UNIVERSIDADE DE FEDERAL DA BAHIA
FACULDADE DE ECONOMIA
CURSO DE GRADUAÇÃO EM CIÊNCIAS ECONÔMICAS

VICTOR MATHEUS MACEDO SANTOS

BLOCKCHAIN E AS CRIPTOMOEDAS: FUNDAMENTOS ECONÔMICOS E TENDÊNCIAS REGULATÓRIAS

SALVADOR
2019

VICTOR MATHEUS MACEDO SANTOS

BLOCKCHAIN E AS CRIPTOMOEDAS: FUNDAMENTOS ECONÔMICOS E TENDÊNCIAS REGULATÓRIAS

Trabalho de conclusão de curso apresentado ao curso de Ciências Econômicas da Universidade Federal da Bahia como requisito parcial à obtenção do grau de bacharel em Ciências Econômicas

Área de Concentração: Economia Política

Orientador: Prof. Me. Ihering Guedes Alcoforado de Carvalho

SALVADOR
2019

S337 Santos, Victor Matheus Macedo

Blockchain e as criptomoedas: fundamentos econômicos e tendências regulatórias/ Victor Matheus Macedo Santos. -- Salvador, 2019.

75 f.; il.

TCC (Graduação) – Universidade Federal da Bahia, Faculdade de Economia. Orientador: Prof. Me. Ihering Guedes Alcoforado de Carvalho.

1. Criptomoedas – tecnologias. 2. Bitcoin. 3. Moeda regulamentação. 4. Sistema monetário. I. Universidade Federal da Bahia. II. Carvalho, Ihering Guedes Alcoforado de. III. Título.

CDD: 332.46

VICTOR MATHEUS MACEDO SANTOS

BLOCKCHAIN E AS CRIPTOMOEDAS:
FUNDAMENTOS ECONÔMICOS E TENDÊNCIAS REGULATÓRIAS

Trabalho de conclusão de curso apresentado ao curso de Ciências Econômicas da Universidade Federal da Bahia, como requisito parcial para a obtenção do grau de bacharel em Ciências Econômicas.

Aprovada em 04 de julho de 2019.

Banca Examinadora

_____

Prof. Me. Ihering Guedes Alcoforado de Carvalho
Universidade Federal da Bahia – UFBA

_____

Prof. Dr. Hamilton de Moura Ferreira Junior
Universidade Federal da Bahia – UFBA

_____

Prof. Dr. Leonardo Bispo de Jesus Júnior
Universidade Federal da Bahia – UFBA

RESUMO

Este artigo busca trazer os elementos para a discussão sobre como a regulação dos governos pode interferir na manutenção e no crescimento das novas tecnologias de criptomoedas. O sistema das moedas virtuais, puxadas pelo Bitcoin e Ethereum é algo novo para a sociedade mundial, que tem em sua história a tradição de segurança em ter nas moedas um equivalente de algo físico com valor, geralmente o ouro. Recentemente após Bretton Woods essa relação de segurança diminui quando o dólar passou ser uma moeda fiduciária, ou seja, sem nenhum lastro em ouro. O que pode estar acontecendo agora pode ser uma mudança nos paradigmas da atual estrutura monetária mundial. As criptomoedas não são reguladas por nenhuma instituição de qualquer país, o que mostra ainda um vácuo de regulamentação na economia mundial. O foco dessa monografia é entender como acontece essa tecnologia e sua relação com as prováveis regulamentações vindas dos governos centrais, pois a depender das medidas para por regras nessa nova tecnologia, para impedir o uso para lavagem de dinheiro, por exemplo, pode fazer com que uma tecnologia que pode vim a mudar o paradigma das relações monetárias possa sofrer sem necessidade, levando o ônus de especulações de que se trata de uma bolha. A tecnologia como um todo pode sofrer por algumas brechas existentes no vácuo regulamentário atual, mas o desenvolvimento dessa tecnologia não deve ser associado a apenas as partes especulativas sobre ela.

Palavras-chave: Criptomoedas. Bitcoin. Ethereum. Regulação. Blockchain

ABSTRACT

ABSTRACT

This paper seeks to bring the elements to the discussion about how the regulation of the governments can interfere in the maintenance and the growth of the new technologies of cryptocurrencies. The system of virtual currencies, drawn by Bitcoin and Ethereum, is something new for world society, which has in its history a tradition of security in having in coins an equivalent of something of value, usually gold. Recently after Bretton Woods, this security ratio declines as the dollar has fewer gold reserves. What may be happening now may be a shift in the paradigms of the current world monetary structure. Cryptocurrencies are not regulated by any institution in any country, which still shows a regulatory vacuum in the world economy. The focus of this paper is to understand how this technology and its relationship to the likely regulations coming from central governments, because depending on the measures by rules in this new technology, to prevent the use for money laundering, for example, can cause a technology that could change the paradigm of monetary relations may suffer without necessity, taking the burden of speculation that it is a bubble, that is, the technology as a whole may suffer from some existing gaps in the current regulatory vacuum, but the development of this technology should not be associated with only the speculative parts about it.

Keywords: Cryptocurrencies. Bitcoin. Ethereum. Regulation

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1 INTRODUÇÃO

A era da globalização junto com o surgimento da internet trouxe mudanças significativas no *modus operandi* da economia mundial, e em especial do sistema financeiro, com transações rápidas e a criação de um mercado global conectado. Nesse mundo interconectado a tecnologia das criptomoedas, que é o nome dado às moedas que tem origem em redes *Blockchain*, surge como uma espécie de evolução adaptativa às condições postas, pois as criptomoedas, lideradas por Bitcoin e Ethereum trazem em sua essência as características do mundo da internet, o mundo que não apresenta fronteiras, e tem uma relação fundamental entre as pessoas envolvidas, internet e o sistema bancário e financeiro.

O tema deste trabalho são as criptomoedas e a *Blockchain*, que é a rede que sustenta o sistema de pagamentos dessas moedas, buscando discutir como a regulação pode interferir no crescimento dessa nova tecnologia. A primeira criptomoeda a surgir foi o Bitcoin, criado por Satoshi Nakamoto. Satoshi discutia como deveria funcionar, na sua concepção, um sistema eletrônico de pagamentos totalmente descentralizado baseado em um sistema criptografado e utilizando-se de tecnologia *peer-to-peer*, ou seja, pessoa-a-pessoa. A ideia de Nakamoto era criar um sistema de pagamentos que não fosse controlado e regulado por nenhuma instituição, que ao ver dele não são confiáveis.

Com o crescimento exponencial das moedas virtuais as discussões sobre sua natureza se tornam cada vez mais extremistas. Há o lado mais conservador que considera as criptomoedas como um tipo caso de bolha financeira, onde os agentes entram apenas de modo especulativo para ter altos retornos, se estar ligado ao processo das moedas. Esse ponto de vista é compartilhado, por exemplo, pelo banco central brasileiro, que considera que os riscos são grandes e que se trata de uma típica bolha.

O outro lado mais otimista com as criptomoedas acredita que essa é uma tecnologia que está apenas nascendo, tendo um grande potencial ainda pela frente, mudando todo um paradigma de como a sociedade mundial usa as moedas, sendo o governo do Japão e da Suíça os países que mais compartilham esse ponto de vista. Os grandes atores para a evolução ou morte das moedas virtuais serão os governos que se articularem para manter o monopólio sobre as

moedas em circulação em seu circuito poderão decretar o fim de uma tecnologia que ainda não mostrou todo seu potencial.

Em função do exposto acima o tema deste trabalho são as criptomoedas, que são moedas virtuais geradas através de complexos processos de criptografia, tendo por trás um sistema que as valida chamado de *Blockchain*, cujos desafios impostos ao seu desenvolvimento são tanto endógenos associado a pesquisa no campo de processamento, e, exógeno, exógeno associado as possíveis instrumentalização possível em muitas outras aplicações.

Em função do exposto, nosso objeto, a bitcoin, primeira criptomoeda a surgir foi o Bitcoin, criado por Satoshi Nakamoto. Satoshi é apenas uma ponta do iceberg. Na sua formulação original se discutia como deveria funcionar um sistema eletrônico de pagamentos totalmente descentralizado baseado em um sistema criptografado e utilizando-se de tecnologia *peer-to-peer*, ou seja, pessoa-a-pessoa.

A ideia de Nakamoto era criar um sistema de pagamentos que não fosse controlado e regulado por nenhuma instituição, que ao ver dele não são confiáveis mas como a rede *Blockchain* e as criptomoedas não são reguladas nem pertencentes a nenhuma instituição ou pessoa, e por esse seu caráter universal e livre a questão da regulação dos Estados será essencial para seu crescimento e maturação como uma tecnologia que pode mudar o paradigma atual da relação das pessoas e dos Estados com o dinheiro e como se adquirir produtos.

O objetivo geral deste trabalho é pesquisar as alternativas regulatórias postas de regulação as criptomoedas e ao *blockchain*, delineando os possíveis efeitos e consequência no desenvolvimento não só das criptomoedas (bitcoin) no sistema eletrônico de pagamentos, mas principalmente nos negócios assentados nelas. Para tanto, este trabalho consta desta introdução, mais três partes e uma conclusão.

Entre objetivos específicos estão uma revisão sistemática da literatura tradicional, que expresse não apenas a sustentação teórica sobre as criptomoedas, além de buscar compreender o sistema *blockchain* e as criptomoedas, na forma como as medidas regulatórias mundiais (endógenas e exógenas) irão impactar o curso de crescimento dessa nova tecnologia.

Este trabalho tem em seu segundo capitulo a discussão sobre o que são as criptomoedas, como elas são produzidas, por quem e como circulam. É um ponto fundamental para o entendimento sobre a natureza das moedas virtuais, evidenciando que se ancora em conceitos de tecnologia de informação sofisticados que, como a maioria das novas tecnologias cujo mecanismos encontra-se fora do alcance dos leigos, é sempre vulnerável a valorização especulativa, sem algo concreto sustentado, ficando seu valor à mercê da subjetividade das "manadas". E que também ancora novos arranjos organizacionais que potencializam a exploração das economias de escala e de escopo.

O terceiro capitulo traz a discussão técnica sobre as redes *blockchain*s, explorando como essa nova tecnologia conseguiu mudar a forma das transações financeiras e de informações, entrando nos conceitos fundamentais para as criptomoedas como criptografia, além de problemas relacionados a área de informática como o problema dos Generais Bizantinos.

O quarto capítulo traz a discussão sobre como as possibilidades regulatórias em diferentes níveis e por diferentes atores podem afetar as criptomoedas. No plano dos níveis, a primeira é a possibilidade da regulação endógena, por meio do estabelecimento de "padrões técnicos" a serem seguidos no desenvolvimento da *blockchain*, e a segunda é a regulação exógena, ou seja, a que contempla a operação e manejo efetivo da tecnologia no suporte da realização de atividades, a exemplo do Bitcoin no sistema eletrônico de pagamentos.

2 AS VISÕES ECONÔMICAS DA *BLOCKCHAIN*

O segundo capitulo deste trabalho traz fundamentação teórica sobre as criptomoedas e a rede *Blockchain*, buscando na literatura tradicional argumentos que dão suporte a essa nova tecnologia. Essa literatura contém obras literárias das mais diversas áreas da ciência econômica, abordando a teoria Neo Institucional com o pensamento Coseano e também os principais autores da escola austríaca.

A tecnologia da *Blockchain* e das criptomoedas é algo relativamente novo, sendo a primeira moeda virtual lançada em 2008, o Bitcoin, porém é possível fundamentar as criptomoedas na literatura tradicional, podendo relacionar com diversas escolas econômicas, como a escola Austríaca, que é marcada pelo liberalismo e pelo papel empreendedor como agente de mudança na sociedade. Outro ponto que se pode associar as moedas virtuais é na área dos custos de transações, já que as criptomoedas se destacam pela realização rápida de transferências monetárias e na confecção de contratos inteligentes.

A principal atribuição da rede *Blockchain* é a transferência monetária e a criação de uma moeda segura e sem vínculo com o Estado, mesmo podendo fazer outras funções como contratos. A moeda tem três funções. É uma reserva de Valor, um Padrão de Valor e um meio de troca (MANKIW,1997, p.112). Seguindo o que Mankiw diz sobre moedas, as criptomoedas ainda não podem ser consideradas de fato moedas, já que elas ainda não são aceitas amplamente como meio de trocar, mesmo considerando que sua aceitação tem crescido. As criptomoedas também não podem ser consideradas como reserva de Valor, já que a economia mundial ainda não a abraçou como uma forma de se proteger, muito pelo contrário ainda é considerada como o um investimento de risco. Não sendo reserva de valor e também não sendo um meio de troca amplamente aceito, como consequência sua função como Padrão de Valor está prejudicada.

O autor da escola Austríaca Friedrich Hayek adiciona uma função a mais do que Mankiw como definição do papel da moeda, que é ter valor para contratos de pagamentos futuros. Essa função pode ter o papel inicial para o crescimento das criptomoedas e da rede *Blockchain*, isso devido a característica das criptomoedas de não pertencerem a um Estado ou ser de uma empresa privada de algum país.

Os contratos feitos pela rede *Blockchain* podem ser uma alternativa nas relações financeiras entre os países, oferecendo uma alternativa rápida e segura nas operações comercias internacionais.

> There are four kinds of uses of money that would chiefly affect the choice among available kinds of currency: its use,· first, for cash purchases of commodities and services, second, for holding reserves for future needs, third, in contracts for deferred payments, and, finally, as a unit of account, especially in keeping books[1](HAYEK,1990,p.67).

Considerando as criptomoedas, que são produtos da rede *Blockchain*, não tem muitas características necessárias para de fato serem moedas, por que então há tanta expectativa sobre elas? A resposta é simples, as criptomoedas não são consideradas moedas de fato por que ninguém as considera moeda, ou seja, o efeito de confiança em uma moeda está baseado na confiança dos agentes.

Para Milton Friedman a moeda é aceita por uma pessoa porque sabe que as outras pessoas irão aceita-la.

> The short answer is that each person accepts them because he is confident that others will. The pieces of green paper have value because everybody thinks they have value. Everybody thinks they have value because in his experience they have had value[2](FRIEDMAN; FRIEDMAN,1990, p.249).

O fator psicológico sobre a aceitação da moeda tem mais força do que apenas suas funções descritas pelos manuais de economia, para que algo vem a exercer tais funções é necessário que se crie uma expectativa na sociedade de que a nova moeda será aceita por todos. O dólar é aceito como moeda devido a influência norte americana no mundo todo, porém para exercer a função de moeda de troca, reserva de valor e unidade de conta, antes foi necessário a criação nos agentes de que aquela moeda seria aceita facilmente devido à quantidade de operações realizadas em toda a economia mundial.

O resultado da aceitação coletiva em uma moeda é fruto de longos períodos de aceitação da mesma, de modo que passe a ser inquestionável a crença de que aquela moeda tenha valor

[1] Há quatro tipos de usos para a moeda que geralmente usam uma escolha entre os tipos de moeda disponíveis: seu uso, primeiro, para fazer compras em dinheiro de mercadorias e serviços, em segundos reservas para as necessidades futuras, em terceiro lugar, nos contratos futuros e, finalmente, como uma unidade de conta, especialmente nos livros de contabilidade. Tradução feita pelo Autor

[2] A resposta curta é que cada pessoa os aceita (dólar) porque está confiante de que os outros o aceitarão. Os pedaços de papel verde têm valor porque todos pensam que têm valor. Todos pensam que têm valor porque em sua experiência eles tiveram valor>Tradução feita pelo Autor

dentro da sociedade. Assim como a aceitação é um processo demorado, a desconstrução dessa aceitação é algo difícil e que necessita de um tempo de maturação, e por isso o Bitcoin e as Criptomoedas sofrem até hoje uma rejeição dos agentes econômicos em todos os países. *The convention or the fiction is no fragile thing. On the contrary, the value of having a common money is so great that people will stick to the fiction even under extreme provocation* (FRIEDMAN; FRIEDMAN 1990, p.249).

Desde o acordo Internacional de Bretton Woods o pilar de confiança de uma moeda é apenas seu emissor, já que foi abandonado o padrão ouro, onde cada quantidade monetária tinha seu respectivo valor em ouro, se consolidando o padrão dólar, no qual o lastro da moeda é a emissão pelo governo dos Estados Unidos. Segundo Mckinnon;

> Amazingly enough, since 1971, when president Nixon officially closed the gold window and so cut what had become just a vestigial tie to gold, the world has remained on an unalloyed dollar standard. The dollar remains the main international unit of account, means of settlement, and official reserve currency [3] . (MCKINNON,2013, p.9).

A relação de como a sociedade entende na moeda algo que tem valor está baseado basicamente hoje em dia na confiança, já que a emissão monetária dos países não é baseada em lastro com algo real. Para dar confiabilidade a sua moeda os Estados compram títulos em moeda estrangeira de outros países, sendo a maioria desses títulos dos Estados Unidos. China (including Hong Kong) *hold* $ 1.4 trillion in US *treasury securities*[4] (CONTRACTOR,2018, p.104).

Esse modo usado pelos Estados para proteger sua moeda e gerar estabilidade na economia é hoje o grande pilar da sustentação da confiança dos agentes monetários sobre a situação de um Pais, o que constrói um possível baralho de cartas, ou seja, problemas gerados sobre a confiança do dólar como moeda forte pode impactar toda a economia mundial em um efeito cascata.

Não será discutido a fundo como a política monetária tradicional pode afetar a economia dos países, sendo que o objetivo aqui é entender que a economia mundial está baseada em dólar,

[3] Surpreendentemente, desde 1971, quando o presidente Nixon fechou oficialmente o lastro com o ouro e assim cortou o que se tornou apenas um vestígio de ouro, o mundo permaneceu em um padrão inalterado do padrão dólar. O dólar continua sendo a principal unidade de conta internacional, meio de troca e moeda oficial de reserva.

[4] A china (incluindo Hong Kong) mantém $1.4 trilhão em títulos do tesouro americano. Tradução feita pelo Autor

que por sua vez é uma moeda fiduciária desde Bretton Woods, o que significa um intrínseco potencial gerador de instabilidades econômicas por todo mundo, já que a política monetária Americana é o núcleo de toda base monetária mundial.

A intenção deste trabalho não é defender que o Bitcoin e outras criptomoedas venham a tomar o papel das moedas tradicionais, discordando de muitos evangelistas que imaginam uma imensa revolução que irá acontecer em pouco tempo. O papel da rede *Blockchain* e das criptomoedas terá grandes impactos sim, proporcionando mudanças na economia via produtividade, mas não necessariamente gerando uma total revolução no paradigma atual de transações monetárias. Este capitulo busca o trazer contribuições teóricas de grandes autores nas mais diversas áreas do conhecimento econômico, buscando fundamentar que a rede *Blockchain* e as criptomoedas podem ser uma ferramenta de grande utilidade, enfrentando problemas já destacados por esses grandes autores econômicos.

2.1 A VISÃO AUSTRÍACA DO BITCOIN

A escola econômica Austríaca é conhecida pela sua visão de liberdade nas decisões econômicas, sempre com pontos favoráveis a liberdade econômica para o avanço da economia, controlando o estado e tendo o individualismo metodológico como um ponto fundamental em sua base teórica, ou seja, o indivíduo produz as ações que justificam os fenômenos econômicos.

A escola austríaca tem como ponto fundamental de sua teoria a efetividade do mercado em alocar recursos, reduzindo e até mesmo retirando o papel governamental como a instituição capaz de levar a economia a um nível de eficiência maior, o que é resultado da tendência governamental de aplicação de políticas monetárias expansionistas, gerando crises de inflação que acabam afetando a produção da economia. *Austrian analysis also highlights the effectiveness of the free market in the allocation of resources and is correspondingly critical of government intervention in the economy* [5](MILNE, 2017, p.61).

[5] A análise austríaca também dá foco á efetividade do livre mercado na alocação dos recursos e é correspondentemente critico á intervenção governamental na economia. Tradução feita pelo autor.

Para Mises o Estado não é por direito o único proprietário do dinheiro, pois isso vai contra a essência do mercado e do uso do dinheiro em uma sociedade livre:

> The concept of Money as a creature of Law and the State is clearly untenable. It is not justified by a single phenomenon of the market. To ascribe to the State the Power of dictating the Laws of exchange, is to ignore the fundamental principles of Money-using society[6] (MISES, 1953, p. 69).
> .

O arcabouço teórico austríaco traz os elementos para o entendimento da função econômica das criptomoedas mesmo tendo sido escrito há muitos anos atrás. A concepção de moeda como algo que é sempre entendido como de fonte governamental é questionada por Hayek e confronta as principais rejeições as criptomoedas, pois a sociedade ainda não consegue ver uma moeda virtual, que foi criada por uma instituição que não seja um Estado nacional uma fonte segura de reserva de valor. As criptomoedas tem o poder de retirar dos governos centrais as decisões sobre política monetária, o que é visto de forma positiva pelos pensadores austríacos. A escola austríaca tem muitos autores de grande importância como Murray Rothbard, Ludwig von Mises e Friedrich Hayek.

2.1.1 Menger e a origem do dinheiro

Um dos fundadores da Escola Austríaca de economia, Carl Menger abordou em sua obra "*on the origins of Money*" questionamentos sobre o papel exercido pelo dinheiro no psicológico das pessoas, questionando como se é possível uma determinação tão grande da sociedade em se empenhar ao máximo para no final obter metais ou papeis, no caso ouro e dinheiro. O papel psicológico que existe na determinação sobre a confiança no dinheiro tem é então fundamental para o crescimento e desenvolvimento da economia, no sentido de que haverá aceitação de outros agentes pela moeda resultará em uma busca para se conseguir o máximo possível de determinadas peças. Para que assim se troquem por outras que de fato os agentes desejam

> But that every economic unit in a nation should be ready to exchange his goods for little metal disks apparently useless as such, or for documents representing the latter, is a procedure so opposed to the ordinary course of things, that we cannot well wonder if even a distinguished thinker like Savigny finds it downright "mysterious[7]"(MENGER,1982,p.11).

[6] O conceito de dinheiro como criação da Lei e do Estado é claramente insustentável. Atribuir ao Estado o poder de ditar as leis de trocas é ignorar o princípio fundamental das sociedades monetizadas. Tradução feita pelo autor
[7] Mas que toda unidade econômica em uma nação deve ser pronto para trocar seus produtos por pequenos discos de metal aparentemente inútil como tal, ou para documentos representando o último, é um procedimento tão

Para Mengel a aceitação em uma moeda é algo que vem em um período anterior até mesmo as primeiras identificações destes metais como moedas, ou seja, um comodity pode exercer uma função de moeda, no sentido de que o esse objeto não sofreu alteração de seu aspecto natural, porém mesmo assim os agentes econômicos a escolheram para depositar confiança como algo de valor. *And even certain other commodities, cattle, skins, cubes of tea, slabs of salt, cowrie-shells, etc*.[8](MENGER,1982, p.12).

Sem o consenso econômico de que algo poderia ter valor como moeda, as transações seriam prejudicadas, em complexidade e quantidade, sendo realizadas apenas quando houvesse uma combinação de intenções entre um comprador e um vendedor, na qual um gostaria de obter o objeto a ser trocado do outro, e vice-versa. A definição do ponto comum surge então como algo necessário para que o comercio prospere, realizando transações entre indivíduos que não gostariam de obter o objeto de outro parceiro comercial.

A moeda se encaixa então como uma solução para os agentes no mercado consigam promover transações sem a necessidade na combinação de desejos de mercadorias dos compradores e vendedores. A *comodity* então que ocuparia o lugar de destaque como ancora para as demais transações seria a que obtivesse o maio grau de vendabilidade, sendo assim aquela que conseguisse maior difusão entre os mais diversos aspectos que Menger citou, ou seja para que algum produto viesse a se tornar uma moeda padrão era necessário (MENGER,1982, p.29)

1. Upon the number of persons who are still in want of the commodity in question, and upon the extent and intensity of that want, which is unsupplied, or is constantly recurring [9].
2. Upon the purchasing power of those persons[10].
3. Upon the available quantity of the commodity in relation to the yet unsupplied (total) want of it [11].
4. Upon the divisibility of the commodity, and any other ways in which it may be adjusted to the needs of individual customers[12].
5. Upon the development of the market, and of speculation in particular. And finally,[13].

---

oposto para o curso normal das coisas, que não podemos bem me pergunto se mesmo um pensador distinto como Savigny acha absolutamente "misterioso". Tradução feita pelo Autor.

[8] E até algumas outras *comodities*, como gado, peles, cubos de chá, ostras, sal, conchas de búzios e etc.

[9] Quanto ao número de pessoas que ainda não tem *comodity* em questão, e sobre a extensão e intensidade dessa falta, que não está fornecida, ou é constantemente recorrente. Tradução feita pelo Autor

[10] A depender do poder de compra destas pessoas. Tradução feita pelo Autor

[11] A depender da quantidade disponível em relação ao total possível de ser feito. Tradução feita pelo Autor.

[12] A depender da divisibilidade da *comodity*, entre outras formas na qual pode ser ajustável aos consumidores. Tradução feita pelo Autor

6. Upon the number and nature of the limitations imposed politically and socially upon exchange and consumption with respect to the commodity in question[14].

A depender de como uma *commodity* se comporta em um Mercado, ela então poderia passar a ser aceita pelos demais agentes como uma medida padrão para que outras transações possam ocorrer. O sal foi por algum tempo uma moeda, e seguindo as condições de Mengel é possível entender o motivo, pois é algo que as pessoas precisavam no presente e passado, como diz a regra 1. Também pode ser facilmente divisível, como sugere a regra 4. Com o passar do tempo outros produtos se tornaram moedas devido a conseguir satisfazer as outras regras de Menger, passando para o Ouro e mais recentemente o papel moeda.

O ponto importante que relacionada a obra de Menger com as Criptomoedas e a rede *Blockchain* está na defesa do Autor de que a moeda é uma solução do mercado, para atender um problema criado pelo também pelo mercado. Menger não cita a necessidade da intervenção do Estado para o uso de determinada moeda por uma sociedade

> Money is not an invention of the state. It is not the product of a legislative act. Even the sanction of political authority is not necessary for its existence. Certain commodities came to be money quite naturally, as the result of economic relationships that were independent of the power of the state[15](MENGER,1982, p.261).

A moeda vem para Menger como uma reposta às necessidades do mercado, sem necessariamente estar associado a uma criação do Estado. Isso não significa que a participação do Estado nas diretrizes econômicas é algo necessariamente ruim. Para o Autor a interferência Estatal trouxe benefícios para o aperfeiçoamento do sistema de pagamentos em reposta a um comercio crescente.

> On the other hand, however, by state recognition and state regulation, this social institution of money has been perfected and adjusted to the manifold and varying needs of an evolving commerce, just as customary rights have been perfected and adjusted[16](MENGER,1982, p.51).

---

[13] A depender do desenvolvimento do mercado, e em especial da especulação.E finalmente(anunciando o próximo tópico. Tradução feita pelo Autor

[14] A depender do número e natureza de limitações impostas políticas e socialmente na troca e consumo. Tradução feita pelo Autor

[15] O dinheiro não é invenção do Estado. Não é o resultado de um ato legislativo; sua sanção por parte da autoridade estatal é totalmente alheia ao conceito de dinheiro. Também a adoção de determinadas mercadorias como dinheiro teve em sua origem em um processo natural a partir das condições econômicas existentes, sem que houvesse necessidade da interferência do Estado nesse processo. Tradução feita pela Autor.

[16] Por outro lado, no entanto, p reconhecimento estatal e regulamentação estatal, esta instituição social do dinheiro foi aperfeiçoada e ajustada às múltiplas e variadas necessidades de um comércio em evolução, da mesma forma que os direitos consuetudinários foram aperfeiçoados e ajustados. Tradução feita pelo Autor

Seguindo a teoria de Menger é possível observar uma relação entre o estágio atual de um mercado e sua respectiva moeda, ou seja, na medida que esse mercado progride, a moeda que vem a se tornar padrão pode mudar, já que esse mercado cresceu e como consequência sua estrutura está maior. Esse processo de "evolução" é resultado da criação de novas necessidades, e como consequência novas formas de respostas serão exigidas para atender as demandas dos agentes econômicos participantes. Uma vantagem na mudança do padrão ouro para o padrão fiduciário foi a redução dos custos de transporte e de custódia do ouro.

O padrão ouro foi resposta às necessidades de uma economia mundial menor e menos complexa. Na medida que a economia foi crescendo a manutenção desse padrão seria possível porem extremamente custoso. A nova economia globalizada demandou um outro padrão para moeda, que permitisse uma melhor resposta as necessidades de maiores quantidade de transações.

Seguindo as posições defendidas por Menger de que a moeda muda a medida de que os mercados exigem isso, é possível especular que uma próxima mudança ocorrerá com as criptomoedas. A rede *Blockchain* surgiu como resposta a demanda por alguns setores da sociedade por um sistema de pagamentos rápido, sem fronteiras e que permitisse a custodia do seu próprio dinheiro. A "evolução" monetária que o Bitcoin e as outras criptomoedas podem trazer é uma nova forma de atuação da moeda, em consequente necessidade de uma economia que está se tornando maior, mais complexa e também mais exigente em relação a velocidade das informações.

O Bitcoin é uma criação que teve sua criação os elementos da internet em resposta ao mundo criado depois da internet. Se considerarmos que a comercialização da internet começou nos anos 90, sua dominância em toda economia mundial após 30 anos é inegável. Em resposta a essa mudança estrutural em todas as sociedades e economias surge o Bitcoin e a rede *Blockchain*, com uma moeda sem associação a nenhum governo, rápida e segura. As criptomoedas são a evolução necessária para a economia construída a partir da globalização e da internet.

2.1.2 Hayek e a moeda privada

Um dos maiores autores da escola austríaca, Friedrich Hayek, em 1974 lançou um livro trazendo ideias sobre a possibilidade de moedas privadas, saindo do *mainstream* econômico e questionando o dogma de que o estado deve emitir moeda. Hayek traz sua ideia visando a estabilidade de preços na economia, obtida retirando dos governos centrais a possibilidade de mascarar políticas públicas ineficientes, que são recorrentes devido ao monopólio da emissão de moeda. O argumento central do livro *denationalization of Money* é: *price level stability can be achieved only by removing from national governments their monopoly of money creation*[17] (HAYEK,1974, p.19).

Em sua obra Hayek questiona o papel do Estado e do dinheiro, considerando que se uma tentativa bem-sucedida de criação de moeda sem o suporte do Estado obter sucesso, logo outros questionamentos nesse sentido, até então imagináveis em ir contra o poder de sustentação de uma moeda pelo Estado irão surgir. A possibilidade sobre o questionamento da autoridade Estatal sobre a moeda animou Hayek, já que se uma funcionasse o questionamento sobre o monopólio dos Governos sobre o dinheiro seria questionada, como está acontecendo com o Bitcoin.

> The further pursuit of the suggestion that government should be deprived of its monopoly of the issue of money opened the most fascinating theoretical vistas and showed the possibility of arrangements which have never been considered[18](HAYEK,1990, p.13).

As criptomoedas trazem a possibilidade de que o dinheiro se torne independente do Estado, já que sua tecnologia permite transações financeiras sem intermediários, mas que ficam registradas em um livro-razão, trazendo segurança para os agentes. Com o crescimento da primeira criptomoeda, outras logo surgiram em sequência, sendo algumas concorrentes diretas no âmbito das transações financeiras, e outras com funções diferentes, como os contratos inteligentes. O ponto que Hayek defende é que se uma experiencia obtiver êxito, logo outras

[17] O argumento central da obra *denationalization of Money* é: a estabilidade do nível de preços só pode ser alcançada quando se remover o monopólio dos governos nacionais na criação de moeda. Tradução feita pelo autor

[18] A continuação da sugestão de que o governo deveria ser privado do seu monopólio da questão do dinheiro abriu novas possibilidades teóricas mais fascinantes e mostrou a possibilidade de arranjos que nunca foram considerados. Tradução feita pelo Autor

apareceriam, o que de fato ocorreu. Com o crescimento do mercado e da exposição para a sociedade, os indivíduos então iriam questionar o papel do Estado como único provedor da moeda.

> As soon as one succeeds in freeing oneself of the universally but tacitly accepted creed that a country must be supplied by its government with its own distinctive and exclusive currency, all sorts of interesting questions arise which have never been examined. The result was a foray into a wholly unexplored field[19] (HAYEK,1990, p.13).

O resultado da criação do Bitcoin e das criptomoedas é uma situação nova, tanto para a sociedade e também para os Governos devido a possibilidade em ganhos de produtividade via rede *Blockchain*, e uma possível retirada do poder de política monetária dos governos, isso se as criptomoedas crescerem em um ritmo acelerado, mudando a estrutura monetária da economia mundial. Para Hayek é importante que essas novas moedas sejam estáveis, para que assim os agentes tenham confiança nesse novo método monetário, migrando do padrão estatal que, para ele, é o grande gerador de crises via excesso na estimulação de investimentos, gerando períodos de recessão. Essa nova política monetária traria assim períodos de estabilidade gerado pelo não uso dos políticos em forçar o crescimento, mudando todo o escopo da política econômica na qual o Estado tem seu papel para estimular o crescimento, passando a ser um agente passivo nesse quesito.

> I have now no doubt whatever that private enterprise, if it had not been prevented by government, could and would long ago have provided the public with a choice of currencies, and those that prevailed in the competition would have been essentially stable in value and would have prevented both excessive stimulation of investment and the consequent periods of contraction[20] (HAYEK,1990, p.14).

Para Hayek a desejada estabilidade monetária se daria não eliminando totalmente o papel do governo e do banco central, mas dando concorrência em um monopólio totalmente inquestionável pelos economistas, levando a uma eficiência que seria precificada na estabilidade da moeda.

Hayek considera a inflação algo prejudicial para qualquer economia ao atingir o mercado financeiro mudando as rentabilidades e custos dos ofertantes e tomadores de empréstimos,

[19] Tão logo como se consegue libertar-se do universalmente, mas tacitamente credo aceito que um país deve ser fornecido por seu governo com sua própria moeda distinta e exclusiva, todos os tipos de questões interessantes surgem, que nunca foram examinadas. O resultado foi uma incursão em um campo totalmente inexplorado. Tradução feita pela Autor

[20] Eu não tenho dúvidas de que essa empresa privada, se não tivesse sido impedida pelo governo, poderia e teria há muito tempo proporcionado ao público uma escolha de moedas, e as que prevaleceram na competição teriam sido essencialmente estáveis em valor e impediram a estimulação excessiva do investimento e os consequentes períodos de contração. Tradução feita pelo Autor

além de gerar difíceis previsões para preços futuros que equilibrem o mercado naquele que seria o mais próximo do ponto ótimo para a economia. Para Hayek:

> If the value of money .is so regulated that an appropriate average of prices is kept constant . . . the unpredictability of particular future prices, inevitable in a functioning market economy, remains, [but] the fairly high long-run chances are that for people in general the effects of the unforeseen price changes will just about cancel out[21](HAYEK,1976,p.20).

Entrando em um cenário hipotético de extrema liberdade política, Hayek traz o que seria um mercado de moedas privadas, e que se encaixa perfeitamente no desenho futuro das criptomoedas. Esse mercado suposto por Hayek não teria controle cambial ou regulação do seu fluxo, significando um aumento no nível competitivo da moeda como produto em um cenário de competição internacional, ou seja, se um emissor de moeda conduziu sua administração de forma mais eficiente ele entraria competindo em mercados estrangeiros, obrigando aos concorrentes locais, entre eles o governo, a conduzir sua política econômica e fiscal de forma mais responsável para que assim consiga competir com a moeda estrangeira.

No Mercado atual de criptomoedas há hoje várias concorrentes disputando a liderança desse novo segmento. O Bitcoin ainda é a grande moeda, a mais visível na mídia, porem outras concorrentes estão chegando mais perto, como o Ripple, que hoje custa em média 2 dólares, mas que se flutuar para 8 dólares passará o Bitcoin. Outras moedas também estão crescendo, como Ethereum e Eos. Essas moedas passaram por grandes testes antes de crescerem, assim como firmas, e muitas outras não conseguiram se sustentar.

O ponto interessante aqui é considerar cada criptomoedas aqui como uma firma, competindo em um mercado extremamente competitivo, já que a informação é farta e há livre acesso de entrada nesse mercado. Do ponto de vista microeconômico a defesa das moedas privadas poderia se dar com a defesa de que sua estabilidade significaria um preço de concorrência, pois aquelas ineficientes sairão logo do mercado se não se ajustarem em relação à estabilidade. Para Hayek:

> Competition would certainly prove a more effective constraint, forcing the issuing institutions to keep the value of their currency constant (in terms of a stated collection of commodities), than would any obligation to redeem the

[21] Se o valor da moeda é tão regulado que uma média apropriada dos preços é mantida constante... a imprevisibilidade dos preços futuros, inevitáveis em uma economia funcionando, permanece, [porém] as chances no grande longo termo são que pessoas em geral o efeito do imprevisto nos preços irá simplesmente cancelar essa expectativa. Tradução feita pelo Autor.

> currency in those commodities (or in gold). And it would be an infinitely cheaper method than the accumulation and the storing of valuable materials [22] (HAYEK,1974, p.48).

Essa estabilidade se dará no longo prazo, pois para a atualidade falar em estabilidade parece utópico. A volatilidade das criptomoedas está diretamente associada a especulações sobre sua regulamentação, ou seja, algo no momento imediato.

Ao se considerar no longo prazo uma consolidação institucional virá e assim dentro das flutuações naturais dos mercados as criptomoedas irão ter seu lugar. Esse nascimento e criação de mercado é algo que o próprio Hayek considerou em sua obra. Para Hayek quando o sistema se estabelecer por completo, a competição iria resultar em algumas dessas moedas como dominantes, excluindo outras menos eficientes:

> I believe that, once the system had fully established itself and competition had eliminated a number of unsuccessful ventures, there would remain in the free world several extensively used and very similar currencies. In various large regions, one or two of them would be dominant, but these regions would have no sharp or constant boundaries, and the use of the currencies dominant in them would overlap in broad and fluctuating border districts. Most of these currencies, based on similar collections of commodities, would in the short run fluctuate very little in terms of one another, probably much less than the currencies of the most stable countries today, yet somewhat more than currencies based on a true gold standard[23](HAYEK,1974, p.48).

Hayek define que uma moeda privada deveria oferecer estabilidade para uma determinada cesta de bens, como ovos e carnes por exemplo. Essa moeda teria relativa estabilidade para oferecer aos seus portadores a mesma quantidade desses produtos. Essa garantia se daria através de ativos do emissor da moeda, logrando confiança para os usuários da moeda.

2.1.2 O Teorema da regressão de Mises

Heinrich Edler Von Mises foi um dos principais autores da escola austríaca econômica. Mises foi um dos principais autores da escola austríaca econômica com ideais característicos de sua

[22] Uma competição iria certamente se provar uma forma mais eficiente de limitação, forçando as instituições problemáticas a manter o valor de sua moeda constante (em termos a uma coleção de commodities), do que iria qualquer obrigação para resgatar a moeda nessas commodities (ou em ouro). E isso iria ser infinitamente um método mais barato do que a acumulação e venda e materiais valiosos. Tradução feita pelo autor.

[23] Eu acredito que, uma vez que o sistema estiver em plena operação e que a competição já tenha eliminado uma quantidade de empreendimentos, então restaria no mundo de concorrência mundial algumas moedas muito usadas e similares. Em várias regiões grandes, uma ou duas delas seria a dominante, porem essas regiões não teriam limites visíveis, e o uso das moedas dominantes superaria as fronteiras locais. A maioria dessas moedas, baseadas em uma similar cesta de commodities, iriam no curto prazo flutuarem muito pouco em relação a outras parecidas, provavelmente menos que moedas da maioria dos países mais estáveis atuais, ainda mais que moedas baseadas no padrão ouro. Tradução feita pelo autor.

corrente de pensamento como a liberdade econômica, a praxeologia e a defesa do capitalismo. Em 1912, na publicação do livro "*teoria do dinheiro e do crédito*" Mises traz a discussão sobre como a moeda podia sim ter utilidade marginal, pois até o momento, a teoria neoclássica trazia uma circularidade na função utilidade da moeda, no sentido que a utilidade da moeda seria os bens que a moeda é capaz de comprar, porém como esses bens são tidos como referência a moeda corrente, então assim se formava assim uma situação de reposta insatisfatória. Porém, se todos esses bens são valorados em termos de dinheiro, e o dinheiro é valorado em termos desses bens, tem-se aí, claramente, um argumento circular – diziam (DAVIDSON; BLOCK, 2017, p.87).

A resposta de Mises a essa situação foi inserir na análise monetária o elemento temporal, ou seja, o tempo. A utilidade do dinheiro tem então relação com o tempo passado, presente e futuro. *The money-prices of today are linked with those of yesterday and before, and with those of to-morrow and after* (MISES, 1953, p. 109)[24]. Com esse pensamento então existiria um ponto de partida, ou ponto zero, no qual se pudesse traçar o caminho pelo qual o dinheiro se consolidou, trazendo um elemento de sustentação histórica, no qual o desenvolvimento do dinheiro poderia ser comparado com o desenvolvimento do mercado. Se retrocedermos o suficiente, chegaremos a um ponto no qual o dinheiro emerge pela primeira vez como um meio de troca no contexto de uma economia de troca pura (DAVIDSON; BLOCK, 2017, p.87).

O entendimento de Mises sobre como uma moeda se desenvolve através do tempo pode ser trazido para a discussão sobre criptomoedas, pois ele acredita que antes de alguma coisa ser aceita como moeda ela deve ter um valor de troca baseado em outra coisa que não apenas sua função monetária. *Before an economic good Begins to function as money it must already possess exchange-value based on some other cause than its monetary function*" (MISES, 1953, p. 111). Isso significa que uma moeda não surge já aceita como um meio de pagamento universal e inquestionável, primeiro uma moeda surge com uma função diferente, como é o caso das criptomoedas em certa medida, pois muitos não as consideram como moedas, mas sim como títulos, ou seja, representações criptografadas de moedas nacionais. Um exemplo de produtos que viraram moedas foram minerais preciosos, como a prata, que era usada em

[24] O preço do dinheiro de hoje é conectado com o de ontem e anteontem, e também com os de amanhã e depois de amanhã. Tradução feita pela Autor.

alguns objetos, como talheres. *Gold for example was valued for its intrinsic beauty and scarcity*[10] (MURPHY, 2003).

É amplamente discutido que as criptomoedas não são, nesse momento, moedas puramente ditas, porém como Mises fundamenta é possível, sim, que venha a se tornar um meio de pagamento aceito, pois nenhuma moeda é criada e usada instantaneamente. As moedas nacionais antes eram fundamentas em ouro, material que no começo de sua mineração não era uma moeda, e que passou a ter valor e se transformou em moeda pela sua raridade.

As criptomoedas são comercializadas em todo o mundo por possuírem características muito mais próximas as características de circulação como moeda, ou seja, se considerarmos que elas não sejam de fato moedas, elas tem características que permitem que essa transformação no futuro seja possível, já que as criptomoedas possuem alta liquidez, podendo ser convertidas em moedas nacionais a qualquer momento, e também possuem a possibilidade de conveniência a seus portadores, no sentido de que o dono da moeda pode mantê-la como bem entender, podendo guardá-las como um arquivo ou manter em uma carteira online, além de poder realizar transações com qualquer pessoa no mundo a qualquer momento.

2.2 *BLOCKCHAIN* E COASE

A organização industrial traz em um dos seus maiores autores, Ronald Coase, uma contribuição importante para o entendimento da aplicação das criptomoedas como algo benéfico para a economia como um todo. Dentro da teoria da organização industrial há vastos trabalhos sobre os custos de transação, que seria no modo mais simplificado, os custos dos agentes em participar de determinado mercado. Ronald Coase define custos de transações como:

> In order to carry out a market transaction it is necessary to discover who it is that one wishes to deal with, to inform people that one wishes to deal and on what terms, to conduct negotiations leading up to a bargain, to draw up the contract, to undertake the inspection needed to make sure that the terms of the contract are being observed, and so on. These operations are often extremely costly, sufficiently costly at any rate to prevent many transactions that would be carried

> out in a world in which the pricing system worked without cost[25] (COASE.1960. p.15).

A possibilidade de transações praticamente instantâneas, transparentes e globais, traz a tecnologia das criptomoedas uma aplicação em que os custos de transações podem ser reduzidos consideravelmente, resultando em uma cadeia global produtiva maior. A tecnologia por trás do Ethereum permite que se faça contratos inteligentes, ou seja, se em determinado momento as condições de ambas as partes sejam satisfeitas, o contrato será realizado e a transferência monetária será executada, diminuindo os custos da execução desses contratos pois a rede Ether irá executar.

Com as criptomoedas, a revolução trouxe um novo modo de interação agora também na esfera econômica, no sentido de transações de um mundo interligado. Hoje há a possibilidade da execução de uma ordem de compra, com o preço definido por um comprador, por exemplo de um componente de informática, em que o vendedor, que pode ser de qualquer lugar do mundo, ao se deparar com o preço proposto e consequentemente aceitar, haverá ali uma transação em que o único intermediário é a *blockchain* de determinada moeda. Isso significa que os custos efetivos de ambos se reduzirão pois menos instituições farão parte do processo.

Para o corpo teórico da organização industrial os custos de transações são um ponto fundamental para a existência e sucesso de uma firma em um mercado competitivo. Os custos de transações estão profundamente ligados a eficiência, e criação das firmas nos mercados em que elas estão inseridas, sendo os custos de transações o ônus sobre a incerteza entre os agentes do mercado, resultando na necessidade de contratos para realizar a segurança própria dos agentes do mercado. Para Coase a necessidade das firmas se dá pela incerteza no mercado que não permita os agentes transacionarem entre si:

> A firm is likely to emerge in those cases where a very short term contract would be unsatisfactory {…} The operation of a market costs something and by forming an organization and allowing some authority to direct resources, certain marketing costs are saved[26].” (COASE,1937, p. 392)

---

[25] Em ordem para manter uma transação de mercado é necessário descobrir com quem se deseja negociar, para informar a população que alguém deseja negociar e em quais termos, para assim conduzi negociações vantajosas, para se elaborar o contrato, para diminuir a inspeção necessária para se ter certeza que os termos dos contratos estão sendo observados, e assim por diante. Essas operações são extremamente custosas, suficientemente custosas a qualquer classificação para que se previna que muitas transações que seriam carregadas em um mundo em que o sistema de preços funcionaria sem qualquer custo. Tradução feita pelo Autor.

[26] É provável que uma firma surja nesses casos onde um contrato de curtíssimo prazo seria insatisfatório {...} a operação dos custos de transações formando uma organização, e permitindo algumas autoridades para direcionar recurso, certamente custos de marketing não seriam reduzidos. Tradução feita pelo autor.

A questão dos custos de transações foi uma das grandes preocupações que o criador do Bitcoin, Satoshi Nakamoto, teve ao criar seu sistema de *Blockchain*. Para ele a dependência de Instituições financeiras como intermediários aumenta o custo geral das transações, além de inibir devido ao alto custo as transações com menor valor. *The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions*[27] (NAKAMOTO,2008, p. 1).

Assim como Coase, Nakamoto associa a existência dos custos de transação a forma de organização dos mercados, gerando incertezas, no sentido do que o outro agente pode fazer. Nakamoto acredita que os custos elevados na internet são resultado da possibilidade em se reverter uma transação, ou seja, o pagador acionar o intermediário para que o pagamento não seja realizado.

As consequências desse modo de realização de transações financeiras é que a pessoa que recebe o pagamento fica mais criteriosa, exigindo mais informações sobre seus clientes, e consequentemente excluído outros que ele considera que pode trazer algum prejuízo a sua atividade. Para Nakamoto:

> …and there is a broader cost in the loss of ability to make non-reversible payments for nonreversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable[28] (NAKAMOTO,2008, p.1).

A ideia de Nakomoto ao criar a rede Blockchain vai de encontro a teoria de Coase, no entendimento de que os custos de transação interferem negativamente na economia, alterando o comportamento dos agentes do mercado ao ter a necessidade de se confiar em um intermediário. Uma mudança nesse modo de fazer transações teria vantagens para os vendedores sem deixar o consumidor sem nenhum tipo de proteção

Na prática ainda existiriam ainda contratos a serem respeitados, porém sem a necessidade fundamental de um agente especifico que o provenha, que é o intermediário, podendo passar a ser algo desenvolvido pelo vendedor ou então seguindo as regras vigentes de comércio.

---

[27] O custo da mediação aumenta os custos de transação, limitando o tamanho mínimo praticado e cortando a possibilidade de pequenas transações casuais. Tradução feita pelo Autor

[28] e há um custo mais amplo na perda da capacidade de efetuar pagamentos não reversíveis para serviços não reversíveis. Com a possibilidade de reversão, a necessidade de confiança se espalha. Os comerciantes desconfiam de seus clientes, incomodando-os por mais informações do que precisariam de outra forma. Uma certa porcentagem de fraude é aceita como inevitável. Tradução feita pelo Autor.

> 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 [29](NAKAMOTO,2008, p.1).

Para Davidson, De Filippi e Potts, segundo a teoria Neo Institucional feita por Coase, a rede *Blockchain* seria capaz de moldar uma nova economia, realizada pelos agentes econômicos que irão buscar estabelecer novas formas de operacionalização, nas quais os custos de transação seriam menores. Os agentes que usarem primeiro essa tecnologia teriam a capacidade de redesenhar a estrutura do mercado, interferindo diretamente em como as instituições passariam a exercer seu papel social, resultando assim para um novo modo vigente que irá se disseminar pela sociedade.

> and therefore, the efficient mix of institutions in an economy will be shaped by agent seeking to economize on transactions costs. Economizing on production costs leads to an efficient allocation of resources and economizing on transactions costs leads to an efficient institutional structure of economic organization and governance[30](DAVIDOSN; DE FILIPPI; POTTS,2016, p.9).

As formas tradicionais de relações econômicas que existem em nossa sociedade são das mais diversas formas amparadas pela proteção institucional do Estado. Isso é causado pela incerteza que sempre existiu nas formas como os agentes econômicos realizam suas transações. Sobre essa forma tradicional existe a formação institucional que faz o papel de resguardo para todas essas situações, que vão das mais simples situações corriqueiras até grandes contratos. A rede *Blockchain* tem a capacidade de interferir no funcionamento dessas instituições tradicionais através do ganho de produtividade em todos os setores, inclusive o setor público.

Para Coase o Estado é uma firma, de forma muito especial, mas é uma firma. *The government is, in a sense, a super-firm (but of a very special kind) since it is able to influence the use of*

[29] O que é necessário é um sistema de pagamentos eletrônicos baseado em criptografia ao invés de confiança, permitindo para as duas partes realizar a transação diretamente com o outro sem a necessidade de uma terceira parte. Transações eletrônicas que são impossíveis de se reverter iriam proteger os vendedores de fraudes, e mecanismos de rotina poderiam ser facilmente criados para proteger os compradores. Tradução feita pela Autor.

[30] e, portanto, a mistura eficiente de instituições em uma economia será moldada pelos agentes que buscam economizar custos de transação. Economizar nos custos de produção leva a uma alocação eficiente de recursos e a economia nos custos de transação leva a uma estrutura institucional eficiente de organização econômica e governamental. Tradução feita pela Autor.

factors of production by administrative decision[31] (COASE,1960, p.17). O Governo ser uma firma significa que, de forma especial, ela muda devido a ganhos de produtividade, ou seja, o Governo muda se o ganho de produtividade aumenta. Um exemplo disso é o uso dos Governos, em todo mundo, de cada vez mais tecnologia aplicada para suas funções essenciais, indo de simples fiscalizações até questões tributárias como o imposto de renda. Se considerarmos que a internet se popularizou na virada do século, ou seja, tem apenas 19 anos, e sua importância hoje para a administração pública é essencial.

A rede *Blockchain* poderá oferecer mudanças além do viés financeiro, impactando também o judiciário ao permitir que contratos possam ser executados sem a necessidade de atuação do Estado. Isso por que a execução de contratos automáticos, que são aqueles que estarão confeccionados na rede *Blockchain*, de forma que uma ação leva a outra de forma automática, pode mudar a forma como grandes Instituições lidem com seus clientes, como por exemplo em um caso de devolução do valor da passagem quando um avião de uma companhia área não decola. Se houver um contrato via *blockchain*, onde um simples reconhecimento de que o avião não realizou aquela viagem, o passageiro receberá de volta seu dinheiro, sem nenhum tipo de interferência, seja pelo seguro de voo ou em outros casos via judiciário.

A teoria dos custos de transação de Ronald Coase traz como ponto principal a importância dos custos existes no mercado e como estes moldam as instituições. Com base em Coase, é possível associar que há fundamento em uma mudança desse *modus operandi* devido aos ganhos de produtividade proporcionado pela rede *Blockchain*, indo muito além dos ganhos apenas na velocidade das transações financeiras. Já existem estudos de aplicações da rede nas mais diversas áreas, que vão de processos eleitorais até setores de logística. Se de fato ocorrer mudanças no espectro institucional devido a ganhos de produtividade, como Coase defende, a rede *Blockchain* irá sim causar significativas mudanças estruturais tanto na sociedade quanto nas instituições privadas e também públicas.

[31] O governo é, de certa forma, uma super firma (mas de um modo especial) desde que é influenciada pelo uso de fatores de produtividade por decisão adminstrativa. Tradução feita pelo Autor

3 *BLOCKCHAIN* E BITCOIN

A maior revolução que Bitcoin trouxe foi a criação de um livro-registro aberto e imutável, na qual sua escrita é feita por vários indivíduos através do consenso. Isso significa dizer que o registro de informações contábeis passa a ser realizados através de informações dispersas, e que são compiladas por poder computacional que pode estar em qualquer lugar no mundo. Se for verificado que as informações são verdadeiras por vários usuários da rede, a transação é feita pois se chegou ao consenso. Basicamente a ideia por traz de uma rede *blockchain* é fazer com uma mesma transação seja verificada por inúmeras pessoas diferentes, sem nenhuma comunicação possível, já que não há identificação pela rede, resultando em códigos decifrados comuns. É nesse sistema que as moedas virtuais são baseadas, sendo a maior o Bitcoin, que foi a primeira moeda baseada em *blockchain* criada, e o Ethereum, segunda maior criptomoeda e que tem uma concepção mais diversificada, saindo apenas da lógica financeira de transferência e tendo em seu código a possibilidade de realização de contratos inteligentes.

Mas afinal qual a definição de moeda eletrônica? Para o criador do Bitcoin, Satoshi Nakamoto, a definição de moeda digital é: *We define an electronic coin as a chain of digital signatures*[32](NAKAMOTO,2008, p,2). Essa resposta aparentemente simples de Nakamoto tem diversos significados, porém sua frase revela alguns significados até mesmo sobre as moedas comuns, feitas pelo Estado. O termo assinaturas que Sakamoto usa se refere as confirmações necessárias para que uma transação na rede *Blockchain* seja realizada com sucesso, porém é possível associar assinaturas também nas moedas como o Dólar e Real.

Toda cédula para ser considerada verdadeira necessita de elementos que provam sua autenticidade, como marcas d'água e imagens ocultas no caso do Real. A assinatura presente na moeda digital e também na tradicional são confirmações de que aquela moeda é de fato verdadeira. O que muda de uma moeda eletrônica para uma emitida pelo Governo é que na moeda eletrônica as assinaturas presentes nas verificações são feitas por inúmeras pessoas anônimas, contra a assinatura única do Estado nas moedas tradicionais.

[32] Nós definimos uma moeda eletrônica como uma cadeia de assinaturas digitais. Tradução feita pelo Autor

A existência de moedas que tem valor assegurado por diversas pessoas ao redor do globo, que executam as verificações de forma anônima é mais que uma simples forma nova de transação eletrônica, é uma mudança revolucionária. É irônico pensar que uma pizza ou um café comprado com Bitcoin ou outra criptomoeda possa ter sido validade graças ao esforço para suportar a rede de um japonês ou de um Chinês. Ao permitir que o esforço de pessoas comuns, via poder de computação empregado por elas consiga validar transações e gerar moeda, uma nova situação foi criada. Agora O Estado não é mais o único provedor e autenticador da moeda que a sociedade pode usar, o que resulta em uma mudança na forma de como uma pessoa pode entender o papel da moeda, ou seja, se as criptomoedas tomarem o espaço da moeda convencional, o papel do cidadão não será apenas de um espectador passivo quando se trata de moeda e política monetária.

Esse novo modo de relação monetária onde o cidadão possui de fato a moeda, diferente da concessão que o Estado dá aos usuários. Uma prova disso é que é no Brasil rasgar dinheiro é um ato ilegal, já que o dinheiro não pertence ao indivíduo que o possui, sendo o que seria uma espécie de dano a algo “alugado”. O bitcoin pelo contrário pode ser destruído sem nenhuma preocupação na infração de leis, basta apenas apagar o seu código e está feito, seus bits serão excluídos e não é possível sua recuperação. Satoshi Nakamoto fez um sistema no qual o termo privado passou então a ter dois sentidos, que são a emissão por pessoas e também o direito de propriedade sobre o que foi emitido, indo contra o modelo atual onde o Estado emite a moeda e mesmo após nas mãos da sociedade todo o dinheiro ainda o pertence, tirando o espirito “livre” necessário aos indivíduos em todas a sociedades.

3.1 *BLOCKCHAIN*

A *Blockchain* é a tecnologia por trás de todas as criptomoedas e que serve como base para que a alta movimentação dos recursos seja feita de forma rápida, segura e transparente, pois qualquer um com acesso a rede consegue ver o registro de todas as transações feitas pela rede de transações das criptomoedas. A *Blockchain* é um livro-razão aberto e imutável no qual as informações ali são escritas após a verificação dos dados por meio da criptografia das informações dadas pela rede. A *Blockchain* é uma espécie de livro aberto que registra todas as

operações que ocorrem em uma rede criptografada, tendo a finalidade de manter a segurança e autenticidade das transações. *Any transaction attribute or information on the agents and goods involved that is stored on a distributed ledger can be cheaply verified, in real time, by market participants*[33](CATALANI; GANS,2016, p. 8).

As transações dentro de uma rede *Blockchain* são agrupadas em blocos, que são disponibilizados para sua rede. São esses blocos que dão nome a essa rede, é uma corrente de blocos, ligadas entre elos, nas quais os blocos são informações de transações agrupadas. A partir do momento que o bloco é "quebrado", outro novo é lançado na rede para ser minerado, que é o processo computacional de descriptografar as informações das transações. Aqueles que conseguirem fazer esse processo será recompensado pela rede com sua moeda, como o Bitcoin, Ethereum e Litecoin. Cada moeda tem seu valor de mercado associado a dificuldade de se obter as informações que a *Blockchain* quer e as expectativas de mercado sobre o futuro uso da rede *Blockchain* nas mais diversas aplicações. De modo simplificado, a ideia é a de que toda criptomoeda reivindicada por um usuário está atrelada a sua identidade, a qual é criptografada por meio de uma sequência alfanumérica aleatória, de modo que somente o usuário pode decodificá-la (CARVALHO,2017, p. 8).

A rede *Blockchain* é, trazendo na forma literal, uma corrente de blocos criptografados. O termo corrente é utilizado por que cada elo está ligado a um antecessor e um sucessor. Cada elo dessa corrente é maior que o anterior pois ele contém todas as informações dele somado com informação momentânea, ou seja, para validar uma transação, independentemente de sua posição cronológica, todas as anteriores serão também processadas, algumas de forma integral e outras de parcial, para que sua validação tenha sucesso.

> Blockchain clearing and settlement could be conducted in very near real time. It is based on a fintech first applied by the Bitcoin virtual currency. The name refers to a chain of data blocs that include the entire history of origin of payments made for securities, goods or other assets[34](CAYTAS,2016, p.4).

[33] Qualquer atributo de transação ou informação sobre os agentes e mercadorias envolvidos que são armazenados em um livro-razão distribuído pode ser verificada de forma barata, em tempo real, pelos participantes do mercado. Tradução feita pelo Autor

[34] A compensação e a liquidação do *blockchain* podem ser realizadas em tempo quase real. Isso é baseado em uma *fintech* aplicada pela moeda virtual do Bitcoin. O nome refere-se a uma cadeia de blocos de dados que inclui todo o histórico de origem dos pagamentos feitos para títulos, bens ou outros ativos. Tradução feita pelo Autor

A técnica matemática que permite o funcionamento das redes *Blockchain* é a criptografia. Essa técnica é usada há bastante tempo com a finalidade de preservar o conteúdo de informações na qual o seu conteúdo não pode ser exposto. Um exemplo simples de criptografia seria criptografar a palavra "casa" usando a letra posterior do alfabeto, ficando então "dbtb", fazendo então com que a pessoa que recebeu essa mensagem só saiba entender o conteúdo sabendo a regra criptográfica ou tentando fazer o caminho inverso, descriptografando pelo método de tentativa e erro. Com o poder computacional que existe hoje em dia a criptografia avançou muito, tendo diversas maneiras possíveis de combinação para criptografar, com logaritmos complexos sendo exigidos para se manter a segurança das informações na internet.

A criptografia é uma técnica essencialmente de defesa, com a finalidade de preservar que as informações não caiam nas mãos de inimigos. Se alguém deseja interceptar uma mensagem criptografa haverá a necessidade de um grande esforço para que se consiga entender o código de criptografia usado e assim descriptografar aquela mensagem, enquanto para se defender e proteger uma mensagem o esforço necessário é muito menor, já que é necessário apenas escolher uma código para transformar sua mensagem. Para Bashir a criptografia é a ciência de fazer informações seguras:

> Cryptography is the Science of making information secure in the presence of adversaries. It provides a means of secure communication in the presence of adversaries with assumed limitless resources. Ciphers are used to encrypt data so that if intercepted by an adversary, the data is meaningless to them without decryption, which requires the secret key[35] (BASHIR,2017p.51).

Com a criptografia a rede *Blockchain* consegue algo no mínimo irônico, mostrar a toda internet um código que tem valor financeiro, mas que ninguém consegue usá-lo, já que para conseguir decifra-lo seria necessária uma invasão na rede e também refazer todo o histórico de transações até o momento da transação atual. A ciência da criptografia permite a rede *Blockchain* a base para essa exposição pública porque tem elementos para prover formas de confiança daquelas informações. *Cryptography provides various security services, such as Confidentiality, Integrity, Authentication, (entity Authentication and Data origin*

[35] A criptografia é a ciência de fazer a informação segura na presença de adversários. Ela fornece um meio de comunicação segura na presença de adversários com recursos supostamente ilimitados. Cifras são usadas para criptografar dados de modo que, se interceptadas por um adversário, os dados não tenham sentido para eles sem descriptografação, o que requer a chave secreta. Tradução feita pelo Autor.

authentication) and non-repudiation. Additionally, accountability and also required in various security systems[36] (BASHIR,2017, p.51).

A ideia inicial de Satoshi Nakamoto ao criar a rede *Blockchain* era permitir um sistema seguro e que impedisse o problema do *double spending*, que é quando uma mensagem criptografada é contabilizada duas vezes, ou seja, quando há uma duplicação na criação da criptomoeda. Uma maneira fácil de exemplificar o que é um pagamento duplo é imaginar um boleto, porém recebendo o dinheiro em vez de enviar para o pagamento de alguma conta. Um boleto pode ser repetido *n* vezes, ou seja, é possível se pagar a mesma conta infinitas vezes, já que seu sistema não tem um controle anterior sobre as transações realizadas. Quando ocorre um erro desse tipo na rede de boletos o receptor do pagamento pode perceber ao notar uma entrada dupla de mesmo valor na conta bancaria e assim e reembolsar quem enviou, porem algumas vezes é necessário que o pagador tenha em mãos um comprovante daquela transferência para que seja regularizada a situação. O grande ponto aqui é que no momento de inserir o código de barra não há uma verificação na transação se aquele código já foi inserido antes, somente depois haverá uma compensação. Se pensarmos o código de barras do boleto como uma transação financeira de uma moeda virtual, o código poderia ser repetido, tirando assim a confiança no sistema.

Em um sistema de pagamentos de Boletos com uma rede *Blockchain* o primeiro pagamento seria aprovado, mas os subsequentes não teriam nenhum valor. Um sistema de pagamentos com erros de *double spending* como esse seria inviável, e essa é a razão de não existir sistemas assim antes do Bitcoin. A solução de Satoshi Nakamoto soluciona o problema ao não permitir que o receptor da transação pudesse replicar o código infinitamente. Se analisarmos as transações online, é possível verificar que já existiam vários sistemas que proporcionavam o recebimento pagamentos, porém Nakamoto criou um sistema de transações que fosse possível enviar e também receber os pagamentos.

Se no sistema de boletos houvesse uma rede *Blockchain* gerando registros das transações anteriores, o segundo pagamento com o mesmo código de barras não poderia ser efetuado, isso porque haveria um registro na rede que iria informar o momento no qual aquele código

[36] A criptografia fornece vários serviços de segurança, como Confidencialidade, Integridade, Autenticação (Autenticação de entidade e Autenticação de origem de dados) e não repúdio. Além disso, a prestação de contas também necessária em vários sistemas de segurança. Tradução feita pelo Autor.

de barras foi usado. *For our purposes, the earliest transaction is the one that counts, so we don't care about later attempts to double-spend*[37](NAKAMOTO,2008p.2)

O grande poder computacional que a rede *Blockchain* do Bitcoin necessita é efeito direto da necessidade em construir um histórico de transações confiável e aberto, pois tecnicamente falando seria simples construir um sistema de pagamentos com registros fechado, porém para assegurar o fator confiança nas transações foi necessário criar esse livro-contábil extenso, pois se alguém daqui a 100 anos alguém propositadamente guardar o primeiro código da rede e usá-lo em uma nova transação, a rede não irá validar esse transação.

> We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work[38](NAKAMOTO,2008, p.1).

O problema do *double spending* é solucionado pelas características do *Blockchain* quando se analisa de forma cronológica, através do acesso aos dados de todos os participantes da rede, o primeiro código criptografado usado, ou seja, as informações contidas na rede permitem comprovar quando um código foi resgatado, não permitindo assim que uma pessoa burle o sistema de pagamentos e faça quantas replicações do código ela queira.

A ideia por traz da rede pública é a validação dos dados pois não é possível acessar e modificar e acessar todos os registros da rede, o que gera segurança quanto a invasões na rede *Blockchain* das moedas. De modo geral, umas das propriedades importantes dessa rede de dados em que há o registro das transações é que, uma vez gravada, não há possibilidade de alteração *a posterior* (CARVALHO,2017, p. 10), gerando assim um linha temporal que existe na rede e que pode sempre ser acessada por qualquer pessoa, impedindo uma mudança nas transações que ocorreram.

Para conseguir resolver o problema do *double spending* o *Blockchain* utiliza os registros armazenados na rede por vários usuários que as verificam, mas como manter a consistência daquelas informações se são várias pessoas que estão ali fazendo o trabalho de verificar? O problema dos generais bizantinos é algo antigo na computação ao se tratar em sistemas sem

[37] Para nossas intenções, a primeira transação é a que vale, então nós não importamos com as transações posteriores que tentam fazer duplicação. Tradução feita pela Autor

[38] Propomos uma solução para o problema do gasto duplo usando uma rede *peer-to-peer*(pessoa a pessoa) . A rede registra as transações de data e hora, transformando-as em uma cadeia contínua de prova de trabalho baseada em *hash*,, formando um registro que não pode ser alterado sem refazer a prova de trabalho.

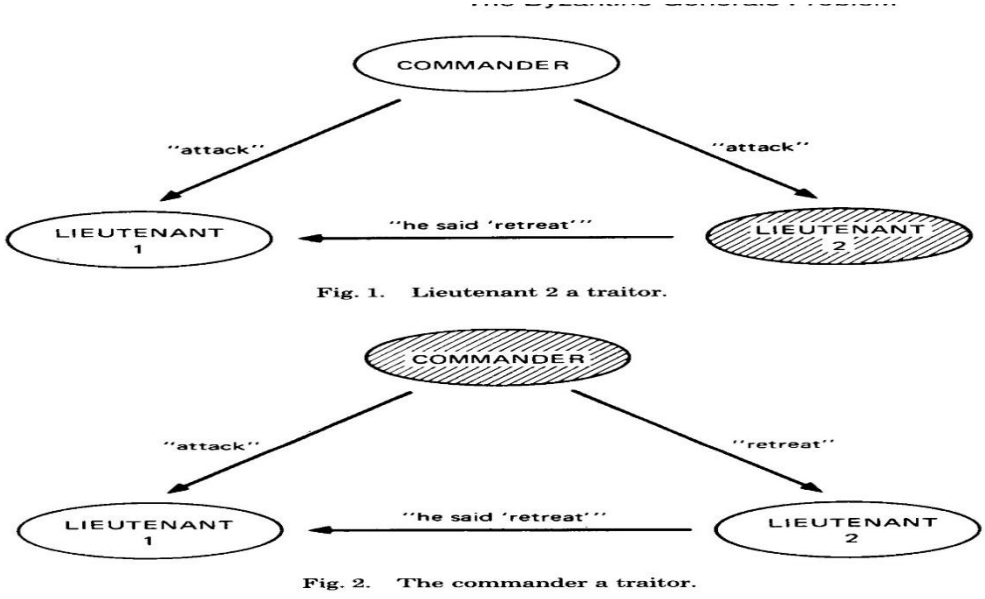
um a gente central, contornando o problema de confiança ao solucionar problemas quando há intenções diferentes pelos agentes daquela rede de informações em passar a informação correta.

Leslie Lamport, Robert Shostak e Marshall Pease trouxeram esse problema relacionado a computação em 1982, sendo que até 2008 na criação do Bitcoin esse problema não foi resolvido de forma satisfatória. Eles definem o problema dos generais como:

> We imagine that several divisions of the Byzantine army are camped outside an enemy city, each division commanded by its own general. The generals can communicate with one another only by messenger. After observing the enemy, they must decide upon a common plan of action. However, some of the generals may be traitors, trying to prevent the loyal generals from reaching agreement.[39](LAMPORT; SHOSTAK; PEASE;1982, p.382).

O problema dos Generais Bizantinos é resultado da possibilidade de que alguns participantes de uma rede possam agir de forma contraria ao objetivo do conjunto. Se um traidor passar a mensagem errada para vários generais e criar uma divisão no ataque, indo alguns grupos e outros não o resultado será a derrota daqueles que foram e também dos que ficaram, pois só seria possível um ataque coordenado. Se um general por exemplo, receber alguma vantagem do rei da cidade a ser invadida, ou o mensageiro for o traidor e que irá levar vantagem, toda a comunicação desse exército será comprometida.

Figura 1- Problema dos Generais Bizantinos



Fonte: LAMPORT; SHOSTAK; PEASE,1982, p.385

[39] Nós imaginamos que várias divisões do exército bizantino estão acampadas do lado de fora de uma cidade inimiga, sendo cada divisão comandada por seu próprio general. Os generais podem se comunicar uns com os outros apenas por mensageiro. Depois de observar o inimigo, eles devem decidir sobre um plano de ação comum. No entanto, alguns dos generais podem ser traidores, tentando impedir que os generais leais cheguem a um acordo. Tradução feita pela Autor

A questão da confiança em um sistema de vários participantes como esse parece ser relativamente simples, porém definir a forma de comunicação e como cada participante exerce sobre os outros tem um papel fundamental para o sucesso de qualquer rede em que um agente central tem o poder de decisão sobre os demais. Abaixo é possível verificar como os autores representaram o problema em uma situação simples, com apenas 3 participantes. Na primeira o Tenente 2 é o traidor, passando para o Tenente 1 a informação contraria. No exemplo abaixo o Comandante é o traidor, passando para seus comandados a informação errada.

O problema dos Generais Bizantinos vem com o passar do tempo apresentando algumas respostas não definitivas, e que passam a ser mais trabalhosas e custosas com o aumento do número de participantes. Como os próprios Autores explicam na conclusão do seu artigo, uma solução mais complexa para o problema dos Generais Bizantinos ainda é necessária. *However, when extremely high reliability is required, such assumptions cannot be made, and the full expense of a Byzantine Generals solution is required*[40] (LAMPORT; SHOSTAK; PEASE,1982, p.401)

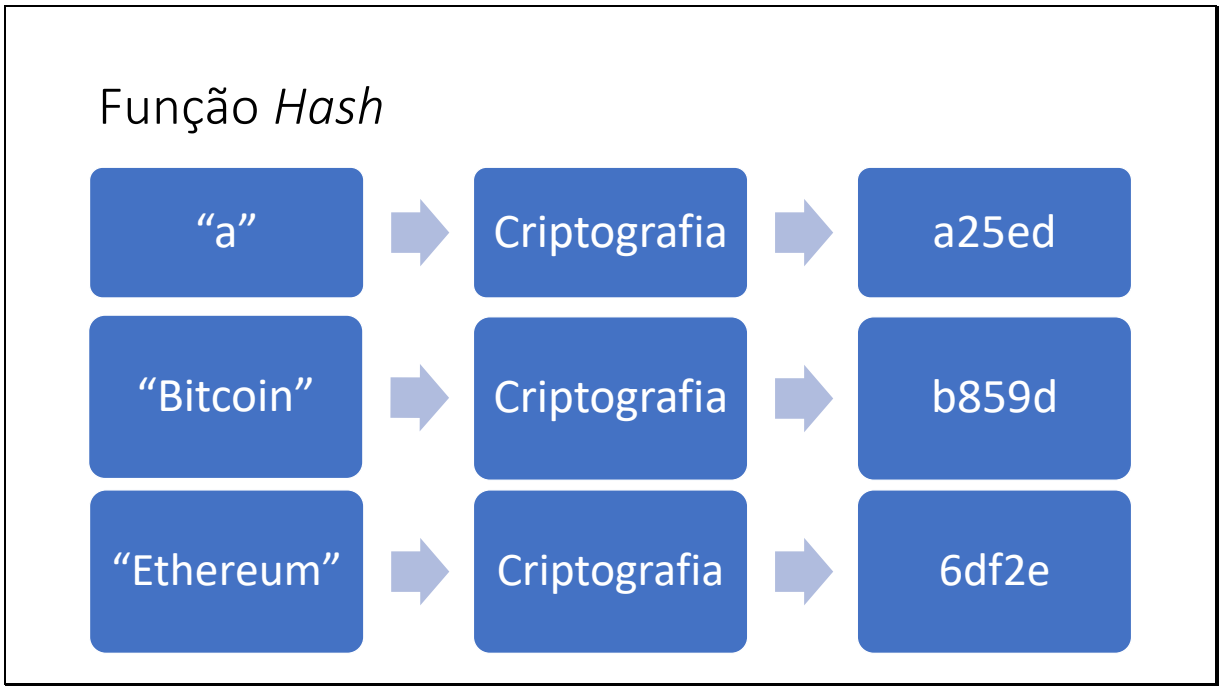
A medida utilizada por Satoshi Nakamoto para criar uma rede de comunicação aberta na qual seus integrantes não fossem capazes de mudar informações e assim afetar a confiabilidade foi a criação do sistema *proof of work*, ou em português prova de trabalho.

Para entender esse sistema é preciso antes algumas noções de programação simples, sendo a primeira o que é *Hash.* Uma função *Hash* é uma técnica criptográfica na qual o resultado de uma codificação terá sempre a mesma quantidade em sua saída, independente da entrada. Se uma letra ou número mudar, o *hash* muda inteiramente.

Vamos supor que o valor definido da função seja 5, se inserirmos para criptografia 1 elemento ou 1000, o resultado criptografado será sempre 5 elementos. Abaixo há uma ilustração simples de como funciona uma função *Hash* ao transformar a entrada na parte esquerda em sempre 5 elementos na parte da direita, após passar por um código criptográfico*:*

[40] Entretanto, se uma solução de alta confiança é requerida, e algumas suposições não podem ser feitas, outra solução para o problema extenso dos Generais Bizantinos é requerida. Tradução feita pelo Autor

Figura 2- Função *Hash*



Fonte: Ilustração feita pela Autor

Na *Blockchain* junto a função *Hash* é adicionado um *nonce*[41], que é um número gerado por um código criptográfico para ir junto com a mensagem desejada, no exemplo dos generais um *nonce* junto com a mensagem seria “atacar quarta Vd7fgda”,a função do *nonce* é que essa mensagem só possa existir uma vez na cadeia de mensagens.

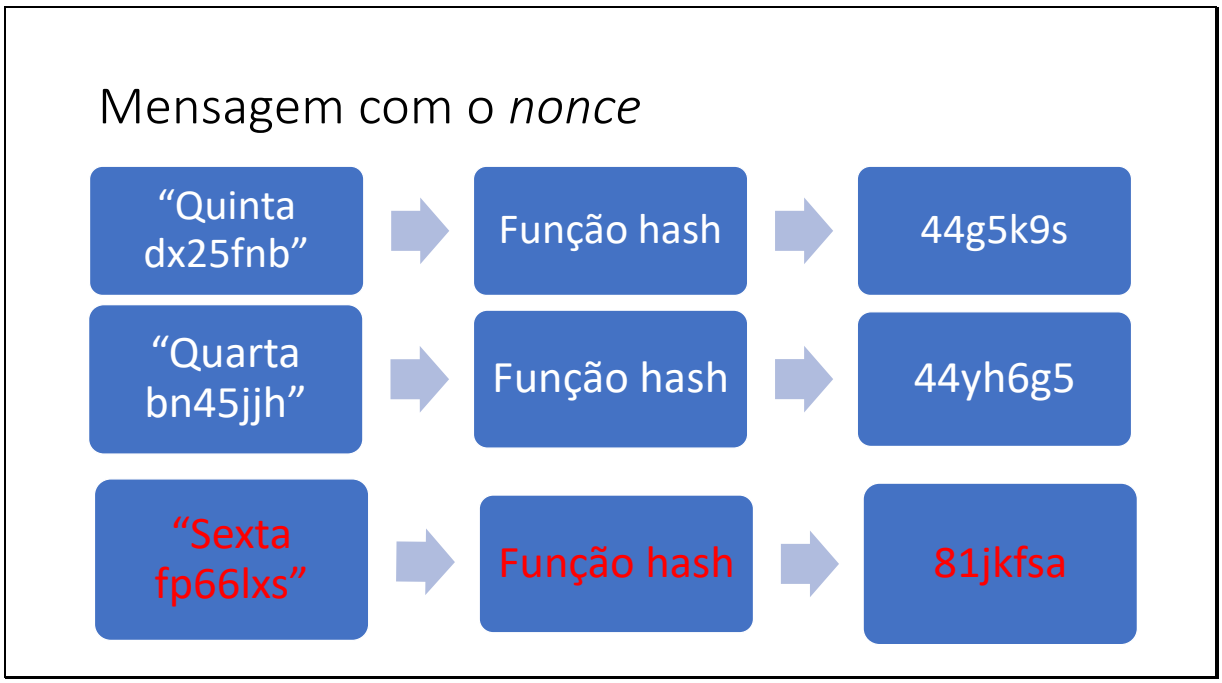
O resultado da função *Hash* ao ser inserido a mensagem com o *nonce* será um código criptográfico que deverá conter características predefinidas dessa rede. Por exemplo o Exército Bizantino pode definir que suas mensagens serão sempre iniciadas por 2 números “4”, ficando sempre a mensagem valida como “44xxxxx”, ou seja, se uma mensagem for inserida na função *Hash* e seu começo for “11xxxxx” essa mensagem não será validada na rede e será considerada falsa.

O grande poder computacional exigido nas redes *Blockchain* é motivado pela necessidade das inúmeras tentativas computacionais para descobrir a solução que combine a transação desejada adicionada ao *nonce* que irá resultar na exigência da rede.

[41] O termo *nonce* é uma expressão em inglês para “*number used only once*”

No quadro abaixo está uma ilustração de como uma mensagem aparentemente verdadeira de seria descoberta pelos outros integrantes do grupo como falsa ao não ter os dois primeiros números “44”, que foi uma hipotética convenção usada pelo Exército.

Figura 3- função *nonce*



Fonte: Ilustração feita pela Autor

Uma solução imaginária para o problema de comunicação entre os generais seria considerar agora que eles têm computadores que possam resolver “*puzzles*”, que na tradução literal são quebra cabeças que os computadores resolvem por tentativa e erro um código criptográfico, o que é chamado de *proof-of-work,* que significa prova de trabalho, já que para conseguir descriptografar o código o único modo possível foi através do trabalho intensivo em fazer tentativas seguidas até conseguir achar o resultado.

A ideia de Nakamoto é que cada general gere uma mensagem com o *nonce*, o que levará tempo pois será um *puzzle* da primeira informação sobre o ataque que ouviu, para que assim uma mensagem seja adicionada a rede. Após o primeiro mandar a mensagem para a rede, os outros trabalharam para mandar sua mensagem adicionada do general anterior, resultando em

uma cadeia na qual todos os generais saberão como os outros irão agir. Em 2008 Nakamoto respondeu em um fórum da internet sua solução:

> They use a proof-of-work chain to solve the problem. Once each general receives whatever attack time he hears first, he sets his computer to solve an extremely difficult proof-of-work problem that includes the attack time in its hash. The proof-of-work is so difficult, it's expected to take 10 minutes of them all working at once before one of them finds a solution. Once one of the generals finds a proof-of-work, he broadcasts it to the network, and everyone changes their current proof-of-work computation to include that proof-of-work in the hash they're working on [42] (NAKAMOTO, 2008).

No Bitcoin é exigido uma certa quantidade de números "0" no começo para que seja considerada válida a mensagem. *The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits* [43] (NAKAMOTO,2008, p.2).

A quantidade de "0" exigida vai depender do estágio da rede, ou seja, quanto mais transações são realizadas maiores serão os "0" exigidos, já que há maiores informações sobres as transações a serem processadas em seu registro histórico, sendo cada bloco é minerado em aproximadamente 10 minutos. Em junho de 2019 são exigidos 19 números "0" para ser considerada válida uma transação.

O processo continuo de verificação de cada bloco, sempre exigindo que a última transação seja verificada cria então um sistema no qual a informação decifrada não pode ser modificada, sempre passando adiante uma informação autentica. Na ilustração do próprio Nakamoto é possível ver que sempre a transação anterior é verificada, gerando segurança para as transações futuras. *Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin*[44] (NAKAMOTO,2008, p.2)

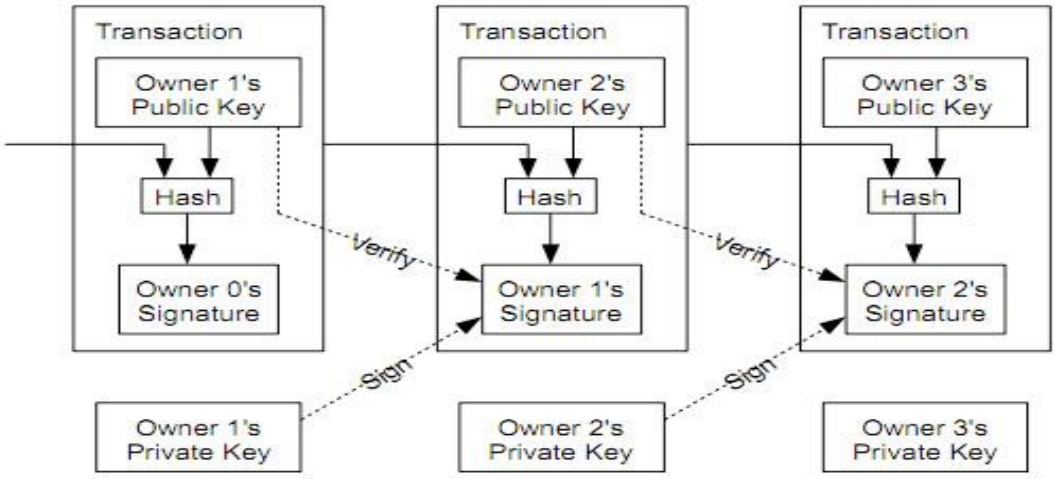
---

[42] Eles usam uma cadeia de prova de trabalho para resolver o problema. Quando cada general recebe o tempo de ataque que ouve primeiro, ele configura seu computador para resolver um problema extremamente difícil de prova de trabalho que inclui o tempo de ataque em seu *hash*. A prova de trabalho é tão difícil, espera-se que leve 10 minutos de todos trabalhando ao mesmo tempo antes que um deles encontre uma solução. Uma vez que um dos generais encontra uma prova de trabalho, ele o transmite para a rede, e todos mudam sua atual comprovação de trabalho para incluir aquela prova de trabalho no hash em que estão trabalhando. Tradução feita pela Autor

[43] A prova de trabalho envolve uma busca por um valor que quando passar pelo *hash*, com o SHA-256(código de criptografia da Blockchain), o *hash* comece com uma determinada quantidade de zeros em seus bits. Tradução feita pelo Autor

[44] Cada proprietário transfere a moeda para o próximo, assinando digitalmente um *hash* da transação anterior e a chave pública do próximo proprietário e adicioná-los ao final da moeda. Tradução feita pela Autor

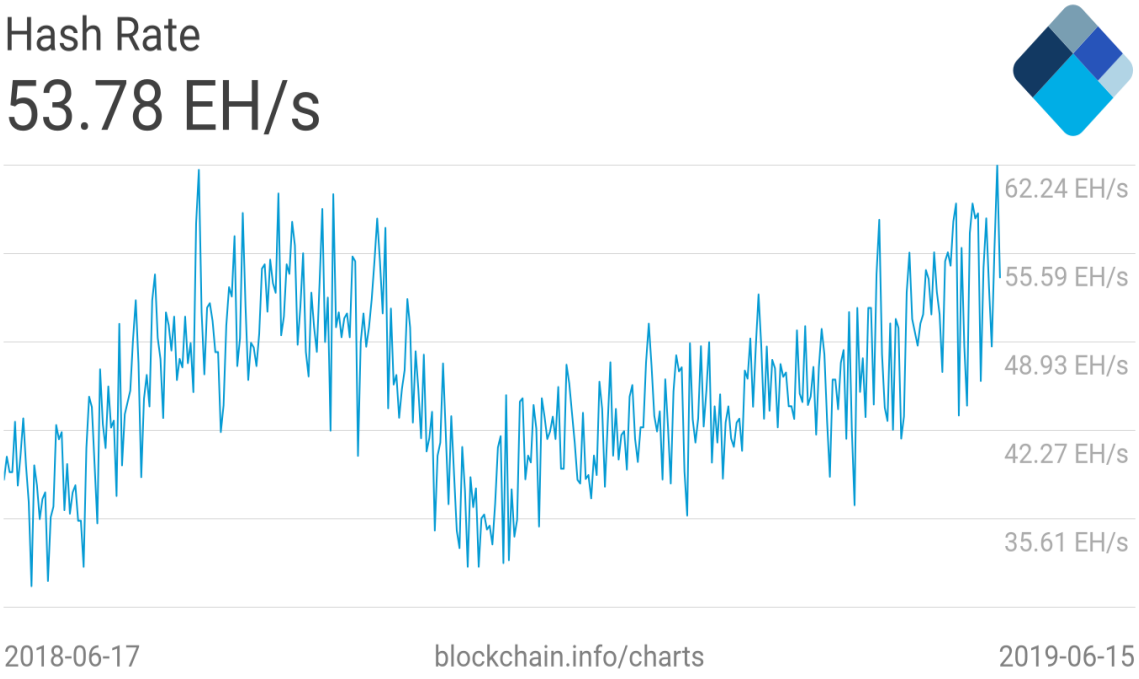
Figura 4-Ilustração de Satoshi Nakamoto sobre a *Blockchain*



Fonte:NAKAMOTO,2008.

Abaixo está a ilustração da evolução da exigência da rede *Blockchain* desde o seu lançamento. O máximo alcançado foi de 62 EH/s em outubro de 2018, o que significa 62 Trilhões de cálculos por segundo tentando fazer o caminho inverso em achar o *nonce* junto ao *hash*, tendo do valor de 53.78 no dia 17 de junho.

Figura 5- *Hash rate* da rede *blockchain*



Fonte:BLOCKCHAIN.COM,2019.

3.2 INSERÇÃO DO BITCOIN NA ECONOMIA

As moedas já eram digitalizadas, no sentido de que existe uma correspondência entre uma unidade de moeda real com uma unidade virtual, porém com altos custos pois depende de um sistema bancário complexo, e por isso sofre para efetuar transferências com maior rapidez.

Uma moeda realmente digital tem seu preço podendo variar na cotação do mercado, ou seja, a modalidade de moeda digitalizada é uma representação contábil, e que por consequência não é capaz de se movimentar rapidamente, pois as barreiras impostas pelas instituições fará com que seja necessário um tempo para a transformação de um tipo de moeda nacional para outro tipo de moeda nacional. Para Schupmann a rede do *Blockchain* muda a forma como a transações são feitas ao se ter um sistema com confiança e sem intermediários.

> The key innovation of blockchain is that it solves the issue of trust. Rather than relying on financial institutions and clearinghouses as intermediaries, blockchain employs sophisticated algorithms that verify the parties and the transaction by harnessing the collective computing power of the computers in the network. Because there is an indelible ledger of all previous transactions within the network, it is possible to track and validate transactions. Cutting out the middleman—or middle*men* as is often the case—vastly simplifies the transaction, while also reducing the cost and time involved[45] (SCHUPMANN,2017, p. 5).

Do ponto de vista econômico o *Blockchain* é um avanço importante em como as transações financeiras poderão passar a ser feitas se adotada essa tecnologia. *While it currently can take five days to fully effectuate a cross-border payment, a blockchain network can accomplish such a payment in ten minutes*[46] (SCHUPMANN,2017, p. 6).

Essa redução pode gerar benefícios a economia mundial, tornando as transações mais rápidas e a menores custos, reduzindo assim os custos de transações nas negociações internacionais, podendo gerar uma nova dinâmica a economia mundial ao se permitir que relações mais diretas e rápidas mudem a forma com que o comercio entre países é feito, no sentido de

[45] A principal inovação do *blockchain* é que resolve o problema de confiança. Em vez de depender de instituições financeiras e câmaras de compensação como intermediários, o *blockchain* emprega algoritmos sofisticados que verificam as partes e as transações acessando o poder computacional coletivo dos computadores da rede. Porque existe um livro-razão indelével de todas as transações anteriores dentro da rede, é então possível rastrear e validar as transações. Cortando o intermediário simplifica consideravelmente as transações, também reduzindo os custos e o tempo envolvido. Tradução feita pelo Autor.

[46] Enquanto atualmente uma transação internacional pode durar 5 dias uma feita pelo *blockchain* pode realizar esse pagamento em 10 minutos. Tradução feita pelo Autor.

sempre ser concentrado a grandes agentes de mercados, tanto na área logística como financeira, como analisam Catalani e Gans:

> The effects of this change have been mostly felt on the intensive margin of production and for digital assets, as established players have moved existing types of transactions onto blockchain-based systems to lower operation costs (CATALANI; GANS,2016, p. 9).

Com a consolidação após mais de uma década desde o seu lançamento, as diversas aplicações nas redes de *Blockchain*s atraiu a atenção dos mais diversos setores da economia mundial players, indo de pequenos investidores em suas casas até grandes atores como os mercados financeiros e o Estados nacionais.

O desenvolvimento de usos eficientes dessa rede poderá mudar as mais diversas relações, assim como a internet mudou a comunicação. A ideia é que o *Blockchain* é a nova grande oportunidade de investimento após a revolução da internet.

> Blockchains offer potential advantages in cost, speed, and data integrity compared with classical methods of proving ownership, and the scale of these potential savings has motivated investments by venture capitalists and by established players in the financial services industry. Entrepreneurs are actively investigating blockchains' suitability for recording ownership of a wide range of assets, from stocks and bonds to real estate, automobile titles, luxury handbags, and works of art. Further applications under study by governments include using blockchains for public records such as real estate titles, birth certificates, driver's licenses, and university degrees[47] (YERMACK,2017, p .8).

A simplificação de ações que podem acontecer automaticamente, somado a confiabilidade das informações mudará todo um sistema econômico complexo e que ainda sofre com barreiras dos Estados e ao problema de confiança existente nos mercados.

Para Shupmman a rede *blockchain* está ainda em sua fase inicial, sendo que já existem diversas direções na criação de tecnologias sobre a *blockchain* em que a moeda não é foco:

> While blockchain technology was developed in relation to bitcoin, many are exploring the technology's applications independent of the digital currency.32 As blockchain is still in its infancy, and given its wide-ranging applications33, there are

[47] As redes *Blockchain* oferecem vantagens potencias no custo, velocidade, e integridade da informação comparada com os métodos clássicos de prova de propriedade, e a escala dessas reduções tem motivado investimentos por capitalistas aventureiros e por *players* estabelecidos no setor financeiro. Empreendedores estão ativamente investigando como a rede irá se comportar em várias áreas, como ações, títulos públicos, propriedade de automóveis, bolsas de luxo e até obras de arte. Outros estudos estão sendo desenvolvidos pelos governos usando *Blockchain* para registros públicos como títulos do governo, certidões de nascimento, carteira de motorista e diplomas universitários. Tradução feita pela Autor.

> innumerable directions in which this technology could develop [48] (SCHUPMANN,2017, p. 5).

O *blockchain* pode vir a se tornar uma tecnologia fundamental no futuro com as aplicações financeiras possíveis dentro dele, gerando ganhos de eficiência grandes ao substituir um sistema lento e custoso de transações internacionais, porém seu registro aberto e sua falta de intervenção serão no futuro alvo de intervenções governamentais.

As consequências de legislações proibitivas podem chegar a desincentivar e até mesmo encerrar essa tecnologia que tem potencial enorme. A assim como de fato há pontos de preocupação por parte dos Estados há também vantagens para a permissão do uso, pois os sistemas são em sua grande parte transparentes, permitindo ao Estado um acesso independente de informações, ou seja, há uma perda de controle por um lado, mas haverá também o acesso a informações confiáveis por outro lado.

Os riscos associados a tecnologia nova e que tem tanto poder econômico trará sim uma cautela no seu uso, principalmente no começo, como Crosby acredita, *We envision Blockchain technology going throught slow adoption due to risk associated*[49](CROSBY,2016, p .17).

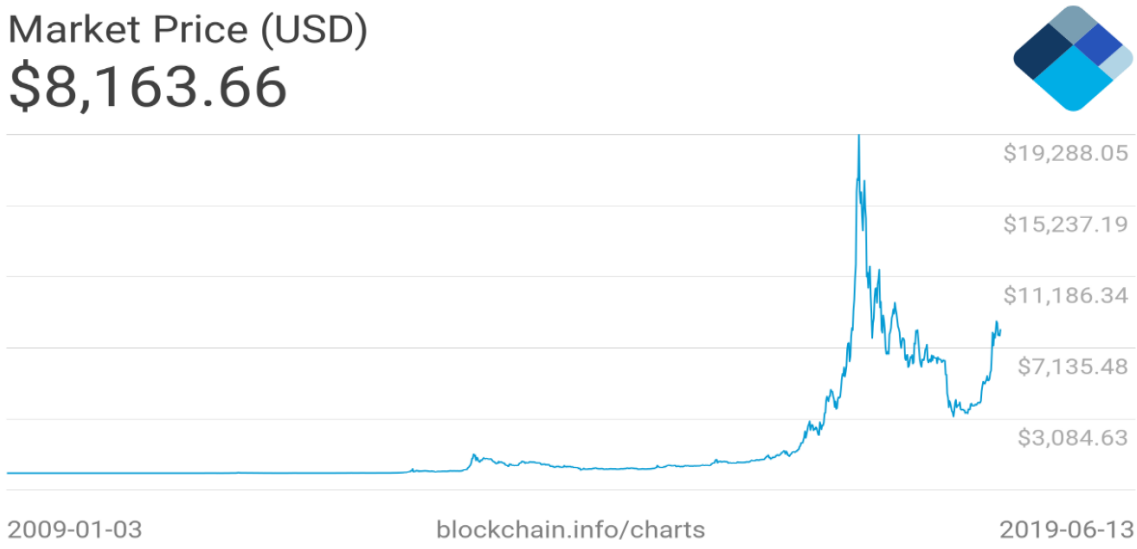
Devido à importância dos produtos que passarão pela rede o desenvolvimento poderá demorar, porém assim como foi com a comunicação no surgimento da internet, a revolução causada será rápida e irreversível.

O pico no preço do Bitcoin foi em janeiro de 2018, chegando perto dos 20.000 dólares. Tal preço não se sustentou, e com a baixa no preço a demanda na rede também começou a cair , porém não é possível observar uma relação tão direta entre preço e demanda da rede, já que o taxa máxima de *rash hate* foi obtida quando o preço da moeda estava em na casa dos 6.500 dólares. No dia 13 de junho o valor de uma unidade de Bitcoin foi de 8.163 dólares. Abaixo está um gráfico com o histórico do valor da criptomoeda.

[48] A tecnologia do *Blockchain* está se desenvolvendo em relação ao Bitcoin, muitos estão explorando tecnologias independentes da moeda digital. Enquanto o *Blockchain* ainda está na infância, as oportunidades estão sendo dadas em inúmeras direções na qual pode se desenvolver. Tradução feita pelo Autor.

[49] Nós prevemos que a tecnologia do *Blockchain* irá ter uma lenta adoção devido ao seu risco associado. Tradução feita pelo Autor

Figura 6- Preço de mercado do Bitcoin



Fonte:BLOCKCHAIN.COM,2019

3.2 ETHEREUM

O Ethereum foi lançado em 2013 por Vitalik Buterin como principal autor junto a Mihai Alisie, Anthony Di Iorio, Charles Hoskinson, Joe Lubin e Gavin Wood, como participantes na criação da criptomoeda. Surgiu como uma ideia que partiu de suas pesquisas em como criar algo diferente do apresentado pelo Bitcoin, sendo que em 2014 sua ideia se transformou em algo sólido e que teve base na Suíça, pais que está se mostrando favorável as criptomoedas. Normalmente se cita apenas Vitalik Buterin como criador por que além de ser ter sido que teve a ideia originalmente, ele ainda se mantem como um porta-voz do Ethereum.

A tecnologia por trás do Ethereum é diferente da rede *Blockchain* do Bitcoin pois tem como objetivo ir além do uso da rede apenas para transferência financeira direta entre indivíduos. A plataforma do Ethereum surge com a proposta de ser algo descentralizado e com foco em *smartcontracts* (contratos inteligentes), o que seria a alocação de capacidade de processamento para unir as partes ofertantes e demandantes para um determinado acordo pré-estabelecido por ambos, podendo consolidar uma transação financeira ou transferência de informações variadas.

A formulação do Ethereum propõe algo mais amplo que o Bitcoin, saindo da parte apenas do valor monetário, e entrando em algo novo como um sistema descentralizado que propõe a utilização do processamento dos computadores mundiais para se formar uma rede complexa de relações comerciais, a serviço de uma nova forma de ligação entre os membros de sua plataforma. A ideia por traz de se minerar para a rede do Ethereum é prover capacidade de processamento para que essa rede funcione. A ideia de Vitalik Buterin foi então uma proposta de *Blockchain* que fosse mais rápida e que trouxesse a possibilidade de ir além das simples transações financeiras, no sentido em que A envia para B apenas:

> Satoshi's blockchain was the first credible decentralized solution. And now, attention is rapidly starting to shift toward this second part of Bitcoin's technology, and how the blockchain concept can be used for more than just money[50] (BUTERIN,2014, p.1).

Quando Buterin fala em ir além de apenas dinheiro sua intenção é permitir que a rede *Blockchain* entre na sociedade por outras formas além do dinheiro, como aplicações em *Blockchain* controlando o trafego de veículos, possibilitando que seguros sejam feitos diretamente, votações online na qual a identificação pessoal é feita pela *Blockchain*, entre outros. Para Buterin existem diversas aplicações que podem ser implementadas hoje pela rede *Blockchain*, porém há varias que ainda nem foram imaginadas ainda. Em uma entrevista[51] em fevereiro deste ano Buterin comparou as criptomoedas com calculadores dedicadas e as que existem nos *smartphones*, onde o Bitcoin seria a calculadora dedicada. Ele fez essa comparação ao afirmar que essa calculadora faz uma única função, de forma excelente, porém os celulares são capazes de realizar a função dessas calculadoras e outras diversas, não apenas uma função por melhor que ela seja, comparando com o Bitcoin. Para Buterin as criptomoedas devem ir além simplesmente do dinheiro:

> What Ethereum intends to provide is a blockchain with a built-in fully fledged Turing-complete programming language that can be used to create "contracts" that can be used to encode arbitrary state transition functions, allowing users to create any of the systems described above, as well as many others that we have not yet imagined, simply by writing up the logic in a few lines of code[52](BUTERIN,2014,p.1).

Para conseguir ir além apenas do dinheiro a proposta feita pelo russo Buterin foi permitir a criação de contratos inteligentes, que são contratos postados na rede *blockchain* e que são

---

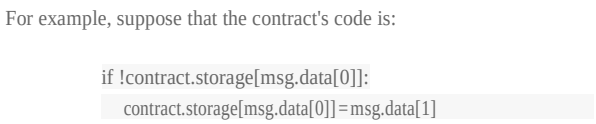
[50] E agora, a atenção está começando a mudar rapidamente para a segunda parte da tecnologia do Bitcoin, e como o conceito do *blockchain* pode ser usado para mais do que apenas dinheiro. Tradução feita pelo Autor

[51] Vídeo disponível no Youtube em: https://www.youtube.com/watch?v=fi0ORZR4A88.

[52] O que Ethereum pretende fornecer é um *blockchain* com um *built-in* Linguagem de programação completa que pode ser usada para criar "contratos" que podem ser usados para codificar funções de transição de estado arbitrário, permitindo aos usuários criar qualquer um dos sistemas descritos bem como muitos outros que ainda não imaginamos, simplesmente escrevendo a lógica em algumas linhas de código. Tradução feita pela Autor

executados de forma automática quando o código escrito for realizável. Um exemplo hipotético de um contrato inteligente seria um seguro para um passageiro que irá realizar uma viagem. Esse seguro hipotético seria então feito pela companhia área, na qual estaria condicionado que se o voo for cancelado, automaticamente os passageiros receberiam de volta o valor de sua passagem, bastando apenas um "sinal" para a rede *Blockchain*, que pode ser implementada de forma automática no futuro com uma integração de sistemas aéreos , executasse o código para que então a transferência seja feita. Basicamente a *Blockchain* iria executar aquilo que foi prometido, ou seja, se a viagem foi cancelada o sistema irá transferir de um lugar para outro o Ethereum, de forma autônoma e sem precisar de validação da companhia aérea. Buterin exemplifica um código desses contratos na figura abaixo

Figura 7 – Ilustração de Vitalik Buterin sobre os *smart contracts*



Fonte: BUTERIN, 2014.p16

Uma das criadoras do Ethereum, Mihai Alisie explicou em um texto para um artigo de Dan Branes qual a visão dela sobre o papel que os *smart contracts* poderiam exercer sobre essa *blockchain*, que se diferenciava por permitir que uma nova geração de aplicação pudesse surgir dentro do Ethereum.

> We have a blockchain that is featureless in a sense and it has embedded within it a programming language that allows people to create all sorts of things that run on top of the blockchain architecture. The building block for Ethereum is a smart contract; it is like a virtual machine or autonomous programme that is maintained by everyone in the network. Inside the contract you can specify what its purpose is. The contracts are the foundations for a new generation of applications on the internet[53](BARNES *apud* ALISIE, 2015, p.4).

Os contratos inteligentes como esses permitiriam então que a inovação criada por Satoshi Nakamoto conseguisse invadir a sociedade além apenas do braço financeiro., porém apesar

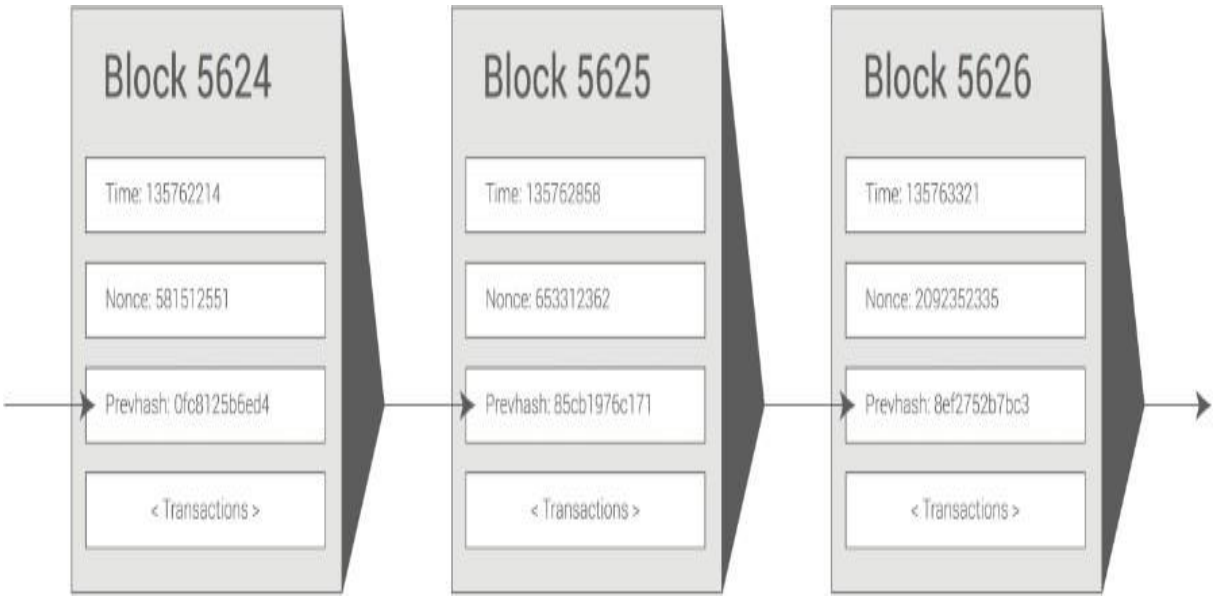
[53] Nós temos uma *blockchain* que é uniforme em certo sentido, e embutiu dentro dele uma linguagem de programação que permite que as pessoas criem todo tipo de coisas que rodam no topo da arquitetura *blockchain*. O bloco de construção para o Ethereum é um contrato inteligente; é como uma máquina virtual ou um programa autônomo que é mantido por todos na rede. Dentro do contrato, você pode especificar qual é o seu propósito. Os contratos são as bases para uma nova geração de aplicativos na internet. Tradução feita pelo Autor

dessa inserção social, Buterin acredita que ainda a principal função de sua rede seja o viés econômico:

> In general, there are three types of applications on top of Ethereum. The first category is financial applications, providing users with more powerful ways of managing and entering into contracts using their money. This includes sub-currencies, financial derivatives, hedging contracts, savings wallets, wills, and ultimately even some classes of full-scale employment contracts. The second category is semi-financial applications, where money is involved but there is also a heavy non-monetary side to what is being done; a perfect example is self-enforcing bounties for solutions to computational problems. Finally, there are applications such as online voting and decentralized governance that are not financial at all (BUTERIN,2014, p.19).[54]

Assim como a *blockchain* do Bitcoin a rede do Ethereum registra as informações anteriores ao em seu *modus operandi* sempre requisitar o *hash* da transação anterior, ou seja, cada nova transferência ou contrato é sempre verificado e adicionado ao anterior. Quando há a verificação do novo registro na *blockchain*, ele é agrupado e permanece então imutável na cadeia de blocos, tendo a característica em ser uma rede transparente, onde cada transação pode ser observada pelo site da rede Ethereum. Logo abaixo há uma ilustração do próprio Vitalik Buterin sobre como é feita a aglomeração dos blocos na rede.

Figura 8- Ilustração de Vitalik Buterin sobre a *Blockchain*



Fonte:BUTERIN,2014, p.6

[54] Em geral, existem três tipos de aplicações para o Ethereum. A primeira categoria é de aplicativos financeiros, oferecendo aos usuários maneiras mais poderosas de gerenciar e entrar em contratos usando seu dinheiro. Isso inclui sub-moedas, derivativos financeiros, contratos de *hedge*, carteiras de poupança, testamentos e até mesmo algumas classes de contratos de trabalho em larga escala. A segunda categoria é a aplicação semi-financeira, onde o dinheiro está envolvido, mas há também um lado não monetário para o que está sendo feito; um exemplo perfeito são recompensas auto-executivas para soluções de problemas computacionais. Finalmente, há aplicações como votação online e governança descentralizada que não são financeiras.Tradução feita pela Autor.

4 A QUESTÃO DA REGULAMENTAÇÃO DAS CRIPTOMOEDAS

As moedas virtuais foram pensadas como algo que se adapte ao novo paradigma mundial da globalização e da internet, se mostrando algo até então revolucionário ao permitir relações econômicas entre agentes sem a tutela de uma instituição governamental para impor regras. Em sua concepção as moedas virtuais buscam formar interações mais liberais, visto que a ideia original do Bitcoin surgiu como uma reposta a crise de 2008, que estava no coração do sistema financeiro mundial, ou seja, nos bancos americanos.

Outro fator que pode gerar regulações duras contra as moedas virtuais é a ideia quase que consensual de que as criptomoedas estão em uma bolha, com valoração anormal e baseada em especulação. Como o sistema de moedas virtuais é algo novo e desregulamentado, uma possível quebra do sistema resultaria em prejuízo muito grande aos detentores dos ativos. Quando o sistema financeiro local tem uma crise, como a de 2008, o governo age para impedir danos maiores a economia, como por exemplo quando o governo Obama liberou ajuda aos grandes bancos nacionais após a falência do Lehman Brothers, resultando em um suporte a aqueles que tinham ativos nos bancos. Se acontecer uma crise no sistema de criptomoedas não há ninguém para salvar os detentores das moedas, algo que pode influenciar fortemente as políticas feitas para regulamentação das moedas virtuais.

No planejamento de políticas sobre as criptomoedas um ponto a ser considerado um *trade- off* pelos *policymakers*, que são as pessoas que realmente pensam as políticas, é a vantagem de ser mais permissivo com essa nova forma monetária. Países podem usar esse mecanismo a seu favor ao atrair capitais que poderão ser produtivos tanto no consumo quanto na poupança pública e privada. Um país como o Brasil, por exemplo, que tem sérios problemas relativos à poupança pública e financiamento de sua dívida pública, poderia aceitar facilmente aceitar a circulação de moedas virtuais destinadas a aquisição de títulos públicos, resultando em juros menores a serem oferecidos como recompensa. Esse exemplo se daria em uma situação otimista na evolução do Bitcoin e pessimista na relação regulamentária vinda dos grandes centros de capitais, ou seja, por ser algo descentralizado essas moedas podem se transformar em outros ativos de forma muita rápida, fazendo com que empecilhos em outros países se

transformem em oportunidades para países com dificuldades. A relação entre a regulação proposta e os riscos associados as criptomoedas também são objeto de pesquisa de Zetzsche, que é um pesquisador alemão e que defende encontrar esse equilíbrio entre segurança e inovação:

> Technology is transforming finance around the world at an unprecedented rate, generating new opportunities and new risks. Financial regulators must develop new approaches to regulation, including the use of technology, to balance the benefits of innovation and economic development with the need for financial stability and consumer protection[55] (ZETZSCHE,2017, p.34).

Para Zetzsche após a crise financeira de 2008(que foi a justificativa de Satoshi Nakamoto para criação do Bitcoin) houve uma reversão na tendência na forma de se entender inovação no setor financeiro, ou seja, antes se via com bons olhos as novas tecnologias aplicadas a essa área, o que foi mudado após a crise.

Dessa forma como ele exemplifica, o pêndulo saiu de um lado favorável às inovações para o outro extremo, que é ainda o receio dos reguladores em não gerar situações como essa:

> Prior to the Global Financial Crisis of 2008 (the Crisis), financial innovation was generally viewed very positively. This led to laissez-faire, deregulatory approaches to regulation particularly in global institutional markets. Post-Crisis financial regulatory reforms have seen a reversal of this approach with the regulatory pendulum arguably swinging to the other extreme[56] (ZETZSCHE,2017, p.34) .

É possível entender esse comportamento como uma reação da sociedade, e como consequência também dos agentes reguladores, já que de forma simplificada, a crise de 2008 foi causada pelo descontrole dos agentes financeiros sobre os empréstimos para setor imobiliário, causando uma bolha devido a regulamentações excessivamente permissivas. O momento pós crise foi tomado por discussões sobre regulamentações para que situações de descontrole não voltassem a acontecer, gerando toda uma visão de que o controle sobre os agentes financeiros e todo o sistema econômico é necessário para que novas crises não sejam produzidas da mesma forma. Se considerarmos que o mundo saiu da crise na mesma década da criação do Bitcoin é possível sim entender a preocupação de Zetzsche, na qual a tendência sobre regular possa ocorrer sem uma mensuração mais trabalhada das vantagens financeiras proporcionadas pelas novas tecnologias. Para ele a crise gerou duas vertentes nas quais os

[55] A tecnologia está transformando as finanças em todo o mundo a uma taxa sem precedentes, gerando novas oportunidades e novos riscos. Os reguladores financeiros devem desenvolver novas abordagens de regulamentação, incluindo o uso de tecnologia, para equilibrar os benefícios da inovação e do desenvolvimento econômico com a necessidade de estabilidade financeira e proteção ao consumidor. Tradução feita pela Autor.

[56] Antes da Crise Financeira Global de 2008 (a Crise), a inovação financeira era geralmente vista de forma muito positiva. Isso levou a abordagens *laissez-faire* e tendências desregulamentadoras, particularmente nos mercados institucionais globais. As reformas regulatórias financeiras pós-crise viram com uma reversão dessa abordagem, com o pêndulo regulatório oscilando para o outro extremo. Tradução feita pela Autor

reguladores deveriam seguir para que assim fosse atendida uma demanda da sociedade e das instituições para gerar maior confiança e segurança na economia:

> Among the main financial regulatory mandates, two were of key importance as the 2008 Crisis unfolded: first, consumer protection (particularly of retail clients, investors, and depositors); and second, financial stability more generally, particularly in the macroprudential context[57](ZETZSCHE,2017, p.37).

O Bitcoin surgiu então indo contra as indicações de política regulatória dos pós crise em não oferecer proteção, no sentindo em ter alguém a recorrer após uma baixa no preço, e também sem ter como objetivo um contexto de preços estáveis. Tais características da criptomoeda levaram assim a uma situação de rejeição em um primeiro momento dessa sociedade ainda abalada pela crise, gerando um cenário de desconfiança prévio, tendo sempre sua valorização associada a uma bolha especulativa, sem real entendimento de que se tratava de algo novo, que proporcionará uma expansão da fronteira do universo de pagamentos, e que veio para ficar.

Um dos pontos fundamentais na necessidade de regulamentação da entrada e saída de criptomoedas está na perda de poder nas decisões sobre política monetária. De novo, em um caso otimista da evolução das criptomoedas, em que vire algo verdadeiramente grande, a entrada dessas moedas pode, por exemplo, ir contra uma política monetária contracionista, resultando em ineficiência da política monetária, já que se está cortando de um lado e permitindo por outro. Esse é o ponto de maior desafio para as criptomoedas, pois lavagem de dinheiro e bolhas ocorrem em vários setores da economia, como agora na China em que se acredita que há em curso uma severa bolha imobiliária. O ponto de diferente que surge com as criptomoedas está em sua interferência na política monetária dos países, algo que muda totalmente o modo em vigência a tanto tempo.

As políticas pensadas sobre as moedas virtuais com certeza não serão medidas simples, já que é algo novo e que pode ter o potencial de interferência significativa nas mais diversas áreas. A complexidade do novo fenômeno econômico que surge é grande, trazendo muita responsabilidade aos *policymakers*, já que possíveis mudanças de paradigmas virão. O crescimento e uso das criptomoedas irão trazer problemas para os *policymakers* ainda não apresentados, ou seja, sem precedentes. Situações relacionadas a atos ilícitos virão se

[57] Entre os principais mandatos de regulamentação financeira, dois eram de importância como a crise de 2008 se desenrolou: primeiro, a defesa do consumidor (particularmente de clientes de varejo, investidores e depositantes); e segundo, estabilidade financeira mais geralmente, particularmente no contexto macroeconômico. Tradução feita pelo Autor

aproveitar das brechas criadas por essa nova tecnologia, porém os benefícios dessa tecnologia serão maiores a longo prazo do que os prejuízos causado pelos oportunistas. É necessário nesse momento de crescimento o mínimo de regulação possível para que a tecnologia das criptomoedas e da *blockchain* cresçam e consigam mudar o paradigma das transações.

As regulações implementadas em alguns países como Coréia do Sul e China, que estão dificultando muito o mercado de criptomoedas pode ser um tiro no pé desses países, pois há uma mobilidade praticamente instantânea desse capital, resultando uma punição para o seu país, a medida que seus habitantes não podem usufruir da tecnologia do *blockchain*. Um ofertante de uma criptomoeda, um minerador, ao produzir e vender na rede aquela moeda produz renda para o seu país, na medida que feita a conversão para a sua moeda local, a criptomoeda irá gerar consumo local. Se um país proíbe a conversão de criptomoedas, a oferta deixada de ser ofertada no mercado mundial resultará em um aumento de preço, resultando aos países que permanecem uma maior fatia do mercado, resultando em consumo no país. Isso significa que um país, isolado, ao proibir o uso das criptomoedas perde duplamente, ao não permitir o uso de uma rede que promove trocas eficientes, além da renda gerada pelos ofertantes das criptomoedas.

A política ideal nesse momento de surgimento das criptomoedas seria a não intervenção no curso de desenvolvimento da tecnologia *Blockchain*. De fato haverão oportunistas que usarão dessa tecnologia para a obtenção de vantagens ilegais, porém nesse momento o desenvolvimento da tecnologia das criptomoedas é algo que pode ser muito mais vantajoso para a economia mundial ao permitir que as transações financeiras sejam mais rápidas, mais baratas e mais seguras. A aplicação de regulamentações desnecessárias poderá trazer ao pais que aplicou mais dano do que o simples retorno financeiro sobre tributação, já que a tecnologia do *blockchain* irá aumentar a produtividade nos mais diversos setores econômicos, podendo melhorar diversas áreas da economia desse pais, transformando a economia e também a sociedade .*Currently, commentary consensus posits for a balanced approach to bitcoin regulation because authors believe that stringent regulatory frameworks produce more harm to innovation than they produce in social utility*[58](BROUWER,2019.p2).

[58] Atualmente, é consenso nos comentários direcionam para uma abordagem equilibrada da regulação bitcoin porque os autores acreditam que os quadros regulamentares rigorosos irão produzir mais danos à inovação do que produzem na utilidade social. Tradução feita pela Autor

Uma situação mais simples que se encaixa nessa situação da regulamentação das criptomoedas, onde há um embate entre novas tecnologias e o Estado é o recente caso dos patinetes elétricos[59] no Brasil. Há alguns anos essa modalidade de transporte alternativo ecológico chegou ao país e obteve muito sucesso nas grandes capitais do Brasil.

A utilização do meio de transporte estava até pouco tempo sem regulamentação por parte das instituições competentes, o que significou preços mais acessíveis. A situação começou a mudar nesse ano, sendo que a prefeitura da cidade de São Paulo[60] criou uma grande discussão sobre como regular algo novo, que melhora a locomoção na cidade de forma relativamente barata, mas que causa transtornos ao trânsito e pode gerar acidentes. No começo de maio então foi criada uma legislação para o uso do patinete elétrico dentro das cidades, exigindo itens como o capacete e proibindo a circulação em calçadas, além de repassar as multas para os usuários pelas infrações[61]. Os autores dessa matéria trazem uma reflexão sobre como pode haver a questão em desencorajar novas ideias devido a regulações malfeitas A grande discussão agora é como essas regulações irão afetar o curso natural de desenvolvimento dessa modalidade de transporte, já que essas regulamentações tem grande chance aumentar o preço já que é exigido mais das empresas.

A situação dos patinetes e das criptomoedas tem semelhanças, pois são novas tecnologias que foram rapidamente adotas porem ainda não chegaram ao seu potencial máximo, e situações como essa regulações inapropriadas propostas pelo Estado irá afetar mais a sociedade do que trazer benefícios, no caso do patinete significaria a volta dessas pessoas para carros e da *blockchain* formas mais ineficientes de transações financeiras e uso em setores produtivos da sociedade. A política adequada nesse momento seria não tentar acertar de primeira toda a estrutura legal, mas ir aos poucos adotando regulamentações e assim se observar as

[59]A utilização do meio de transporte estava até pouco tempo sem regulamentação por parte das instituições competentes, o que significou preços mais acessíveis. A situação começou a mudar nesse ano, sendo que a prefeitura da cidade de São Paulo[59] criou uma grande discussão sobre como regular algo novo, que melhora a locomoção na cidade de forma relativamente barata, mas que causa transtornos ao trânsito e pode gerar acidentes. No começo de maio então foi criada uma legislação para o uso do patinete elétrico dentro das cidades, exigindo itens como o capacete e proibindo a circulação em calçadas, além de repassar as multas para os usuários pelas infrações[59]. Os autores dessa matéria trazem uma reflexão sobre como pode haver a questão em desencorajar novas ideias devido a regulações malfeitas A grande discussão agora é como essas regulações irão afetar o curso natural de desenvolvimento dessa modalidade de transporte, já que essas regulamentações tem grande chance aumentar o preço já que é exigido mais das empresas.

[60] Matéria jornalística do estadão disponível em: https://politica.estadao.com.br/blogs/fausto-macedo/a-regulamentacao-provisoria-dos-patinetes-eletricos-na-contramao-da-mobilidade/

[61]Matéria jornalística do G1 dispinivel em: https://g1.globo.com/sp/sao-paulo/noticia/2019/05/15/yellow-e-grin-repassarao-multas-para-usuarios-de-patinetes-eletricos-em-sp.ghtml

consequências. Pode ser muito pesado para negócios em crescimento a criação regulamentações definitivas sobre algo que a sociedade e os legisladores não entendem completamente, tentando usar outras políticas já feitas para outras situações.

4.1 CONSEQUÊNCIAS DAS REGULAMENTAÇÕES

O futuro das moedas virtuais passa fundamentalmente pela forma como os governos centrais irão trata-las, podendo surgir assim uma tecnologia nova que perdure ou algo que foi abafado no seu nascimento. Isso se deve ao fato de que a maioria das pessoas que são "consumidoras" dos serviços prestados pelas diversas redes *Blockchain* trocam por dinheiro, ao contrário dos mineradores, que prestam serviço para a rede e são recompensados por suas moedas.

A regulação direta das criptomoedas seria algo muito difícil para vários países juntos, e impossível para apenas um determinado país. Não há instituição a quem recorrer para se controlar uma *Blockchain*, já é algo descentralizado e não tem uma instituição central, ou seja, não há raízes diretas entre uma *Blockchain* e um Estado Nacional. *It poses unique regulatory challenges, as unlike legacy payment systems, no central institution controls bitcoin. This makes bitcoin intrinsically difficult for regulators to command control over the bitcoin network* (BROUWER,2019, P.1.)

A regulação das criptomoedas afeta diretamente seu uso ao desestimular a porta de entrada do mundo não virtual para o mundo das *blockchain*, que são as *exchanges*. Esses agentes intermediários fazem o papel em comprar as moedas dos mineradores e vender para aqueles que desejam possuir uma criptomoeda, fazendo a troca do dinheiro fiat para criptomoeda. As *exchanges* fazem o papel de um intermediário tradicional, ao manter os ativos, realizar transações e poder sacar de volta as criptomoedas em dinheiro.

Muito se fala em como as redes *blockchain* podem desafiar o Estado em relação ao seu poder de regulamentação, sendo que alguns evangelistas liberais acreditam que no futuro essa tecnologia irá conseguir mudar todo o Estado, porém o fato é que se um dia isso vier a acontecer, todo desenvolvimento desse tecnologia passará também pelas *exchanges*, na qual o Estado tem de fato um poder muito grande pois estas podem sofrer localmente o peso da

administração Estatal, e é isso que a maioria dos países estão fazendo, mudando o foco da *blockchain* para as exchanges.

> Bitcoin's decentralised structure poses unique challenges to regulators because they can only control single access points that connect to the real-world economy. As a result, regulators have started to invoke strict legal obligations on bitcoin exchange platforms as these entities embody similar characteristics to traditional financial institutions and securities exchange markets[62] (BROUWER,2019, p.21).

Diferentemente das *Blockchain*s que estão na nuvem e não respondem a autoridade dos Estados, as *exchanges* são intermediários com foco na atuação geralmente em um país especifico, com vários funcionários e que tem localização física. Seu funcionamento é como o de uma empresa comum, respeitando as regras vigentes financeiras e trabalhistas.

> If regulators cannot regulate the bitcoin network, then they must allocate their scare regulatory resources to regulate other controllable bitcoin phenomenon. With bitcoin exchanges now penetrating deeper into the financial sector, these monetary conduits that connect the cryptocurrency ecosystem to legacy economic actors present unaccounted for risks[63] (BROUWER,2019, p.5).

Além das *Exchanges* as regulamentações sobre as criptomoedas têm um efeito muito forte na questão do investimento, podendo comprometer novas linhas de pesquisa que possam incrementar usos da rede nas mais diversas áreas da economia. Uma posição contraria por parte do Estado iria desestimular que vários setores da sociedade desistam de estudar e aplicar novas formas sobre a rede *blockchain*, prejudicando algo que está se mostrando um avanço na área financeira e também em relação a produtividade Inter setorial. O setor privado não teria interesse em investir em algo que lhe cause uma confrontação com interesses nacionais maiores, como foi o caso do Google ao retirar seus serviços dos celulares da Huawei, que é uma empresa Chinesa e que enfrenta acusações de espionagem pelo governo dos Estados Unidos[64]. Outro exemplo é o caso de Edward Snowden, que divulgou diversas informações sigilosas do Governo dos Estados Unidos, que segundo ele espionava os cidadãos americanos

[62] A estrutura descentralizada do Bitcoin apresenta desafios únicos aos reguladores porque eles só podem controlar pontos de acesso únicos, que se conectam à economia do mundo real. Como resultado, os reguladores começaram a invocar obrigações legais rígidas em plataformas de troca de bitcoins, uma vez que essas entidades incorporam características semelhantes às tradicionais instituições financeiras e mercados de valores mobiliários.
[63] Se os reguladores não puderem regular a rede bitcoin, eles devem alocar seus recursos regulatórios assustadores para regular outros fenômenos de bitcoins controláveis. Com as *exchanges* penetrando agora mais profundamente no setor financeiro, esses canais monetários que conectam o ecossistema da criptomoeda a agentes econômicos tradicionais apresentam riscos não contabilizados. Tradução feita pelo Autor
[64]Noticia disponível em: https://noticias.uol.com.br/ultimas-noticias/deutschewelle/2019/05/20/google-suspende-parte-de-acesso-da-huawei-ao-android.htm

através dos servidores das grandes empresas de tecnologia, como Google, Apple e Facebook[65].

Os casos dessas empresas revelam que há uma tendência das empresas americanas em seguir seu governo, ou seja, elas não são tão rebeldes o quanto poderiam ser, se reservando a alguns casos isolados na qual as grandes empresas de tecnologia desafiam seu governo. Sendo assim é difícil imaginar uma posição de confronto ao se investir nas redes *blockchain* em um cenário hipotético, no qual o governo americano seja fortemente contrário às moedas virtuais. Junto as empresas também se juntariam as universidades americanas, que estão entre as melhores do mundo.

O caso americano foi um exemplo para mostrar que as criptomoedas podem ser atingidas, sim, em seu desenvolvimento ao se restringir a entrada da economia *mainstream* via *exchanges*, além de também interferir no seu curso de desenvolvimento caso governos não aprovem regulações favoráveis, como é o caso atual da China, forçando a retirada de grandes *players* dos mais diversos setores na criação de novas formas de uso da tecnologia do *blockchain*, já ainda há um longo caminho a ser feito para que essas redes se integrem de fato á economia "real", atingindo grande parte da população com o que ela é capaz de oferecer, que são transações mais rápidas e seguras, e setores com maior produtividade ao integrar informações de forma barata e eficiente

4.2 A REGULAÇÃO NAS TRÊS MAIORES ECONOMIAS DO MUNDO E NO BRASIL

Estados Unidos, China e Japão possuem, respectivamente, os maiores PIB entre todas as nações, segundo o Banco Mundial[66]. Se considerarmos que os Estados Unidos têm 20 trilhões de dólares em seu PIB, a China tem 12 trilhões de dólares e o Japão 5 trilhões de dólares, contra 80 trilhões de dólares do resto do mundo, significa dizer que apenas esses países possuem 46% de toda riqueza mundial. A importância desses 3 países para o desenvolvimento e demanda das redes *blockchain* é essencial, já que além de sua importância financeira em relação ao mundo, esses países são os grandes criadores de novas tecnologias. A aceitação e o

[65] Noticia disponível em: http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html
[66] BANCO MUNDIAL.disponível em : https://data.worldbank.org/indicator/ny.gdp.mktp.cd?view=map

uso em larga escala das criptomoedas irão passar como esses países dominantes irão tratar e passar a de fato aplicar sua tecnologia.

O modo como as três maiores nações do mundo trata as criptomoedas são diferentes, sendo os Estados Unidos em uma posição neutra, sem tomar decisões proibitivas fortes, mas cauteloso em relação a regulação no mercado financeiro.

A China possui uma relação com as criptomoedas muito negativa, chegando a propor políticas para banir a mineração em seu território[67],além de tentar bloquear o acesso de seus cidadãos a *exchanges* em outros países[68]. Já o Japão é um dos países com maior aceitação da ideia das criptomoedas, com regulações favoráveis ao seu uso como até mesmo moeda como uma moeda comum, aceita em transações locais, além de ver com bons olhos a questão da auto regulação[69], que é quando se cria uma entidade para validar as transações dentro do pais.

As três maiores economias do mundo tratam a nova tecnologia das criptomoedas de forma diferente, trazendo assim situações diferentes situações em cada país, já que a maneira como o país vê a inovação é diferente. A atuação desse trio irá interferir de forma significativa no desenvolvimento dos países, porem se as criptomoedas crescerem de forma a acompanhar a expectativa que há sobre elas, o inverso acontecerá, e cada pais poderá colher os resultados de medidas regulatórias apresentadas agora, já que o desenvolvimento de tecnologia é algo demorado, e que tem em todas as economias, algumas mais outras menos influência dos Estados. É importante o entendimento de como as regulações estão sendo feitas nos maiores países do mundo de forma mais detalhada, para assim se ter uma possível direção neste sentido já que estes são os países mais influentes.

Também será discutido como está se dando as regulações no Brasil, na qual há uma situação semelhante á americana, no sentido de que há uma proteção para o capital, mas não há impedimentos para que as pessoas possam adquirir criptomoedas.

---

[67] Disponível em: https://techcrunch.com/2019/04/09/china-considers-ban-crypto-mining/
[68] Disponível em: https://portaldobitcoin.com/china-quer-bloquear-acesso-a-exchanges-de-criptomoedas-de-fora-do-pais/
[69] Disponível em :https://guiadobitcoin.com.br/japao-lei-auto-regulamentacao-mercado-criptomoedas/

4.2.1 Estados Unidos

A forma como os Estados Unidos trata a questão da regulamentação das criptomoedas é de fundamental importância para um desenvolvimento rápido dessa tecnologia. A maior economia do mundo tem influencias para o tratamento das criptomoedas em 3 formas diferentes: uso na sua economia, influência nos demais países e desenvolvimento de novas tecnologias através do setor de informática que há no país

Se considerarmos que o PIB americano é de 20 trilhões de dólares e o PIB mundial é de 80 trilhões, 25% do produto global passa pelo solo americano, e não é de se esperar um número tão diferente sobre as criptomoedas, ou seja, é possível que 1 em cada 4 criptomoedas tenham alguma relação com a economia americana, já que sua economia atrai capital de todo o resto do mundo. Não é possível ainda ter com exatidão a circulação exata de criptomoedas relacionadas aos Estados Unidos, porém não há como não existir uma relação direta entre o tamanho da sua economia com seu efeito "imã" de capitais entre outros países. Em uma situação de políticas regulatórias restritivas sobre as criptomoedas a reação seria que agentes dessa economia diminuam sua demanda pelo serviço de pagamento das redes *blockchain*, significando uma queda no preço das moedas.

Outra consequência de um possível endurecimento americano contra as criptomoedas seriam desestimular o investimento de sua indústria de tecnologia em aplicações novas da rede *blockchain*, afetando assim a entrada dessa tecnologia na economia. O vale do silício é onde ficam as maiores empresas de tecnologia do mundo, como Google, Microsoft e IBM. Esses gigantes da área de TI (tecnologia da informação) teriam assim motivos para ir contra a criação de novas formas de uso que iriam não só para os Estados Unidos, mas para todo o mundo, sendo o efeito contrário também valido, ou seja, uma definição futura favorável pode levar a uma corrida das grandes empresas em conseguir entregar soluções para consumidores que usem a rede *blockchain*.

A conduta até o momento do governo americano em relação as criptomoedas tem sido de forma moderada, permitindo que seus cidadãos possam ter criptomoedas e também receber pagamentos por ela. Em 2013 o *Financial crimes enforcement network* (FinCen), que está associado ao departamento de tesouro americano criou uma resolução de 6 páginas que

permanece como um guia para o tratamento das moedas em solo americano[70]. Dentro deste texto há vários pontos que são positivos no ponto de visto da liberação e outros nos quais o tratamento é muito parecido com o existente para outros serviços financeiros. O FinCen expressa seu entendimento sobre as criptomoedas, dando o tom para como o governo passou a tratar o que na época era uma tecnologia totalmente nova, associando a moeda "real" como aquela em papel que circulam nos países, considerando as criptomoedas um meio de troca incompleto, sem todas as atribuições necessárias para uma moeda:

> FinCEN's regulations define currency (also referred to as "real" currency) as "the coin and paper money of the United States or of any other country that [i] is designated as legal tender and that [ii] circulates and [iii] is customarily used and accepted as a medium of exchange in the country of issuance." 3 In contrast to real currency, "virtual" currency is a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency. In particular, virtual currency does not have legal tender status in any jurisdiction[71] (FINCEN,2013, p.1).

O documento também determinou quem deve seguir as regras do departamento de tesouro, excluindo assim o usuário comum que compra e usa as criptomoedas em transações, porém exigindo que *exchangers* e administradores tenham que seguir regras especificas. O FinCen define esses agentes como:

> A user is a person that obtains virtual currency to purchase goods or services. 7 An exchanger is a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency. An administrator is a person engaged as a business in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency[72](FINCEN,2013, p.2).

Basicamente após definir os tipos de usuário das criptomoedas essa regulação excluiu os usuários e passou a interferir na parte ligada aos negócios criados pelas criptomoedas,

---

[70] EUA. The Financial Crimes Enforcement Network ("FinCEN"). Application of FinCEN's regulations to persons administering, exchanging, or using virtual currencies. Disponível em: https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf. Acesso em: 29 jun. 2019

[71] Os regulamentos do FinCEN definem a moeda (também conhecida como moeda "real") como "moeda e papel-moeda dos Estados Unidos ou de qualquer outro país que [i] seja designado como moeda legal e que [ii] circule e [iii] seja habitualmente usado e aceito como meio de troca no país de emissão. "3 Em contraste com a moeda real, a moeda "virtual" é um meio de troca que opera como moeda em alguns ambientes, mas não possui todos os atributos da moeda real. moeda. Em particular, a moeda virtual não tem curso legal em qualquer jurisdição. Tradução feita pelo Autor

[72] Um usuário é uma pessoa que obtém moeda virtual para comprar bens ou serviços. Um *exchanger* é uma pessoa envolvida como empresa na troca de moeda virtual por moeda real, fundos ou outra moeda virtual. Um administrador é uma pessoa envolvida como empresa na emissão (colocação em circulação) de uma moeda virtual e que tem a autoridade para resgatar (para retirar de circulação) essa moeda virtual. Tradução feita pelo Autor.

tentando assim gerar um grau de confiança para que os usuários americanos não sejam vítimas de golpes relacionados as vendas das moedas. As regras sobre os *exchangers* e os administradores foram direcionadas para se evitar crimes de lavagem de dinheiro, ao propor regulações já existentes para os serviços financeiros tradicionais, como a exigência de documentação e limites de valores para certos tipos de transações, levando assim regulamentações já usadas antes.

> The definition of a money transmitter does not differentiate between real currencies and convertible virtual currencies. Accepting and transmitting anything of value that substitutes for currency makes a person a money transmitter under the regulations implementing the BSA.12 FinCEN has reviewed different activities involving virtual currency and has made determinations regarding the appropriate regulatory treatment of administrators and exchangers under three scenarios: brokers and dealers of e-currencies and e-precious metals; centralized convertible virtual currencies; and de-centralized convertible virtual currencies(FINCEN,2013,p.3).

De um lado o governo americano tratou com moderação a parte mais associada ao consumo da população ao permitir que usuários comuns usem, controlando os ofertantes e deixando os demandantes com poucas regras. Porém por outro lado o governo americano tem tomado decisões restritivas quando se trata de acesso ao mercado financeiro títulos, com a *Securities and exchange comission*(SEC) rejeitando várias propostas de fundos baseados em criptomoedas. As rejeições foram direcionadas aos produtos financeiros ETP[73] e ETF[74].

> The U.S. Securities and Exchange Commission's ("SEC") rejection of nine proposed bitcoin-based exchange-traded funds ("ETFs") and their second rejection of the Winklevoss bitcoin-based exchange-traded products ("ETPs")5 showcased the tension between financial market regulators and cryptocurrency market innovators (BROWN,2019, p.2).

O setor financeiro americano ainda não aceitou as criptomoedas como produtos capazes de serem seguros para o público em geral, deixando de fora dos grandes capitais relacionados ao setor financeiro de *wall street.* Possivelmente essas ações estão ligadas a alta instabilidade nos preços das criptomoedas, o que gera grande reação pelos reguladores para que assim proteger a população e as instituições. Os reguladores do mercado financeiro foram criticados em relação a crise de 2008, sendo sempre acusados de políticas permissivas e que resultaram em uma grande crise, sendo natural uma reação adversa a ativos tão instáveis como as

[73] *Exchange traded produtcs* são produtos financeiros que contem índices de cestas de produtos negociados pelas bolsas americanas, como *comodities*. Um ETP na pratica iria tratar a criptomoeda com um produto físico, no caso o código da moeda, permitindo assim sua operacionalização no mercado

[74] *Exchange traded funds* são produtos financeiros que contem índices de fundos, como ações e títulos públicos

criptomoedas, que não tem regulação central e também ainda não se desenvolveu completamente.

O governo americano adota uma estratégia cautelosa, gerando regulamentações sobre os ofertantes e também protegendo o mercado de grandes capitais, porém sem desestimular sua população a usar as criptomoedas. É natural esse caminho após a crise de 2008, resultando em aplicações de políticas já existentes para assim se criar confiança dos agentes sobre essa nova tecnologia. *Overall, the US has focused on fitting cryptocurrencies into existing regulations instead of formulating new cryptocurrency-specific regulation* (SIMS; KARIYAWASAM; MAYES, 2018.p 96).

4.2.2 China

A China é atualmente a segunda maior economia do mundo, ficando atrás apenas dos Estados Unidos. O gigante asiático tem relações econômicas importantes com todo o mundo, sendo a fabrica do planeta. Além disso sua população é a maior, com 1,3 bilhão de pessoas, o que significa um papel de grande destaque, negativo e positivo, no uso do sistema de pagamentos das redes *blockchain*.

A relação da China com as criptomoedas tem sido vista pelo mercado como restritiva ao uso e desenvolvimento de novas tecnologias. Diferente das outras nações, a China tem um papel fundamental pois está concentrado lá as maiores mineradoras de todas as criptomoedas, em especial do Bitcoin que é a maior criptomoeda. *China plays an important role in the bitcoin mining ecosystem. In the last month, it accounted for 80% of all mined bitcoins* [75] (SHARMA,2019, p.1).

Essa concentração de poder de mineração na China é explicada pelo baixo custo da eletricidade, pois a mineração exige que os computadores fiquem ligados o tempo todo, e também menor custo nos componentes dos computadores, já que a maioria é fabricada no país. A questão da quantidade necessária de eletricidade tem chamado a atenção dos reguladores, que argumentam sobre como esse polo de mineradoras tem sido prejudicial ao

[75] A China tem uma grande importância no ecossistema de mineração de Bitcoin. No mês passado(maio), foi registrado 80% de todos os Bitcoins minerados vindos da China. Tradução feita pelo Autor.

país. Os pesquisadores americanos Kaiser, Jurado e Ledger também argumentam sobre essa situação

> The Chinese government enjoys broad regulatory authority that it can bring to bear on domestic Bitcoin users, exchanges, and miners. Regulators have issued policy decrees to directly influence the exchange and mining sectors and also targeted Bitcoin indirectly through externalities like energy prices[76] (KAISER; JURADO; LEDGER,2019, P.5).

Em abril deste ano a agencia de notícias britânica Reuters trouxe a informação de que o governo chinês publicou uma nota através da Comissão Nacional de Desenvolvimento e Reforma da China (CNRD), na qual planeja aplicar uma proibição nas empresas mineradoras localizadas no país[77]. O relatório cita diversas atividades nas quais trariam inseguranças para o país, além de serem desperdícios de recursos ou poluentes.

> The draft for a revised list added cryptocurrency mining, including that of bitcoin, to more than 450 activities the NDRC said should be phased out as they did not adhere to relevant laws and regulations, were unsafe, wasted resources or polluted the environment (GOH; JUN, 2019, p.1).

Medidas como essa anunciadas pela China causaram grande agitação em todo o mercado de criptomoedas pois tal decisão pode ter impactos significativos no uso e também nos valores das criptomoedas. Uma eventual saída dos grandes mineradores da China para outros países poderá resultar em um aumento de preço das criptomoedas, resultado de tarifas de energia mais caras em outros países. Tal situação seria prejudicial ao desenvolvimento das criptomoedas pois esse aumento de preço seria resultando de uma contração na oferta, resultando em possíveis adiamentos de projetos sobre *blockchain*s.

As regulamentações propostas pela China também são desfavoráveis as criptomoedas no lado financeiro, afetando as *exchanges* chinesas e o mercado financeiro relacionado a produtos financeiros. Estas medidas governamentais são um conjunto de ações do governo chinês contrario as criptomoedas no lado da oferta e da demanda, tentando assim atingir os mineradores para que não consigam transformar suas receitas em criptomoedas na moeda local, sufocando a indústria de mineração.

---

[76] O governo chinês desfruta de ampla autoridade que ele pode trazer para os usuários nacionais de Bitcoin, trocas e mineradores. Reguladores emitiram decretos políticos para influenciar diretamente a troca de setores de mineração, e também direcionados ao Bitcoin indiretamente através de externalidades como os preços da energia

[77] Disponível em:https://www.reuters.com/article/us-china-cryptocurrency/china-says-it-wants-to-eliminate-bitcoin-mining-idUSKCN1RL0C4

A posição central do governo é não considerar as criptomoedas como moedas, retirando delas as possibilidades como meio de pagamentos no país. *The government's refusal to recognise cryptocurrency as money has been clear since December 2013 when the People's Bank of China and four other ministries and agencies issued a notice curtailing financial institutions' involvement with bitcoin*[78] (LOW, WU,2019, p.6). O não reconhecimento como uma moeda significou uma exclusão do seu sistema financeiro, tendo assim o tratamento como uma *commodity*:

> Although bitcoin is called a "currency", but as it is not issued by a monetary authority, it does not have the legal tender characteristics of a currency, and so cannot really be regarded as a true currency. Based on its characteristics, bitcoin should be treated as a form of virtual commodity that does not share the same legal status of a currency. Nor can, or should, it be circulated or used in the marketplace as a currency[79](LOW; WU, 2019, p.6).

O direcionamento Chinês em não considerar as criptomoedas como dinheiro é resultado de uma aversão aos fundamentos das moedas virtuais, direcionando uma regulação proibitiva movida aos receios sobre sua possibilidade na lavagem de dinheiro e o fato delas não serem controlados, o que levaria a instabilidades econômicas.

> After taking a relatively benign stance on Bitcoin a month prior, the Chinese Communist Party's first major restriction on the cryptocurrency came in December of 2013 and forbid financial institutions from trading the currency on the premise of its overly speculative nature. In April of 2014, the Party's next restrictive policy was driving crypto-to crypto digital exchanges out of China by not allowing such companies to operate through the central banks[80](MANN,2019, p.60).

A China então tenta sufocar as criptomoedas pelos dois lados, na oferta que é o caso dos mineradores, e na demanda que é no seu setor financeiro. Diferente do Japão que sempre viu com bons olhos as criptomoedas, a China foi para o lado sempre gerando regulações que visavam impedir o uso e a criação das moedas dentro de seu território. É questionável até que ponto isso é vantajoso para o país, já que o movimento natural agora será a saída dos mineradores do país, resultando em maiores preços no primeiro momento, mas que não irão afetar o curso de desenvolvimento das criptomoedas a longo prazo. *China's regulatory*

---

[78] A recusa do governo em reconhecer a criptomoeda como dinheiro tem sido clara desde dezembro de 2013, quando o Banco Popular da China e outros quatro ministérios e agências emitiram uma notificação restringindo o envolvimento das instituições financeiras com o bitcoin. Tradução feita pelo Autor.

[79] Embora o bitcoin seja chamado de "moeda", mas como não é emitido por uma autoridade monetária, ele não possui as características legais de uma moeda e, portanto, não pode realmente ser apreciado como uma verdadeira moeda. Ser tratado como uma forma de mercadoria virtual que não compartilha o mesmo status legal de uma moeda, nem pode ou deve ser circulada ou usada no mercado como moeda. Tradução feita pelo Autor.

[80] Depois de tomar uma posição relativamente benigna sobre Bitcoin um mês antes, a primeira grande restrição do Partido Comunista Chinês à criptomoeda veio em dezembro de 2013 e proibiu as instituições financeiras de negociar a moeda na premissa de sua natureza excessivamente especulativa. Em abril de 2014, a próxima política restritiva do Partido estava impulsionando as trocas digitais criptografadas para a criptografia fora da China, por não permitir que essas empresas operassem através dos bancos centrais.

crackdowns have seen some cryptocurrency trading activity shift to its neighbours Japan and South Korea (LOW;WU,2019, p.2). Essa mudança poderá se mostrar um erro a China pois fechar as empresas mineradoras significa transferir uma indústria que tem grande potencial de crescimento no futuro, e que no presente gera resultados positivos, pois se essas empresas se mantem no pais significa que há uma atividade viável no pais, ao criar criptomoedas para o resto do mundo usar.

4.2.3 Japão

O Japão está entre as economias mundiais mais favoráveis á adoção das criptomoedas, e entre as 10 maiores é o líder na adoção da tecnologia *blockchain*. Desde o começo da adoção das criptomoedas, o país asiático em um primeiro momento tratou com cautela seu uso no país, porém sem criar legislações proibitivas até o seu entendimento. *Japan is attempting to position itself as the leading cryptocurrency and blockchain jurisdiction* [81] (SEDGWICK,2017, p.1).

O pais é famoso entre os entusiastas das criptomoedas por permitir caixas eletrônicos localizados que trocam o dinheiro local pelo equivalente em Bitcoin, revelando um alto grau de aceitação tanto do Governo mas também da população, que tem adotado as criptomoedas como forma de pagamentos dentro do país, indo na direção contraria da China e tomando a posição de maior negociador de Bitcoin do mundo como afirmam Low e Wu: *Soon after the regulatory clampdown in China in September 2017, Japan took over from China as the leader in market share in bitcoin trading*[82](LOW;WU,2019,p.2).

Em abril de 2017 o Japão passou a aceitar as criptomoedas oficialmente como meio de pagamento em todo país, gerando mais confiança no papel das criptomoedas e seguindo a tendência do país em ter regulações que favoreçam o uso no país. *In Japan, bitcoin is recognized as 'a means of payment that is not legal currency', and in 2017, the Japanese*

[81] O Japão está tentando se posicionar como a nação pioneira na regulação de criptomoedas e *blockchains*. Tradução feita pelo Autor.
[82] Logo após a repressão regulatória na China em setembro de 2017, o Japão tomou da China a liderança em participação de mercado na negociação de Bitcoin. Tradução feita pelo Autor

government officially recognized bitcoin as a method of payment[83] (DÉCOURT *et al*, 2017, p.7).

Na prática é como se o governo japonês autorizasse uma moeda estrangeira em seu país, como o dólar, porém mantendo a sua oficial como a padrão de pagamentos. Junto com a aceitação como meio de pagamento foram criadas regras para as *exchanges*, exigindo o seguimento de regras financeiras comuns e também termos de segurança para a proteção dos dados e das moedas dos japoneses, além da necessidade da prestação de contas anuais:

> that law goes into effect on 1st April, putting in place capital requirements for exchanges as well as cybersecurity and operational stipulations. In addition, those exchanges will also be required to conduct employee training programs and submit to annual audits (KEIRNS,2017, p.1).

Com regras simples, porém bem formuladas o Japão busca ser o "paraíso" das criptomoedas neste momento de crescimento. A aceitação das criptomoedas pode ter alguma relação com Satoshi Nakamoto, que supostamente é japonês, porém a aceitação tanto social quanto governamental pode ter motivos diferentes.

A sociedade japonesa é conhecida pela sua cultura em valorizar a poupança, com tendências maiores em poupar do que consumir. O bitcoin surge para essa sociedade como um ativo que traz segurança, pois sua característica é ser uma moeda descentralizada, sem a interferência de politicas governamentais que estimulam o consumo e como consequência se muda o valor real da moeda. Já o governo japonês pode obter vantagem ao aceitar as criptomoedas na intenção de se gerar no país um polo onde se concentra o capital vindo destas moedas, que mesmo estando fora da legislação quando em criptomoedas, mas que ao passar pela economia irá gerar receita. *Japan treats the taxation of cryptocurrencies interestingly as it treats it as miscellaneous income, and not the same as income made from stocks or foreign currencies*[84] (TAKEO; TAKAHASHI.2018, p.1). Além do fator tributário há também oportunidades na criação de novas tecnologias criadas pelo avançado setor de informática e robótica japonês, podendo gerar incrementos futuros em como irá se usar as novas tecnologias das redes *blockchain* em produtos diretos para os consumidores em todo o mundo, além de atrair pessoas qualificadas das mais diversas nacionalidades para o país.

---

[83] No Japão, Bitcoin é reconhecido como um meio de pagamento que não é moeda legal, e em 2017, o governo japonês reconheceu oficialmente bitcoin como um método de pagamento. Tradução feita pelo Autor

[84] O Japão trata a taxação das criptomoedas interessantemente como renda variada, e não o mesmo que ações e moedas estrangeiras. Tradução feita pelo Autor.

O Japão conseguiu sair na frente dos seus concorrentes China e Estados Unidos quanto a regulação econômica das criptomoedas. Seu esforço em permitir que as criptomoedas cresçam porem assegurando proteção para a economia e para os usuários já estão dando resultados, como foi citado acima a tomada da liderança da China em participação de mercado. O jornal Financial Times expressou esse sentimento do mercado e dos usuários locais em relação ao país asiático: *entrepreneurs do not often welcome regulation. For Japanese cryptocurrency start-ups, however, a framework put in place by the country's financial authorities has been a boon*[85]*(*TERAZONO,2017, p.1).

O que o Japão conseguiu fazer em relação a regulamentação das criptomoedas é de fundamental importância para demonstrar que é possível, sim, gerar proteção para o país e para as pessoas sem a necessidade de interferência no curso natural das redes *blockchains*. Enquanto outros países discutem a natureza das criptomoedas e como controla-las, o Japão está um passo a frente, mostrando que é possível a conciliação entre o novo e o tradicional, trazendo vantagens para o seu país sem deixar de lado questões essenciais de políticas públicas.

4.2.4 Brasil

A regulamentação das criptomoedas no Brasil ainda está na fase de discussões no Senado Federal e na câmera Federal. A primeira reação do Estado brasileiro com a chegada das criptomoedas foi a não interferência, para que assim se fomentar discussões para a então efetiva regulação. Em um segundo momento a reação foi diferente, com regulações que visam impedir o acesso do grande capital financeiro.

A primeira iniciativa institucional brasileira sobre o sistema de criptomoedas foi feita pelo Banco Central[86], no qual emitiu uma nota alertando sobre os riscos das moedas virtuais, com destaque ao terceiro parágrafo, no qual destaca a falta de regulamentação por instituições:

---

[85] Empreendedores geralmente não recepcionam bem regulações. Para as *startups* japonesas, no entanto, a estrutura posta pelas autoridades tem sido uma benção. Tradução feita pelo Autor.

[86] BANCO CENTRAL DO BRASIL. Comunicado 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. Disponível em: http://www.bcb.gov.br/pre/normativos/busca/normativo.asp?numero=25306&tipo=Comunicado&data=19/2/2014. Acesso em: 30 jun. 2019.

> 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 (BANCO CENTRAL,2014, p.1).

Em 2015 então foi apresentado um projeto de lei[87] na qual se discutiu pela primeira vez a questão das criptomoedas no Brasil, tendo uma tendência negativa neste caso, no sentido de que o modo que foi discutido estava em um tom contrario a aprovação, mas que no final das contas não houve uma decisão definitiva e esse projeto está parado na Câmara dos Deputados.

A tendência negativa sobre as criptomoedas também era expressada pelo presidente do Banco Central, Ilan Goldfajn, que em uma entrevista concedida em 2017 emitiu sua opinião sobre o Bitcoin. Para o então presidente as criptomoedas eram bolhas e também pirâmides, já que elas não têm lastro e também não têm instituições que as davam suporte. Goldfajn analisou apenas a questão de mercado, onde de fato há uma forte volatilidade de preços, porém emitiu uma opinião sem considerar a tecnologia por trás do Bitcoin, gerando assim uma repercussão negativa nacionalmente sobre as criptomoedas:

> Não hipoteque a sua casa para comprar essas moedas virtuais", disse Ilan, pontuando que investidores estão aplicando nas bitcoins com a pura expectativa de vendê-las a preços mais altos no futuro. "É a típica bolha, a típica pirâmide, que em algum momento vai deixar de subir e vai voltar (CAMPOS; RIBEIRO *apud* GOLDFAJN,2017, p.1).

Seguindo a tendência contraria as criptomoedas, a CVM (Comissão de Valores Mobiliários) publicou um oficio em janeiro de 2018[88],na qual proibia os fundos de investimentos brasileiros a compra de criptomoedas, com a justificativa de gerar proteção para os investidores brasileiros:

> Assim e baseado em dita indefinição, a interpretação desta área técnica é a de que as criptomoedas não podem ser qualificadas como ativos financeiros, para os efeitos do disposto no artigo 2º, V, da Instrução CVM nº 555/14, e por essa razão, sua aquisição direta pelos fundos de investimento ali regulados não é permitida (CVM,2018,p.1).

---

[87] BRASIL. Projeto de Lei 2303, de 8 de julho de 2015. Dispõe sobre a inclusão das moedas virtuais e programas de milhagem aéreas na definição de "arranjos de pagamento" sob a supervisão do Banco Central.Disponível:http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=1555470.

[88] Comissão de Valores Mobiliários. Ofício Circular nº 1/2018/CVM/SIN. disponível em: http://www.cvm.gov.br/export/sites/cvm/legislacao/oficios-circulares/sin/anexos/oc-sin-0118.pdf. Acesso em 30 jun 2019

Para finalizar as citações sobre os principais pontos em como as instituições brasileiras estão tratando as criptomoedas, a Receita Federal emitiu em seu documento[89] de perguntas e respostas ao contribuinte como se deveria declarar a aquisição das moedas virtuais, sendo então declaradas como "outros bens", e não como moeda:

> As moedas virtuais (bitcoins, por exemplo), muito embora não sejam consideradas como moeda nos termos do marco regulatório atual, devem ser declaradas na Ficha Bens e Direitos como "outros bens", uma vez que podem ser equiparadas a um ativo financeiro. Elas devem ser declaradas pelo valor de aquisição (RECEITA FEDERAL,2019, p.183).

Em resumo as principais instituições brasileiras trataram a situação das criptomoedas no âmbito regulatória de forma cautelosa, sempre com desconfianças e algumas tendências negativas em relação a aceitação da nova tecnologia, de forma que não tomou medidas tão drásticas em relação ao uso individual, seguindo assim a maioria dos países do mundo em primeiro resguardar o setor financeiro e alertar sobre as potências volatilidades

A crise de 2014 pode ter ser papel em uma demora sobre a discussões em torno da regulamentação das criptomoedas, já que o pais passa ainda por uma situação de instabilidade macroeconomia que exige medidas mais urgentes e com maior repercussão para serem discutidas em um primeiro momento. A entrada de um governo que tem em sua equipe econômica uma visão mais liberal que a anterior pode trazer novas formas de ver a situação das criptomoedas, com perspectivas melhores para a aplicação e desenvolvimento de uso das tecnologias *blockchain* no Brasil.

O momento agora em junho é de retomada de discussão no legislativo brasileiro, ao se resgatar o projeto de lei de 2015 e que agora volta ao debate público. O presidente da câmara dos deputados, Rodrigo Maia, aprovou a criação de uma comissão especial[90] envolvendo senadores e deputados para se retomar o debate nacional sobre as criptomoedas.

A politica de regulamentação brasileira tem semelhanças com as politicas americanas ao não tentar afetar o usuário, e sim direcionar para a proteção daqueles que são atraídos pela publicidade gerada pelos rápidos aumentos de preço das criptomoedas. A entrada das

---

89 BRASIL. Receita Federal. Perguntas e Respostas, imposto sobre a Renda das Pessoas Físicas 2019, pergunta nº 447. Disponível em: http://receita.economia.gov.br/interface/cidadao/irpf/2019/perguntao/perguntas-e-respostas-irpf-2019.pdf

90 Rafael Gregório. Valor Investe. Senadores e Deputados irão debater as criptomoedas. Disponível em:. https://valorinveste.globo.com/mercados/cripto/noticia/2019/06/05/senadores-e-deputados-vao-debater-as-criptomoedas.ghtml . Acesso em 30 jun 2019

criptomoedas no grande mercado financeiro ainda não está permitida, gerando assim expectativas futuras sobre quando isso vai acontecer. A expectativa é positiva pois é vista pelo mercado como uma criação de regulamentações, e não de completa proteção contra as criptomoedas.

5 CONCLUSÃO

O surgimento das criptomoedas trouxe novas formas de transações e informações, gerando novas oportunidades para a sociedade e economia, e gerando preocupações sobre para os reguladores. Se de um lado há a pulsação gerada pela inovação, do outro lado está a mão forte do Estado em tentar controlar uma tecnologia totalmente nova, e que tem em sua essência a tentativa de se desconectar do poder Estatal.

Quando o Bitcoin foi criado, seu criado Satoshi Nakamoto pensou em fazer algo direcionado para o setor financeiro, que após a crise de 2008 se mostrou como algo pouco confiável na visão dele. Porém o que Nakamoto criou permitiu novas ideias sobre como usar não uma rede de transações, mas de informações. Talvez nem o próprio criado poderia imaginar que o que ele pensou como solução poderia se tornar algo com tanto potencial de penetrar as mais diversas camadas da economia e sociedade, afetando a pessoas nas mais diversas formas

O grande papel do Estado nesse momento é não atrapalhar o desenvolvimento de uma tecnologia com tanto potencial, permitindo que os setores que tenham ideias de aplicações em redes *blockchains* tenham uma segurança ao tentar criar novas formas e aplicações que irão beneficiar a todos, inclusive o próprio Estado. Defender a não interferência não significa que o Estado deve abdicar de seu papel regulador, mas criar situações onde exista controle contra crimes a sociedade, sem deixar ser tomado pelo receio do crescimento dessa nova tecnologia.

Quando uma tecnologia que tem real aplicação surge é muito difícil o controle Estatal a segurar, podendo no máximo retardar sua aplicação. Aplicativos que até pouco tem nem existiam hoje são considerados cruciais para o funcionamento das sociedades, como o WhatsApp e Uber e muitos outros. Suas inserções nas vidas das pessoas foram de forma rápida, silenciosa e agora são irreversíveis. As criptomoedas serão assim também, já que sua base de usuários é cada vez maior, e quando menos notarmos já poderemos comprar um cafezinho com Bitcoin ou qualquer outra criptomoeda.

A revolução das criptomoedas já está em curso, podendo ser a definitiva mudança de paradigma na questão monetária e na formo como se executa condições sociais envolvendo valores, podendo ser a ruptura de um sistema financeiro mundial baseado em moedas com

lastro apenas na confiança do Estado, o que pode estar gerando uma nova crise devido aos altos endividamentos das nações e ao “castelo de areia” que é a sustentação do modo como o dinheiro é visto no nosso momento. O futuro pode nos reservar uma economia onde o Estado tem menos poder, e as pessoas terão mais liberdade sobre o que elas produzem.

REFERÊNCIAS

ABADI, Joseph; BRUNNERMEIER, Markus. **National Bureau of Economic Research**, 2018. Disponível em: <https://www.nber.org/papers/w25407>. Acesso em: 02 fev. 2019

ABRAMOWICZ, Michael B. **Cryptocurrency-Based Law**. Disponível em: https://ssrn.com/abstract=2573788. Acesso em: 25 jun 2019.

BANCO CENTRAL DO BRASIL. Comunicado 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**. Disponível em: <http://www.bcb.gov.br/pre/normativos/busca/normativo.asp?numero=25306&tipo=Comunicado&data=19/2/2014>. Acesso em: 30 jun. 2019.

BARNES, Dan. Blockchain manoeuvres: applying Bitcoin's technology to banking. **The Banker**, v. 14, 2015.

BASHIR, Imran. **Mastering blockchain**. Birmingham: Packt Publishing, 2017. 504 p.

BECK, Roman *et al*. **Blockchain–the gateway to trust-free cryptographic transactions**. 2016.Dísponivelem:<https://pdfs.semanticscholar.org/ee1e/fd77e8b6287438d312b244177bb143f7a072.pdf.>. Acesso em: 21 jun. 2019.

BERG, Chris; DAVIDSON, Sinclair; POTTS, Jason. **Byzantine Political Economy**.2019. Disponivel em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3344110>. Acesso em: 25 jun. 2019.

BLANDIN, Apolline *et al*. **Global Cryptoasset Regulatory Landscape Study.** 2019. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3379219>. Acesso em: 25 abr. 2019.

BLOCKCHAIN.COM. 2019. Disponível em: <https://www.blockchain.com/en/>. Acesso em: 15 jun. 2019.

BRASIL. **Projeto de Lei 2303, de 8 de julho de 2015**. Dispõe sobre a inclusão das moedas virtuais e programas de milhagem aéreas na definição de "arranjos de pagamento" supervisão doBancoCentral.Disponível:<http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=1555470>. Acesso em: 30 jun. 2019

_____. Receita Federal. **Perguntas e Respostas, imposto sobre a Renda das Pessoas Físicas 2019**. Disponível em: <http://receita.economia.gov.br/interface/cidadao/irpf/2019/perguntao/perguntas-e-respostas-irpf-2019.pdf>. Acesso em: 30 jun. 2019.

_____. Comissão de Valores Mobiliários. **Ofício Circular nº 1/2018/CVM/SIN**. Disponível em: <http://www.cvm.gov.br/export/sites/cvm/legislacao/oficios-circulares/sin/anexos/oc-sin-0118.pdf>. Acesso em: 30 jun. 2019.

BROUWER, Eric. **Regulating Bitcoin Exchanges**: A Risk-Based Approach. 2019. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3354023>. Acesso em: 21 abr. 2019.

BUTERIN, Vitalik *et al***. A next-generation smart contract and decentralized application platform**. 2014. Disponível em: <http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf>. Acesso em: 05 abr 2019

CAMPOS, Eduardo; Ribeiro, Alex. Bitcoin é bolha e pirâmide, alerta Ilan. **Valor Economico**. 2017. Disponível em: <https://www.valor.com.br/financas/5227033/bitcoin-e-bolha-e-piramide-alerta-ilan>. Acesso em: 30 jun. 2019.

CARVALHO, Carlos Eduardo *et al*. Bitcoin, criptomoedas, blockchain: desafios analíticos, reação dos bancos, implicações regulatórias. **Fórum liberdade econômica**. São Paulo, 2017.

CATALINI, Christian; GANS, Joshua S. Some simple economics of the blockchain. **National Bureau of Economic Research**, 2016. Dísponivel em: <https://www.nber.org/papers/w22952>. Acesso em:15 jun. 2019.

CAYTAS, Joanna. Developing blockchain real-time clearing and settlement in the EU, US, and globally. **Columbia Journal of European Law**. 2016.

CHAPMAN, James T.E. *et al*. Crypto" money": perspective of a Couple of Canadian Central Bankers. **Bank of Canada**, 2019. Disponível em: <https://www.bankofcanada.ca/wp-content/uploads/2019/02/sdp2019-1.pdf>. Acesso em: 20 jun 2019

CHIU, Jonathan; KOEPPL, Thorsten V. **The economics of cryptocurrencies–bitcoin and beyond**. 2017. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3048124>. Acesso em: 12 jun 2019

COASE, Ronald H. **The nature of the firm**. Londres: Economica. 1937. 405 p.

_____. The problem of social cost. **Journal of law and economics**, v. 3, n. 1, p. 1- 44, 1960.

CONTRACTOR, Farok J. Ten Quick Facts about US Trade: Deficits and Discords. **Rutgers Business Review**, v. 3, n. 2, 2018.

CROSBY, Michael *et al*. Blockchain technology: Beyond bitcoin. **Applied Innovation**, v. 2, p. 6-10, 2016.

DAVIDSON, Laura; BLOCK, Walter. Bitcoin, o teorema da regressão e a emergência de um novo meio de troca. **MISES: Interdisciplinary Journal of Philosophy, Law and Economics**, v. 5, n. 1, p. 83-98, 2017.

DAVIDSON, Sinclair; DE FELLIPE, Primavera; POTTS, Jason. Blockchain and the Economic Institutions of Capitalism**. Journal of Institutional Economics**.2018

_____. **Economics of blockchain**. 2016. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2744751>. Acesso em: 30 mar. 2019.

DÉCOURT, Roberto Frota; CHOHAN, Usman W.; PERUGINI, Maria Letizia. Bitcoin returns and the monday effect. **Horizontes Empresariales**, v. 16, n. 2, 2017.

FRIEDMAN, Milton; FRIEDMAN, Rose. **Free to choose**: A personal statement. New York: Houghton Mifflin Harcourt, 1990. 338 p.

GOH, Brenda; JON, Alun. China wants to ban Bitocoin mining. **The Thomsom Reuters**. 2019. Disponível em: <https://www.reuters.com/article/us-china-cryptocurrency/china-wants-to-ban-bitcoin-mining-idUSKCN1RL0C4>. Acesso em: 29 jun. 2019.

GREGÓRIO, Rafael**.** Senadores e Deputados irão debater as criptomoedas. **Valor Investe** Disponível em: <https://valorinveste.globo.com/mercados/cripto/noticia/2019/06/05/senadores-e-deputados-vao-debater-as-criptomoedas.ghtml>. Acesso em: 30 jun. 2019

HE, Dong *et al*. **Virtual currencies and beyond**: initial considerations. 2016. Disponível em: <https://www.jdcoin.us/images/sdn1603.pdf>. Acesso em: 14 jun 2019

KAISER, Ben; JURADO, Mireya; LEDGER, Alex. **The Looming Threat of China**: an analysis of chinese influence on Bitcoin. 2018.Dísponivel em: <https://arxiv.org/abs/1810.02466>. Acesso em: 05 jun 2019

KEIRNS, Garret. Japan's Bitcoin Law Goes Into Effect Tomorrow. **Coindesk**. 2017. Disponível em: <https://www.coindesk.com/japan-bitcoin-law-effect-tomorrow>. Acesso em: 31 jun. 2019.

KOCHERLAKOTA, N. R. Money is memory**. Journal of Economic Theory**. 1998.

KOSBA, Ahmed *et al.* Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. **IEEE symposium on security and privacy**. 2016. p. 839-858.

LAMPORT, Leslie; SHOSTAK, Robert; PEASE, Marshall. The Byzantine generals problem. **ACM Transactions on Programming Languages and Systems (TOPLAS)**. v. 4, n. 3, p. 382-401, 1982.

LOW, Kelvin FK; WU, Ying-chieh. **The Characterisation of Cryptocurrencies in East Asia**. Cryptocurrencies in Public and Private Law, 2019. Disponivel em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3361458>. Acesso em: 04 jun 2019

MANKIW, N. Gregory. **Macroeconomia**. 3. ed.. Rio de Janeiro: Livros técnicos e Científicos Editora S.A,1997. 391 p.

MANN, Tyler J. Blockchain Technology-China's Bid to High Long-Run Growth. **Gettysburg Economic Review**, v. 11, n. 1, p. 5, 2019.

MCKINNON, Ronald I**. The unloved dollar standard**: From Bretton Woods to the rise of China. Oxford: Oxford University Press, 2013. 219 p.

MENGER, Carl. On the origins of money. **Economic journal**, v. 2, n. 6, p. 239-255, 1892.

_____. **Principles of economics**. Auburn: Ludwig Von Mises Institute,1976. 328 p.

MILNE, Alistair K. L **Cryptocurrencies from an Austrian Perspective**.2017. Disponível em: <https://ssrn.com/abstract=2946160>. Acesso em: 05 jan. 2019.

MURPHY, Robert P. The Origin of Money and Its Value. **Mises Daily**, 2003. Disponível em: <http://www.ubirataniorio.org/antigo/origin.pdf.pagespeed.ce.o_j3e6n3X3.pdf>. Acesso em: 07 jun 2019

NAKAMOTO, Satoshi. **Bitcoin**: A peer-to-peer electronic cash system. Disponível em: <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.221.9986>. Acesso em: 20 jan 2019

_____. **Bitcoin P2P e-cash paper answer**. Disponível em: <https://satoshi.nakamotoinstitute.org/emails/cryptography/1/>. Acesso em: 15 jun. 2019.

OSTROY, J. M. The informational efficiency of monetary exchange. **American Economic Review**. v. 63, n. 4, p. 597–610.

RIBEIRO, Debora Elisa**.** A (r) evolução das obrigações empresariais: do escambo ao Bitcoin e o anseio por uma regulamentação brasileira. **Revista da AMDE**, v. 13, p. 173- 189, 2017.

RICCI, Rochelle; FERNANDES, Caio. A regulamentação provisória dos patinetes elétricos, na contramão da mobilidade. **Estadão**,2019.Dísponivel em: <https://politica.estadao.com.br/blogs/fausto-macedo/a-regulamentacao-provisoria-dos-patinetes-eletricos-na-contramao-da-mobilidade/>. Acesso em: 19 jun. 2019.

SEDGWICK, Kai. Japan Teaches Western Governments a Lesson in Cryptocurrency Regulation. **News.bitcoin.com**. 2017. Disponível em: <https://news.bitcoin.com/japan-teaches-western-governments-lesson-cryptocurrency-regulation/>. Acesso em: 27 jun 2019

SHARMA, Rakesh. China intensifies crackdown on Bitcoin mining. **Investopedia**. 2019.

TELLES, Christiana Mariani da Silva. **Sistema bitcoin, lavagem de dinheiro e regulação**. 2019. 146f Tese (Doutorado em Direito) – Escola de Direito do Rio de Janeiro, Fundação Getúlio Vargas, Rio de Janeiro,2017

TERAZONO, Emiko. Bitcoin gets official blessing in Japan**. Financial Times**. 2017.Disponivel em: <https://www.ft.com/content/b8360e86-aceb-11e7-aab9-abaa44b1e130>. Acesso em: 31 jun. 2019.

THE FINANCIAL CRIMES ENFORCEMENT NETWORK (“FinCEN”). **Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies**.2013. Disponível em:< https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf>. Acesso em: 28 jun. 2019.

ULRICH, Fernando. **Bitcoin**: a moeda na era digital. São Paulo: Instituto Ludwig Von Mises Brasil, 2017. 100 p.

VON HAYEK, Friedrich August. **Denationalisation of money**: the argument refined: an analysis of the theory and practice of concurrent currencies. London: Institute of Economic Affairs,1976. 144 p.

VON MISES, Ludwig; BATSON, Harold Edward. **The theory of money and credit**. Yale University Press: New Haven,1953. 493 p.

WRIGHT, Aaron; DE FILIPPI, Primavera. Decentralized Blockchain Technology and The Rise of LEX CRYPOGRAPHY. **Electronic Journal**. 2015

YAMEY, B. S. **Scientific bookkeeping and the rise of capitalism**. **The Economic History Review**, New Series 1. 1949.

YERMACK, David. Corporate governance and blockchains. **Review of Finance**, v. 21, n. 1, p. 7-31, 2017.

ZETZSCHE, Dirk A. *et al***.** Regulating a revolution: from regulatory sandboxes to smart regulation. **Fordham J. Corp. & Fin. L**. v. 23, p. 31, 2017.