aos erros, inexatidões e omissões a que se refere o caput, desde que sejam corrigidos ou supridas antes de iniciado qualquer procedimento de ofício.

CAPÍTULO VIII DISPOSIÇÕES FINAIS

Art. 13. Esta Instrução Normativa entra em vigor na data de sua publicação no Diário Oficial da União e produz efeitos a partir de 1º de agosto de 2019.

MARCOS CINTRA CAVALCANTI DE ALBUQUERQUE

*Este texto não substitui o publicado oficialmente.

ANEXO III: COMUNICADOS DO BANCO CENTRAL

COMUNICADO Nº 25.306, DE 19 DE FEVEREIRO DE 2014

Esclarece sobre os riscos decorrentes da aquisição das chamadas "moedas virtuais" ou "moedas criptografadas" e da realização de transações com elas.

O Banco Central do Brasil esclarece, inicialmente, que as chamadas moedas virtuais não se confundem com a “moeda eletrônica” de que tratam a Lei nº 12.865, de 9 de outubro de 2013, e sua regulamentação infralegal. Moedas eletrônicas, conforme disciplinadas por esses atos normativos, são recursos armazenados em dispositivo ou sistema eletrônico que permitem ao usuário final efetuar transação de pagamento denominada em moeda nacional. Por sua vez, as chamadas moedas virtuais possuem forma própria de denominação, ou seja, são denominadas em unidade de conta distinta das moedas emitidas por governos soberanos, e não se caracterizam dispositivo ou sistema eletrônico para armazenamento em reais.

2. A utilização das chamadas moedas virtuais e a incidência, sobre elas, de normas aplicáveis aos sistemas financeiro e de pagamentos têm sido temas de debate internacional e de manifestações de autoridades monetárias e de outras autoridades públicas, com poucas conclusões até o momento.

3. As chamadas moedas virtuais não são emitidas nem garantidas por uma autoridade monetária. Algumas são emitidas e intermediadas por entidades não financeiras e outras não têm sequer uma entidade responsável por sua emissão. Em ambos os casos, as entidades e pessoas que emitem ou fazem a intermediação desses ativos virtuais não são reguladas nem supervisionadas por autoridades monetárias de qualquer país.

4. Essas chamadas moedas virtuais não têm garantia de conversão para a moeda oficial, tampouco são garantidos por ativo real de qualquer espécie. O valor de conversão de um ativo conhecido como moeda virtual para moedas emitidas por autoridades monetárias depende da credibilidade e da confiança que os agentes de mercado possuam na aceitação da chamada moeda virtual como meio de troca e das expectativas de sua valorização. Não há, portanto, nenhum mecanismo governamental que garanta o valor em moeda oficial dos instrumentos conhecidos como moedas virtuais, ficando todo o risco de sua aceitação nas mãos dos usuários.

5. Em função do baixo volume de transações, de sua baixa aceitação como meio de troca e da falta de percepção clara sobre sua fidedignidade, a variação dos preços das chamadas moedas virtuais pode ser muito grande e rápida, podendo até mesmo levar à perda total de seu valor.

6. Na mesma linha, a eventual aplicação, por autoridades monetárias de quaisquer países, de medidas prudenciais, coercitivas ou punitivas sobre o uso desses ativos, pode afetar significativamente o preço de tais moedas ou mesmo a capacidade de sua negociação.

7. Além disso, esses instrumentos virtuais podem ser utilizados em atividades ilícitas, o que pode dar ensejo a investigações conduzidas pelas autoridades públicas. Dessa forma, o usuário desses ativos virtuais, ainda que realize transações de boa-fé, pode se ver envolvido nas referidas investigações.

8. Por fim, o armazenamento das chamadas moedas virtuais nas denominadas carteiras eletrônicas apresenta o risco de que o detentor desses ativos sofra perdas patrimoniais decorrentes de ataques de criminosos que atuam no espaço da rede mundial de computadores.

9. No Brasil, embora o uso das chamadas moedas virtuais ainda não se tenha mostrado capaz de oferecer riscos ao Sistema Financeiro Nacional, particularmente às transações de pagamentos de varejo (art. 6º, § 4º, da Lei nº 12.685/2013), o Banco Central do Brasil está acompanhando a evolução da utilização de tais instrumentos e as discussões nos foros internacionais sobre a matéria – em especial sobre sua natureza, propriedade e funcionamento –, para fins de adoção de eventuais medidas no âmbito de sua competência legal, se for o caso.

Aldo Luiz Mendes
Diretor de Política Monetária

Luiz Edson Feltrim
Diretor de Regulação, substituto

COMUNICADO Nº 31.379, DE 16 DE NOVEMBRO DE 2017

Alerta sobre os riscos decorrentes de operações de guarda e negociação das denominadas moedas virtuais.

Considerando o crescente interesse dos agentes econômicos (sociedade e instituições) nas denominadas moedas virtuais, o Banco Central do Brasil alerta que estas não são emitidas nem garantidas por qualquer autoridade monetária, por isso não têm garantia de conversão para moedas soberanas, e tampouco são lastreadas em ativo real de qualquer espécie, ficando todo o risco com os detentores. Seu valor decorre exclusivamente da confiança conferida pelos indivíduos ao seu emissor.

2. A compra e a guarda das denominadas moedas virtuais com finalidade especulativa estão sujeitas a riscos imponderáveis, incluindo, nesse caso, a possibilidade de perda de todo o capital investido, além da típica variação de seu preço. O armazenamento das moedas virtuais também apresenta o risco de o detentor desses ativos sofrer perdas patrimoniais.

3. Destaca-se que as moedas virtuais, se utilizadas em atividades ilícitas, podem expor seus detentores a investigações conduzidas pelas autoridades públicas visando a apurar as responsabilidades penais e administrativas.

4. As empresas que negociam ou guardam as chamadas moedas virtuais em nome dos usuários, pessoas naturais ou jurídicas, não são reguladas, autorizadas ou supervisionadas pelo Banco Central do Brasil. Não há, no arcabouço legal e regulatório relacionado com o Sistema Financeiro Nacional, dispositivo específico sobre moedas virtuais. O Banco Central do Brasil, particularmente, não regula nem supervisiona operações com moedas virtuais.

5. A denominada moeda virtual não se confunde com a definição de moeda eletrônica de que trata a Lei nº 12.865, de 9 de outubro de 2013, e sua regulamentação por meio de atos normativos editados pelo Banco Central do Brasil, conforme diretrizes do Conselho Monetário Nacional. Nos termos da definição constante nesse arcabouço regulatório consideram-se moeda eletrônica “os recursos em reais armazenados em dispositivo ou sistema eletrônico que permitem ao usuário final efetuar transação de pagamento”. Moeda eletrônica, portanto, é um modo de expressão de créditos denominados em reais. Por sua vez, as chamadas moedas virtuais não são referenciadas em reais ou em outras moedas estabelecidas por governos soberanos.

6. É importante ressaltar que as operações com moedas virtuais e com outros instrumentos conexos que impliquem transferências internacionais referenciadas em moedas estrangeiras não afastam a obrigatoriedade de se observar as normas cambiais, em especial a realização de transações exclusivamente por meio de instituições autorizadas pelo Banco Central do Brasil a operar no mercado de câmbio.

7. Embora as moedas virtuais tenham sido tema de debate internacional e de manifestações de autoridades monetárias e de outras autoridades públicas, não foi identificada, até a presente data, pelos organismos internacionais, a necessidade de regulamentação desses ativos. No Brasil, por enquanto, não se observam riscos relevantes para o Sistema Financeiro Nacional. Contudo, o Banco Central do Brasil permanece atento à evolução do uso das moedas virtuais, bem como acompanha as discussões nos foros internacionais sobre a matéria para fins de adoção de eventuais medidas, se for o caso, observadas as atribuições dos órgãos e das entidades competentes.

8. Por fim, o Banco Central do Brasil afirma seu compromisso de apoiar as inovações financeiras, inclusive as baseadas em novas tecnologias que tornem o sistema financeiro mais seguro e eficiente.

Otávio Ribeiro Damaso
Diretor de Regulação

Reinaldo Le Grazie
Diretor de Política Monetária

ANEXO IV- NOTAS DA COMISSÃO DE VALORES MOBILIÁRIOS

Notícias

11/10/2017

Initial Coin Offering (ICO)

Nota da CVM a respeito do tema

Considerando o avanço das operações conhecidas como *Initial Coin Offerings* (ICOs), a CVM julga pertinente esclarecer que está atenta às recentes inovações tecnológicas nos mercados financeiros global e brasileiro. A Autarquia vem acompanhando tais operações e buscando compreender benefícios e riscos associados, seja por meio de fóruns internos, como o Comitê de Gestão de Riscos – CGR e o Fintech Hub, ou de discussões no âmbito internacional, como em trabalhos desenvolvidos pela IOSCO.

Em linha com as competências definidas na Lei 6.385/76, a CVM busca estimular o empreendedorismo e a introdução de inovações tecnológicas no mercado de valores mobiliários, sempre que alinhados ao norte da segurança dos investidores e da integridade do mercado.

Assim, a Autarquia presta os seguintes esclarecimentos quanto aos riscos decorrentes dos chamados ICOs e de sua relação com o regime regulatório atualmente vigente no âmbito do mercado de valores mobiliários:

1. Podem-se compreender os ICOs como captações públicas de recursos, tendo como contrapartida a emissão de ativos virtuais, também conhecidos como *tokens* ou *coins*, junto ao público investidor. Tais ativos virtuais, por sua vez, a depender do contexto econômico de sua emissão e dos direitos conferidos aos investidores, podem representar valores mobiliários, nos termos do art. 2º, da Lei 6.385/76.
2. Nesse contexto, a CVM esclarece que certas operações de ICO podem se caracterizar como operações com valores mobiliários já sujeitas à legislação e à regulamentação específicas, devendo se conformar às regras aplicáveis. Incorrem na mesma situação companhias (abertas ou não) ou outros emissores que captem recursos por meio de uma ICO, em operações cujo sentido econômico corresponda à emissão e à negociação de valores mobiliários.
3. As ofertas de ativos virtuais que se enquadrem na definição de valor mobiliário e estejam em desconformidade com a regulamentação serão tidas como irregulares e, como tais, estarão sujeitas às sanções e penalidades aplicáveis. **A CVM alerta que, até a presente data, não foi registrada nem dispensada de registro nenhuma oferta de ICO no Brasil.**
4. Por outro lado, há operações de ICO que não se encontram sob a competência da CVM, por não se configurarem como ofertas públicas de valores mobiliários.
5. A CVM esclarece que valores mobiliários ofertados por meio de ICO não podem ser legalmente negociados em plataformas específicas de negociação de moedas virtuais (chamadas de *virtual currency exchanges*), uma vez que estas não estão autorizadas pela CVM a disponibilizar ambientes de negociação de valores mobiliários no território brasileiro.
6. Quanto à participação de potenciais investidores em operações de ICO, alerta-se para os seguintes riscos inerentes a tais investimentos (em especial no que diz respeito a emissores ou ofertas não registradas na CVM):
 - a. Risco de fraudes e esquemas de pirâmides (“Ponzi”);

- b. Inexistência de processos formais de adequação do perfil do investidor ao risco do empreendimento (*suitability*);
- c. Risco de operações de lavagem de dinheiro e evasão fiscal/divisas;
- d. Prestadores de serviços atuando sem observar a legislação aplicável;
- e. Material publicitário de oferta que não observa a regulamentação da CVM;
- f. Riscos operacionais em ambientes de negociação não monitorados pela CVM;
- g. Riscos cibernéticos (dentre os quais, ataques à infraestrutura, sistemas e comprometimento de credenciais de acesso dificultando o acesso aos ativos ou a perda parcial ou total dos mesmos) associados à gestão e custódia dos ativos virtuais;
- h. Risco operacional associado a ativos virtuais e seus sistemas;
- i. Volatilidade associada a ativos virtuais;
- j. Risco de liquidez (ou seja, risco de não encontrar compradores/vendedores para certa quantidade de ativos ao preço cotado) associado a ativos virtuais; e
- k. Desafios jurídicos e operacionais em casos de litígio com emissores, inerentes ao caráter virtual e transfronteiriço das operações com ativos virtuais.

7. A CVM recomenda aos potenciais investidores que se deparam com anúncios de ICO, como forma de evitar o risco de fraude, verificar no **site da Autarquia** se o ofertante é emissor registrado na CVM ou se a oferta foi registrada ou dispensada de registro. Além disso, a Autarquia, por meio de seus **canais de atendimento ao investidor**, encontra-se à disposição para receber denúncias e reclamações sobre possíveis irregularidades em tais operações.

8. Os investidores devem avaliar atentamente as características de tais operações, de forma a identificar sinais indicadores de irregularidades, tais como: altos retornos garantidos, pressão para participar das transações imediatamente, ofertantes ou ofertas não registradas na CVM, ausência de requisitos mínimos para a participação em tais operações, entre outros.

A CVM permanece atenta à evolução das ICOs e, sendo o caso, tomará, no momento apropriado, as medidas cabíveis no âmbito de sua competência legal, de forma a assegurar a estabilidade e o contínuo desenvolvimento do mercado de capitais brasileiro.

No dia 16 de novembro de 2017, a CVM emite uma nova nota, explicando o que seria um ICO, e outros assuntos pertinentes ao tema.

Notícias

16/11/2017

Initial Coin Offerings (ICOs)

FAQ da CVM a respeito do tema

Considerando o avanço das operações conhecidas como Initial Coin Offerings (ICOs), a CVM esclarece que está atenta às recentes inovações tecnológicas nos mercados financeiros global e brasileiro. A **Autarquia divulgou nota** na qual explicitou que vem acompanhando tais operações e buscando compreender benefícios e riscos associados, seja por meio de fóruns internos, como o Comitê de

Gestão de Riscos – CGR e o Fintech Hub, ou de discussões no âmbito internacional, como em trabalhos desenvolvidos pela IOSCO.

Em linha com as competências definidas na Lei 6.385/76 e considerando seu mandato legal de fomentar a formação de capitais, a CVM busca estimular a introdução de inovações tecnológicas no mercado de valores mobiliários, sempre que alinhados ao norte da segurança dos investidores e da integridade do mercado.

Assim, a Autarquia presta os seguintes esclarecimentos quanto aos riscos decorrentes dos chamados ICOs, tendo por base as dúvidas mais frequentes sobre o assunto, à luz do regime regulatório atualmente vigente no âmbito do mercado de valores mobiliários:

1. O que são Initial Coin Offerings?

R. Podem-se compreender os ICOs como captações públicas de recursos, tendo como contrapartida a emissão de ativos virtuais, também conhecidos como tokens ou coins, em favor do público investidor. Tais ativos virtuais, por sua vez, a depender do contexto econômico de sua emissão e dos direitos conferidos aos investidores, podem representar valores mobiliários, nos termos do art. 2º da Lei 6.385/76.

Os ICOs vêm sendo utilizados como uma estratégia inovadora de captação de recursos por parte de empresas ou projetos em estado nascente ou de crescimento, muitos ainda em estado pré-operacional, o que enseja um componente de risco por si só.

A inovação associada aos ICOs é oriunda de uma sequência de fatores. Primeiro, por utilizar-se de meios exclusivamente digitais, essa forma de captação facilita a captação de recursos de investidores a partir de qualquer localidade, mediante a transferência de moedas virtuais ou moedas fiduciárias, com maior facilidade e agilidade quando comparado às vias tradicionais.

Segundo, a “digitalização” da cadeia de processos operacionais costuma valer-se de criptografia, programação lógica, protocolos de rede de computadores descentralizados e tecnologias de registro distribuído (“distributed ledger technology - DLT”), o que em tese possibilita maior velocidade e precisão de registros.

2. Quais são as modalidades de ICO mais comuns?

R. Em certos casos, os ativos virtuais emitidos no âmbito de ICOs podem claramente ser compreendidos como algum tipo de valor mobiliário, principalmente quando conferem ao investidor, por exemplo, direitos de participação no capital ou em acordos de remuneração pré-fixada sobre o capital investido ou de voto em assembleias que determinam o direcionamento dos negócios do emissor.

Em outros casos, quando ocorre a emissão de um “utility token”, a distinção não é tão clara, podendo ou não haver entendimento de que houve emissão de valor mobiliário. A emissão de “utility tokens” ocorre quando o ativo virtual emitido confere ao investidor acesso à plataforma, projeto ou serviço, nos moldes de uma licença de uso ou de créditos para consumir um bem ou serviço.

3. No caso de um ativo virtual a ser emitido corresponder a um valor mobiliário, qual seria a orientação aos possíveis emissores de um “ICO”?

R. O regramento da CVM, em especial a Instrução CVM 400, estabelece que a “distribuição de valores mobiliários nos mercados primário e secundário, no território brasileiro, dirigida a pessoas naturais, jurídicas, fundo ou universalidade de direitos, residentes, domiciliados ou constituídos no Brasil, deverá ser submetida previamente a registro na Comissão de Valores Mobiliários”, exceto nos casos de

dispensa de registro ou de requisitos de oferta, conforme dispostos nos Artigos 4º e 5º da referida Instrução.

No que se refere a ofertas de distribuição de valores mobiliários emitidos no exterior, realizadas por intermédio da Internet, para que não se caracterizem como dirigidas ao público residente no Brasil e, conseqüentemente, sujeitas à regulação, fiscalização e registro pela Comissão de Valores Mobiliários, a CVM já se posicionou sobre critérios a serem observados nos Pareceres de Orientação CVM nº 32 e 33, de 2005.

Recentemente, a CVM regulamentou uma possibilidade de dispensa automática de registro de oferta pública por meio da modalidade de crowdfunding, (Instrução CVM 588), com características próprias.

Ademais, o § 1º, Art. 4º da Lei 6.404/76, estipula que somente os valores mobiliários de emissão de companhia registrada na Comissão de Valores Mobiliários podem ser negociados em mercados secundários de valores mobiliários, com o intuito de fornecer à CVM e ao público um conjunto de informações de interesse de potenciais investidores e assegurar a transparência das informações referentes ao emissor.

Por fim, ressalta-se que os mercados secundários aludidos são aqueles admitidos ao funcionamento pela CVM, em especial conforme estipulado pela Instrução 461. O acesso do público investidor aos mercados regulamentados, bem como a negociação de tais valores mobiliários, deve ser feita por meio de intermediários autorizados pela CVM (corretoras e distribuidoras de valores mobiliários – vide Instrução CVM 505), os quais devem atentar para as exigências de prevenção à lavagem de dinheiro (Instrução CVM 301) e para a adequada identificação do perfil do investidor (Instrução CVM 539), utilizando infraestrutura de mercado autorizada pela CVM (por exemplo, centrais depositárias, custodiantes e escrituradores – vide respectivamente Instruções CVM 541, 542 e 543).

Assim sendo, um possível emissor desejoso de efetuar um ICO no mercado brasileiro deve atentar a todo arcabouço regulatório existente, brevemente descrito acima, de forma a se assegurar quanto à viabilidade jurídica da operação pretendida à luz das normas em vigor.

As ofertas de ativos virtuais que se enquadrem na definição de valor mobiliário e estejam em desconformidade com a regulamentação vigente serão tidas como irregulares e, como tais, estarão sujeitas às sanções e penalidades aplicáveis. A CVM alerta que, até a presente data, não foi registrada nem dispensada de registro nenhuma oferta de ICO no Brasil.

4. O que são as chamadas “Exchanges” de ativos virtuais?

R. No Brasil, as chamadas “Exchange” de ativos virtuais são empresas prestadoras de serviços não regulamentadas pela CVM, que oferecem os serviços de negociação, pós-negociação e custódia de ativos virtuais que não caracterizam valores mobiliários.

Essas empresas não são autorizadas pela CVM ou pelo Banco Central para prestar quaisquer serviços relativos a ativos financeiros. Quando o ativo financeiro envolvido for um valor mobiliário, tais empresas devem buscar os registros devidos para o exercício das atividades citadas junto à CVM.

5. O que diferencia um prospecto exigido nas ofertas públicas registradas na CVM dos chamados “white papers” comumente verificados em ICOs?

R. O prospecto é documento essencial em uma oferta pública e regulamentado pela Instrução CVM 400, e disponibiliza informações essenciais padronizadas para que o investidor entenda a proposta da companhia e tome sua decisão de investimento. Dentre outras, encontram-se no prospecto as seguintes informações: perspectivas e

planos da companhia; situação do mercado em que ela atua; os riscos do negócio e da oferta; o quadro administrativo da empresa, bem como informações sobre a oferta em si.

Os chamados “white papers” disponibilizados nos ICOs não correspondem aos prospectos mencionados. Além de não terem respaldo da CVM, são mais breves, genéricos, não padronizados e compostos por algumas informações técnicas operacionais sobre o ICO.

6. Qual a posição da CVM sobre alguns aspectos de governança comumente verificados em ICOs?

R. Diversos ICOs utilizam como ferramentas de amparo reputacional estratégias tais como a publicação de seus códigos-fonte, a divulgação de que houve auditoria independente de seus códigos-fonte e a divulgação de opiniões de supostos especialistas técnicos a respeito da oferta e do projeto em questão. Essas técnicas não são exigidas em prospectos de ofertas regulamentadas pela CVM.

Por outro lado, é importante frisar que tais operações de ICOs não contam com mecanismos de governança exigidos para as ofertas sujeitas a registro junto à CVM, tais como diligências do líder da oferta e do emissor do valor mobiliário, auditoria independente das demonstrações financeiras, verificação da regularidade do emissor junto à autarquia, entre outros aspectos que visam conferir segurança ao valor mobiliário emitido.

7. Qual a posição de outros reguladores internacionais em relação aos ICOs?

R. Há reguladores financeiros que adotam uma postura mais restritiva em relação à captação de recursos via ICOs e a negociação de ativos virtuais em “Exchanges”, chegando a proibi-las.

Outras autoridades, por sua vez, têm compreendido que as normas do mercado de capitais devem ser respeitadas por possíveis emissões via ICO em um processo de captação pública de recursos no qual há emissão de valores mobiliários.

8. Quais os principais riscos associados à negociação de ativos virtuais e à participação em ICOs?

R. Quanto à participação de potenciais investidores em operações de ICO, alerta-se para os seguintes riscos inerentes a tais investimentos (em especial no que diz respeito a emissores ou ofertas não registradas na CVM):

- i. Risco de fraudes e pirâmides financeiras;
- ii. Inexistência de processos formais de adequação do perfil do investidor ao risco do empreendimento (suitability);
- iii. Risco de operações de lavagem de dinheiro e evasão fiscal/divisas;
- iv. Prestadores de serviços atuando sem observar a legislação aplicável;
- v. Material publicitário de oferta que não observa a regulamentação da CVM;
- vi. Riscos operacionais em ambientes de negociação não monitorados pela CVM;
- vii. Riscos cibernéticos (dentre os quais, ataques à infraestrutura, sistemas e comprometimento de credenciais de acesso dificultando o acesso aos ativos ou a perda parcial ou total dos mesmos) associados à gestão e custódia dos ativos virtuais;
- viii. Risco operacional associado a ativos virtuais e seus sistemas;
- ix. Volatilidade associada a ativos virtuais;

x. Risco de liquidez (ou seja, risco de não encontrar compradores/vendedores para certa quantidade de ativos ao preço cotado) associado a ativos virtuais; e

xi. Desafios jurídicos e operacionais em casos de litígio com emissores, inerentes ao caráter multijurisdicional das operações com ativos virtuais.

A CVM recomenda aos potenciais investidores, como forma de evitar os riscos aqui apontados, verificar no site da Autarquia se o ofertante é emissor registrado na CVM e se a oferta foi registrada ou dispensada de registro. Além disso, a Autarquia, por meio de seus canais de atendimento ao investidor, encontra-se à disposição para responder a consultas sobre ofertas registradas na Autarquia, bem como investigar denúncias e reclamações sobre possíveis irregularidades nessas e em outras operações.

Os investidores devem avaliar atentamente as características de tais operações, de forma a identificar indícios de possíveis irregularidades, tais como: promessas de retornos elevados com baixo risco, pressão para participar das transações imediatamente (sentido de urgência), ofertantes ou ofertas não localizadas no site da CVM, ausência de análise da capacidade financeira e perfil de risco do investidor, entre outros.

A CVM permanece atenta à evolução dos ICOs e, sendo o caso, tomará, no momento apropriado, as medidas cabíveis no âmbito de sua competência legal, de forma a assegurar a estabilidade e o contínuo desenvolvimento do mercado de capitais brasileiro.

O Banco Central também [divulgou um FAQ](#) e [Comunicado nº 31.379](#), alertando sobre os riscos das operações de guarda e negociação das moedas virtuais.

Quatro meses após a nota acima citada, no dia 07 de março de 2018, novamente a CVM emite uma nova nota a respeito do ICO.

Notícias

07/03/2018

Initial Coin Offerings (ICOs)

CVM esclarece que não faz recomendação ou ratifica ofertas

Considerando os recentes comunicados a respeito das operações de ofertas de ativos virtuais conhecidas como *Initial Coin Offerings* (ICOs), bem como as análises de casos concretos realizados desde então, a CVM julga pertinente esclarecer alguns pontos sobre o tema.

Primeiramente, a CVM informa que, até o presente momento, nenhum ICO obteve dispensa ou registro de oferta pública de distribuição de valores mobiliários na Autarquia.

Os trabalhos realizados pela Autarquia abarcam desde a análise de documentos utilizados na distribuição desses ativos virtuais até o monitoramento de notícias veiculadas na imprensa e redes sociais, incluindo, quando necessário, pedidos de esclarecimentos aos agentes envolvidos em tais operações.

Em todo caso, as análises e decisões tomadas pela CVM não ratificam ou recomendam uma oferta de valores mobiliários. Estas e outras ações têm como objetivo verificar se as operações de ICOs estão enquadradas nas definições de

oferta pública de valores mobiliários estabelecidas nos normativos da CVM para que, quando a resposta for positiva, sejam tomadas as medidas cabíveis.

Sobre esse aspecto, vale reforçar que quaisquer comunicações, efetuadas por terceiros, que envolvam o uso da sigla, logotipo ou slogan da CVM devem atender ao disposto na Deliberação CVM 749, em especial no art. 4º, que trata da indução de terceiros ao erro ou confusão. Comunicações em desconformidade com a regulação são tidas como irregulares e estarão sujeitas às penalidades aplicáveis.

A CVM destaca, ainda, que lhe cabe regular a oferta e negociação de ativos que se enquadrem no conceito legal de valor mobiliário, não estando em seu escopo de atuação os que não têm essa característica.

A Autarquia recomenda que os investidores tenham atenção aos seguintes riscos relacionados aos investimentos em ICOs (em especial no que diz respeito a emissores ou ofertas não registradas na CVM):

- i. Risco de fraudes e pirâmides financeiras;
- ii. Inexistência de processos formais de adequação do perfil do investidor ao risco do empreendimento (*suitability*);
- iii. Risco de lavagem de dinheiro ou de evasão fiscal ou de divisas;
- iv. Atuação de prestadores de serviços sem observância da legislação aplicável;
- v. Material publicitário de oferta que não observa a regulamentação da CVM;
- vi. Riscos operacionais em ambientes de negociação não monitorados pela CVM;
- vii. Riscos cibernéticos (dentre os quais, ataques à infraestrutura, sistemas e comprometimento de credenciais de acesso dificultando o acesso aos ativos ou a perda parcial ou total destes) associados à gestão e custódia dos ativos virtuais;
- viii. Risco operacional associado a ativos virtuais e seus sistemas;
- ix. Volatilidade associada a ativos virtuais;
- x. Risco de liquidez (ou seja, risco de não encontrar compradores/vendedores para certa quantidade de ativos ao preço cotado) associado a ativos virtuais; e
- xi. Desafios jurídicos e operacionais em casos de litígio com emissores, inerentes ao caráter multijurisdicional das operações com ativos virtuais.

Por fim, a CVM lembra que os investidores podem enviar denúncias ou reclamações sobre possíveis irregularidades em tais operações por meio dos **canais de atendimento ao cidadão**.