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

EDUARDO PREDEBON PEREIRA E D'ALENÇON

ANÁLISE DA ADEQUAÇÃO DO BITCOIN AO CONCEITO DE MOEDA

Porto Alegre
2019

EDUARDO PREDEBON PEREIRA E D'ALENÇON

ANÁLISE DA ADEQUAÇÃO DO BITCOIN AO CONCEITO DE MOEDA

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

Orientador: Prof. Dr. Antonio Ernani Martins Lima

Porto Alegre

2019

CIP - Catalogação na Publicação

d'Alençon, Eduardo Predebon Pereira e
Análise da adequação do Bitcoin ao conceito de moeda / Eduardo Predebon Pereira e d'Alençon. -- 2019.
58 f.
Orientador: Antonio Ernani Martins Lima.

Trabalho de conclusão de curso (Graduação) -- Universidade Federal do Rio Grande do Sul, Faculdade de Ciências Econômicas, Curso de Ciências Econômicas, Porto Alegre, BR-RS, 2019.

1. Bitcoin. 2. Blockchain. 3. Funções da moeda. I. Lima, Antonio Ernani Martins, orient. II. Título.

Elaborada pelo Sistema de Geração Automática de Ficha Catalográfica da UFRGS com os dados fornecidos pelo(a) autor(a).

EDUARDO PREDEBON PEREIRA E D'ALENÇON

ANÁLISE DA ADEQUAÇÃO DO BITCOIN AO CONCEITO DE MOEDA

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

Aprovada em: Porto Alegre, 02 de julho de 2019.

BANCA EXAMINADORA:

_____

Prof. Dr. Antonio Ernani Martins Lima - Orientador

UFRGS

_____

Prof. Dr. Leonardo Xavier da Silva

UFRGS

_____

Prof. Dr. Sabino da Silva Porto Júnior

UFRGS

“I don’t believe we shall ever have a good money again before we take the thing out of the hands of the government. We can’t take it violently out of the hands of government, all we can do is by some sly roundabout way introduce something that they can’t stop.”

F.A Hayek, 1984

RESUMO

Esta monografia tem como objetivo central uma análise do Bitcoin, visando determinar a atual adequação da criptomoeda ao conceito de moeda. Os instrumentos utilizados para a realização do trabalho foram uma análise histórica da moeda e do Bitcoin, uma análise técnica do funcionamento da criptomoeda, de suas bases teóricas, de suas vantagens e desvantagens e uma análise da adequação do Bitcoin às características e funções básicas da moeda. Assim, foi possível determinar que, mesmo que tenha surgido em 2009 como uma alternativa às moedas tradicionais em meio a um contexto de desconfiança nos bancos centrais causado, principalmente pela crise do Subprime, o Bitcoin ainda não pode ser considerado como moeda no sentido tradicional da palavra, tendo em vista que não satisfaz as funções básicas da moeda.

Palavras-chave: Bitcoin. Blockchain. Funções da Moeda.

ABSTRACT

The main objective of this undergraduate thesis is an analysis of Bitcoin, aiming to determine its current adequacy to the concept of money. The instruments utilized in the accomplishment of this paper are a historical analysis of currency and of Bitcoin, a technical analysis of the cryptocurrency, its theoretical basis, its advantages and disadvantages and an analysis of Bitcoin's adequacy to the basic characteristics and functions of money. Thus, it was possible to determine that, even though it has emerged in 2009 as an alternative to traditional currencies in a context of distrust in Central Banks caused primarily by the Subprime Mortgage Crisis, Bitcoin cannot be considered as a form of money in the traditional sense of the word yet, as it does not satisfy the basic functions of money.

Keywords: Bitcoin. Blockchain. Functions of Money.

LISTA DE FIGURAS

LISTA DE GRÁFICOS

LISTA DE QUADROS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

Ao longo da história econômica, a moeda representou, além de um simples instrumento de troca, parte da identidade dos povos pelas quais eram utilizadas. Dessa forma, sua produção esteve, na grande maioria dos casos, associada a algum tipo de poder central. Após o término dos impérios coloniais, onde a moeda da metrópole também era utilizada pelos povos dominados, iniciou-se o processo de proliferação das moedas nacionais, onde, gozando de maior liberdade, diversos países buscavam o domínio sobre os fluxos monetários em seus territórios.

Nas últimas décadas, entretanto, pode-se notar o surgimento de um processo inverso ao anterior, no qual as moedas nacionais vêm sofrendo uma relativa diminuição em sua importância. Como exemplo pode-se citar o surgimento da Zona do Euro, onde diversos países europeus abriram mão de suas moedas em troca de uma unificação monetária, e o caso de países como o Panamá e o Equador, que passaram a utilizar como moeda o Dólar. É nesse contexto, aliado a uma considerável desconfiança no sistema monetário e financeiro tradicional, que surge o Bitcoin, uma moeda altamente descentralizada e baseada em complexos sistemas de criptografia, sendo mantida em funcionamento pelos próprios usuários.

Desde sua introdução no ano de 2009, o Bitcoin vem apresentando, ainda que com significativa volatilidade, um forte ritmo de valorização. Em decorrência desse processo, a criptomoeda, inicialmente transacionada apenas em fóruns especializados em informática por entusiastas de criptografia, tornou-se conhecida ao redor do mundo, sendo transacionada nas maiores bolsas e corretoras internacionais e apresentando um valor agregado de mercado na casa das centenas de bilhões de dólares.

Em decorrência da expressiva dominância apresentada pelo Bitcoin frente às outras criptomoedas disponíveis atualmente no mercado, foi realizada a escolha de sua utilização como o representante do conjunto como um todo.

Sendo assim, para realmente entender seu funcionamento, torna-se necessária uma análise dos componentes que influenciam a demanda pela referida criptomoeda, buscando a resposta da seguinte pergunta: O Bitcoin corresponde de fato a um método inovador de pagamento ou representa apenas um novo ativo financeiro?

Dessa forma, o objetivo geral deste trabalho é, à luz da sua evolução histórica e das características de funcionamento da moeda como meio de pagamento, realizar uma análise do Bitcoin, visando a determinar a atual adequação da criptomoeda ao conceito de moeda. A importância do estudo decorre da carência de conhecimentos sobre o assunto, o que acaba por impedir uma maior compreensão sobre as dinâmicas de seu mercado, aumentando o nível de insegurança dos agentes envolvidos.

A monografia está dividida em três capítulos. O primeiro corresponde a uma análise histórica da evolução da moeda em geral e do Bitcoin em particular, com o objetivo específico de expor as motivações para a sua criação e resumir os principais acontecimentos temporais pertinentes à criptomoeda. O segundo capítulo consiste em uma análise técnica do Bitcoin, com o objetivo específico de esclarecer, além de seu método de funcionamento, suas possíveis vantagens e desvantagens e as especificidades de sua regulação. O terceiro capítulo consiste em uma análise da atual adequação do Bitcoin às três funções básicas da moeda (meio de troca, unidade de conta e reserva de valor), com o objetivo específico de buscar esclarecer se o Bitcoin pode de fato ser considerado como moeda nos dias de hoje.

A hipótese inicial utilizada é a de que o Bitcoin, ainda que no longo prazo tenha capacidade de atuar como moeda, atualmente não se adéqua ao conceito de moeda.

2 PERSPECTIVA HISTÓRICA DA MOEDA E DO BITCOIN

Ao realizar qualquer tipo de análise no âmbito das ciências sociais aplicadas, é imprescindível que se leve em conta o contexto histórico pertinente ao objeto de pesquisa. Não considerar a influência dos acontecimentos passados nas presentes relações sociais significa abrir as portas aos mais diversos erros de interpretação e simplificações exageradas.

Dessa forma, torna-se essencial para o desenvolvimento do presente trabalho uma contextualização histórica do Bitcoin a partir da breve história da moeda. Este capítulo tratará dos principais acontecimentos temporais relacionados à moeda e à citada criptomoeda, buscando formar não apenas uma simples linha do tempo de acontecimentos, mas sim um instrumento através do qual o leitor torna-se capaz de extrair as motivações e dinâmicas por trás do Bitcoin.

Os assuntos abordados no capítulo serão o surgimento e evolução da moeda como facilitador de trocas, a criação das primeiras criptomoedas, a criação do Bitcoin por Satoshi Nakamoto, o considerável uso do Bitcoin em mercados ilícitos durante sua fase inicial, o surgimento das criptomoedas alternativas e a evolução de preços do Bitcoin.

2.1 SURGIMENTO DA MOEDA

2.1.1 Moeda Mercadoria

As primeiras moedas, longe da sofisticação apresentada em dias atuais, tomavam a forma de simples mercadorias, possuindo, além de valor de troca, valor de uso. Dessa forma, para que a mercadoria apresentasse a ampla aceitação necessária como instrumento de troca para seu funcionamento como moeda, uma ampla aceitação da utilidade de seu uso também se fazia necessária (LOPES E ROSSETTI, 2005).

As mercadorias escolhidas como instrumento de troca dependiam fortemente da estrutura do mercado em questão, variando de sociedade para sociedade. O quadro abaixo exemplifica algumas das moedas-mercadorias utilizadas ao longo da história:

Quadro 1: Principais moedas-mercadorias ao longo da história econômica.

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

Fonte: (LOPES E ROSSETTI, 2005, p.30).

2.1.2 Moeda Metálica

A partir do aumento de complexidade dos mercados e do crescente número de mercadorias transacionadas, surge a necessidade de formas mais desenvolvidas

de moeda. Entre as mercadorias utilizadas, os metais foram, ao longo do tempo, adquirindo significativa importância.

Além de possuírem grande resistência a danos externos, as características físicas dos metais possibilitavam o processo de cunhagem, essencial para o processo de evolução da moeda. Através da cunhagem, as unidades da moeda são vinculadas a um agente emissor e produzidas de forma padronizada, garantindo sua aceitabilidade (ORRELL E CHLUPATÝ, 2016).

Inicialmente, os metais utilizados para a confecção de moedas eram não-preciosos, como cobre, bronze e ferro. Entretanto, devido à grande abundância natural apresentada pelos referidos metais e ao aperfeiçoamento das técnicas de fundição utilizadas em seus processamentos, eles apresentaram significativas flutuações em seus valores, comprometendo seu uso. A solução para este problema foi a adoção do ouro e da prata, metais suficientemente escassos que garantiam a estabilidade dos preços ao longo do tempo (LOPES E ROSSETTI, 2005).

Ainda que não sejam mais amplamente utilizados como moeda nos dias de hoje, os metais preciosos ainda representam importantes métodos de reserva de valor, especialmente em tempos de turbulência financeira.

2.1.3 Moeda-Papel

O sistema monetário baseado em metais preciosos, ainda que representasse um grande avanço frente às moedas-mercadorias, apresentava algumas deficiências, como é exemplificado pelo parágrafo abaixo.

> Com a multiplicação das trocas entre regiões e países diferentes, manifestaram-se alguns inconvenientes da moeda metálica como instrumento de pagamento. O transporte de metais a longas distâncias tornou-se relativamente difícil (em decorrência do peso) e sujeito a riscos (em decorrência de roubos). Pela precariedade das estradas e dos meios de transporte e, sobretudo, pelos riscos envolvidos no porte de metais preciosos desenvolveram-se esforços para a criação e a difusão de instrumentos monetários mais flexíveis que, ao mesmo tempo em que contornassem os inconvenientes da moeda metálica, também facilitassem a efetivação de operações de crédito. Ademais, as relações comerciais só poderiam desenvolver-se se esse novo instrumento monetário passasse a ser aceito de forma ampla, ainda que tivesse a necessária contrapartida de lastro metálico integral. (LOPES E ROSSETTI, 2005, p. 32).

Em decorrência destas inconveniências, surgiram os certificados de depósito, emitidos por instituições que guardavam, sob garantia, as quantias em metais

preciosos. Com a proliferação destes certificados de depósito, institui-se a chamada moeda-papel, uma forma representativa de moeda com lastro total e plena garantia de conversibilidade (LOPES E ROSSETTI, 2005).

2.1.4 Moeda Fiduciária

Após a popularização da moeda-papel, tornou-se claro para as instituições emissoras dos certificados de depósito que, como os detentores não solicitavam a reconversão de seus certificados ao mesmo tempo, o lastro total não era necessário. Dessa forma, fazendo uso da confiança dos agentes econômicos em relação à solidez das instituições emissoras, certificados com lastro inferior a 100% começaram a ser emitidos. Essa nova forma de certificado resultou na criação do chamado papel-moeda, uma das formas mais importantes da moeda ao longo de sua evolução histórica (LOPES E ROSSETTI, 2005), (ORRELL E CHLUPATÝ, 2016).

O papel moeda, entretanto, também passou por transformações ao longo do tempo. Ainda que possuísse lastro metálico parcial em suas fases iniciais, a inflexibilidade trazida pela necessidade da posse de metais pelo agente emissor para a emissão de novas unidades da moeda motivou à instituição, ainda que de forma gradual, de notas inconversíveis. A partir de 1971, com o fim do lastro do dólar em ouro, todos os sistemas monetários de relevância para o mercado internacional operam de forma puramente fiduciária (LOPES E ROSSETTI, 2005).

2.1.5 Moeda Bancária

Em meio ao contexto de hegemonia apresentado pelo papel-moeda, surge, de forma acidental, uma nova forma de moeda constituída, basicamente, de depósitos monetários em instituições bancárias. Um dos primeiros exemplos de moeda bancária pode ser observado na Inglaterra do século XIX, onde a expressiva movimentação de depósitos bancários por meio de cheques causou, devido ao efeito multiplicador de tais depósitos, uma significativa expansão dos meios de pagamento disponíveis aos agentes econômicos (LOPES E ROSSETTI, 2005).

Ao longo do tempo, a moeda bancária sofreu grandes alterações. Com a popularização da internet e dos sistemas digitais, passou a apresentar um caráter

majoritariamente virtual, tomando a forma de arquivos computacionais nos servidores das instituições bancárias (ORRELL E CHLUPATÝ, 2016).

Nos dias atuais, o expressivo uso da moeda bancária juntamente à moeda fiduciária torna evidente um processo de desmaterialização da moeda. A moeda, antes representada por produtos ou metais distancia-se cada vez mais de uma representação física.

2.2 PRIMEIRAS CRIPTOMOEDAS

Somando-se a esse processo de desmaterialização, é importante considerarmos o papel da criptomoeda, uma forma puramente eletrônica de meio de pagamento que busca romper com os limites e restrições das moedas tradicionais de curso forçado. Embora o conceito de criptomoeda apenas tenha ganhado popularidade através do Bitcoin, sua gênese ocorreu décadas antes, através do desenvolvimento de suas bases teóricas essenciais.

A maior inovação tecnológica das criptomoedas é o uso da tecnologia *blockchain*, um sistema ponto-a-ponto (*peer-to-peer*) que funciona como uma espécie de registro público onde todas as transações são adicionadas. As informações contidas no *blockchain* são de livre acesso por todos os usuários do sistema, conferindo alto nível de transparência às transações (CROSBY *et al*, 2016).

Devido ao uso do *blockchain*, as criptomoedas possibilitam que tanto o cliente quanto o servidor desempenhem o mesmo papel no mesmo nível de atuação, dispensando a existência de um nodo central de processamento (VICENTE, 2017).

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

O primeiro exemplo de moeda digital criptografada foi o Ecash, proposto por David Chaum no ano de 1983 através do artigo “*Blind signatures for untraceable payments*”. Motivado por preocupações acerca da privacidade e segurança de transações monetárias por meio de sistemas bancários eletrônicos, Chaum

introduziu um novo sistema de criptografia capaz de, segundo o autor, criar um sistema automatizado de pagamentos marcado pelas seguintes características:

> -Incapacidade de agentes externos determinarem o beneficiário, horário ou quantidade de pagamentos realizados por um indivíduo.
> -Capacidade de indivíduos fornecerem provas de pagamento, ou determinarem a identidade do beneficiário sob situações excepcionais.
> - Capacidade de interromper o uso de meios de pagamento reportados como roubados. (CHAUM, 1983, p 199-200).

A ideia foi posta em prática por Chaum no ano de 1990 através da fundação da empresa *Digicash*. Ainda que tenha atraído pesados investimentos de *venture capital* em sua fase embrionária, o insatisfatório desempenho do *Ecash* levou a *Digicash* a declarar falência no ano de 1998 (BUNTINX, 2016).

Outro importante precursor para o Bitcoin é o *B-Money*. Introduzido no ano de 1998 através do artigo "*B-money, an anonymous, distributed electronic cash system*" publicado por Wei Dai, o *B-Money*, ainda que nunca tenha sido de fato posto em prática, operaria de maneira fortemente similar à grande maioria das criptomoedas atuais.

Em seu artigo, Wei Dai descreve o *B-Money* como um instrumento a partir do qual indivíduos anônimos poderiam realizar transações monetárias entre si sem o auxílio de terceiros. Para tanto, o autor propôs a utilização de um sistema similar ao *blockchain*, com a necessidade de processamento computacional e verificação pública para a validação das transações e criação de novas unidades da moeda (BUNTINX, 2016).

Ainda no ano de 1998, Nick Szabo introduz o *BitGold*, em uma tentativa de emular as características positivas do ouro no que diz respeito à sua função como reserva de valor ao mesmo tempo em que buscava eliminar seus problemas, como seu alto nível de volatilidade.

Sendo baseado em uma rede descentralizada de agentes econômicos anônimos e assegurada por criptografia, o *BitGold* foi concebido como um instrumento capaz de fornecer independência de instituições financeiras e facilitar a realização de transações através de fronteiras nacionais (BUNTINX, 2016).

Ainda que, assim como o *B-Money*, o *Bitgold* nunca tenha sido de fato implementado como meio de troca, ele é visto como uma das principais influências para o desenvolvimento do Bitcoin aproximadamente 10 anos mais tarde.

2.3 SURGIMENTO DO BITCOIN

O Bitcoin foi introduzido de maneira teórica através do artigo "*Bitcoin: A Peer-to-Peer Electronic Cash System"* escrito pelo pseudônimo Satoshi Nakamoto no ano de 2008. A criptomoeda representava, segundo o autor, um novo meio através do qual agentes econômicos poderiam realizar transações monetárias sem a dependência de instituições financeiras, proporcionando, além de maior agilidade e menores custos de transação, maior segurança aos envolvidos.

Para tanto, o Bitcoin faz uso da tecnologia *blockchain*[1], um sistema que funciona como uma espécie de registro público onde todas as transações são adicionadas. As informações contidas no *blockchain* são de livre acesso por todos os usuários do sistema, conferindo alto nível de transparência às transações (CROSBY *et al*, 2016).

Como são descentralizadas, não dependendo de um órgão emissor de moeda, novas unidades são geradas de maneira endógena, a partir de um processo chamado mineração[2]. Através desse processo, os usuários utilizam o poder de cálculo de seus computadores para adicionar registros de transações ocorridas no *blockchain* em troca de retornos em unidades da criptomoeda, garantindo, além da criação de novas unidades monetárias, a manutenção do próprio sistema como um todo (ULRICH, 2014).

Devido a um nível crescente de dificuldade no processo de mineração - onde, com o passar do tempo, mais poder de cálculo é exigido dos computadores- é possível estimar-se com precisão a oferta da moeda, oferecendo uma maior estabilidade ao sistema. No código base do Bitcoin, Nakamoto estipulou um limite máximo de 21 milhões de unidades da moeda, patamar que, de acordo com previsões baseadas na taxa média de evolução da capacidade de processamento dos computadores, deverá ser alcançada em torno do ano 2140 (FRASCAROLI E PINTO, 2016).

[1] O *blockchain* será explicado em maiores detalhes no terceiro capítulo.
[2] A mineração será explicada em maiores detalhes no terceiro capítulo.

A rede de Bitcoins foi inaugurada de fato no dia 03 de janeiro de 2009, após Satoshi Nakamoto minerar seu primeiro bloco, chamado de Bloco Genesis. A primeira transação verificada de Bitcoins foi realizada nove dias após a criação do Bloco Genesis, quando Satoshi Nakamoto enviou 10 unidades da moeda para Hal Finney, criador do primeiro sistema de *proof-of-work* reutilizável, a base da verificação digital das criptomoedas.

Ao longo do primeiro ano de vida do Bitcoin, as transações realizadas serviram, basicamente, como testes da solidez da rede do *blockchain*. Apenas no ano de 2010, através de uma postagem no fórum bitcointalk.com, Laszlo Hanyecz realizaria a primeira troca entre Bitcoins e bens reais. Hanyecz ofertou 10.000 BTC em troca de duas pizzas grandes da pizzaria *Papa John's*, que, na época, totalizavam cerca de 30 dólares.

2.4 MERCADO ILÍCITO

Uma das maiores fontes de polêmica acerca das criptomoedas, com especial destaque para o Bitcoin, é seu potencial uso para transações de natureza ilícita. O elevado nível de anonimato oferecido pela moeda torna-a extremamente atrativa para uso como meio de troca em mercados ilícitos.

O principal exemplo de uso de Bitcoins para tal fim foi o caso do *Silk Road*, site fundado por Ross Ulbricht no início de 2011. O site foi o primeiro mercado digital de grande relevância da *Darknet* - parte da internet acessível apenas através de programas especializados onde os usuários operam de forma anônima. Para assegurar a não rastreabilidade dos pagamentos realizados na plataforma, o Silk Road utilizava como moeda obrigatória para a realização de transações o Bitcoin.

O site possuía regras internas contra a venda de determinados produtos ou serviços, como, por exemplo, pornografia infantil, dados de cartões de crédito, armas de fogo e assassinatos. Ainda assim, estima-se que aproximadamente 70% das transações realizadas através do *Silk Road* envolviam algum tipo de entorpecente ilícito.

Após quase três anos de funcionamento, o *Silk Road* foi fechado pelo FBI (*Federal Bureau of Investigation*) após a prisão de seu fundador, no dia 02 de outubro de 2013. Ulbricht, acusado de, entre outros delitos, lavagem de dinheiro e

invasão de computadores, foi condenado à prisão perpétua sem possibilidade de condicional.

Segundo dados do processo contra Ulbricht, entre 06 de fevereiro de 2011 e 23 de julho de 2013, 1.229.465 transações foram realizadas através da plataforma, totalizando uma receita de 9.519.465 Bitcoins, dos quais 614.305 foram coletados pelo site em forma de comissão sobre produtos vendidos. As transações realizadas através do *Silk Road* eram de tamanha significância para o mercado de Bitcoins em geral que, no dia do fechamento do site, o preço da moeda inicialmente apresentou uma queda de quase 30%, com subsequente valorização motivada por especulação.

O gráfico abaixo retrata a grande variação de preço do Bitcoin com fechamento do *Silk Road*:

Gráfico 1: Variação de preço do Bitcoin após o fechamento de Silk Road.

Fonte: BITCOINCHARTS. Disponível em: <https://commons.wikimedia.org/wiki/File:Bitcoin_October_2013.png>.

2.5 ALTCOINS

Ainda que nos dias de hoje o número de criptomoedas esteja na casa dos milhares, durante um longo período de tempo - entre janeiro de 2009 e meados de 2011 - o Bitcoin foi a única criptomoeda disponível no mercado.

Apenas em abril de 2011, mais de dois anos após a introdução do Bitcoin ao mercado, surge a primeira das chamadas altcoins, as criptomoedas alternativas. A moeda em questão, disponível até os dias de hoje, é chamada de *Namecoin*. A *Namecoin* é baseada no código base do Bitcoin, possuindo o mesmo limite de 21 milhões de unidades e utilizando o mesmo sistema de função *hash*[3] no processo de criptografia dos dados.

Devido à necessidade de diferenciação originada pelo alto nível de competição apresentado pelo mercado de criptomoedas após a popularização do conceito, tornou-se comum a introdução de novas funcionalidades - além das básicas já apresentadas pelo Bitcoin - às moedas desenvolvidas.

Entre essas criptomoedas alternativas munidas de funcionalidades adicionais, podemos citar:

a) Ethereum: Introduzida ao mercado apenas em 2015, a criptomoeda tem como principal característica de diferenciação a possibilidade de introduzir contratos ao próprio *blockchain*;

b) Litecoin: Criada por Charles Lee, ex-engenheiro da Google, a criptomoeda possibilita, devido a alterações no protocolo de formação dos blocos da *blockchain*, transações muito mais ágeis. Enquanto o tempo médio de confirmação das transações realizadas por Bitcoin gira na casa dos dez minutos, transações via Litecoin geralmente são confirmadas em apenas dois minutos.

No que diz respeito à capitalização de mercado, o Bitcoin ainda apresenta uma expressiva dominância frente às altcoins. Segundo dados do *website coinmarketcap.com,* o Bitcoin representa, em junho de 2019, 56% da capitalização total das criptomoedas, possuindo um valor agregado de 156 bilhões de dólares. Em comparação, a segunda criptomoeda no ranking, a Ethereum, apresenta uma capitalização de apenas 28 bilhões de dólares, menos de 20% do valor total do Bitcoin.

A figura abaixo lista as quinze maiores criptomoedas em termos de capitalização de mercado:

[3] Função matemática usada no processo de criptografia. Será explicada em mais detalhes no terceiro capítulo.

Figura 1: Ranking das 15 maiores criptomoedas.

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply
1	Bitcoin	$156.192.219.508	$8.794,01	$18.862.913.432	17.761.212 BTC
2	Ethereum	$28.627.524.799	$268,79	$8.438.522.825	106.504.649 ETH
3	XRP	$17.407.002.056	$0,409558	$1.363.994.178	42.501.950.124 XRP *
4	Litecoin	$8.531.052.134	$137,07	$4.386.984.006	62.239.451 LTC
5	Bitcoin Cash	$7.467.588.480	$418,59	$1.644.710.390	17.839.763 BCH
6	EOS	$6.302.853.597	$6,86	$2.473.773.623	919.263.604 EOS *
7	Binance Coin	$4.611.374.615	$32,66	$462.319.986	141.175.490 BNB *
8	Bitcoin SV	$3.749.405.941	$210,20	$412.342.208	17.837.711 BSV
9	Tether	$3.450.434.609	$1,00	$18.464.702.281	3.437.125.225 USDT *
10	Stellar	$2.443.481.344	$0,125899	$332.532.750	19.408.200.674 XLM *
11	Cardano	$2.373.790.822	$0,091556	$166.641.552	25.927.070.538 ADA
12	TRON	$2.165.277.592	$0,032472	$661.396.618	66.682.072.191 TRX
13	Monero	$1.592.863.968	$93,46	$228.159.538	17.043.676 XMR
14	Dash	$1.368.446.282	$154,33	$312.088.879	8.866.887 DASH
15	IOTA	$1.210.314.075	$0,435438	$38.390.129	2.779.530.283 MIOTA *

Fonte: COINMARKETCAP. Disponível em:<https://coinmarketcap.com/>.

2.6 EVOLUÇÃO DOS PREÇOS DO BITCOIN

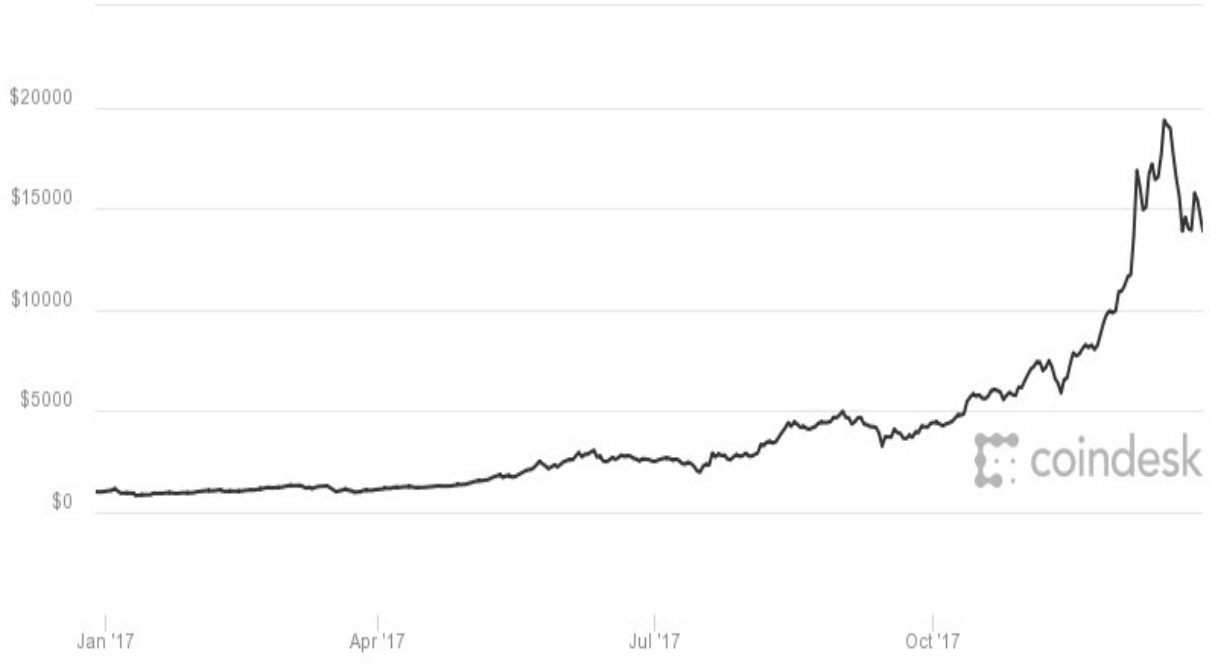
Uma das características mais marcantes do Bitcoin é a extrema volatilidade apresentada por seus preços.

Partindo de um valor inicial inferior a US$ 0,01, quando Laszlo Hanyecz trocou 10.000 BTC por duas pizzas, o Bitcoin apenas alcançou paridade com o dólar em 09 de fevereiro de 2011. Ainda em 2011, o Bitcoin apresentou sua primeira bolha, atingindo brevemente o patamar de US$ 31,00 e voltando a cair para US$ 2,00.

O ano de 2012, entretanto, foi um período de relativa calmaria nos preços da criptomoeda. Após iniciar em baixa devido à queda apresentada no final de 2011, o Bitcoin passou o restante do ano em uma constante valorização, atingindo, no mês de dezembro, o valor de aproximadamente US$ 13,00 por unidade da moeda.

Após o período de calmaria, o Bitcoin apresentou, durante o ano de 2013, grandes variações de preço. Devido ao aumento de popularidade da moeda, o valor por unidade ultrapassou pela primeira vez a casa dos US$ 1.000,00. Durante período entre 2014 e 2016 o preço da criptomoeda manteve-se, com significativas oscilações, entre US$ 200,00 e US$ 1.000,00.

Gráfico 2: Evolução do preço do Bitcoin no ano de 2017.



Fonte: COINDESK. Disponível em: <https://www.coindesk.com/>.

O ano de 2017, retratado no gráfico acima, foi, sem sombra de dúvidas, o período de maior valorização desde a criação da criptomoeda. Após iniciar o ano no patamar de US$ 900,00, o Bitcoin iniciou uma trajetória extremamente positiva,

alcançando, após meses de euforia, o valor máximo de US$ 19.783,21 em 17 de dezembro. O valor, entretanto, não se sustentou. Dias após beirar os US$ 20.000,00 o preço da criptomoeda recuou para menos de US$ 11.000,00, terminando o ano com significativa volatilidade.

Diferentemente de 2017, o ano de 2018 trouxe grandes quedas ao preço do Bitcoin. Após iniciar o período com um preço de mercado beirando os US$ 13.000,00, a criptomoeda manteve ao longo de todo o ano uma acentuada queda, perdendo aproximadamente 70% de seu valor, terminando dezembro abaixo dos US$ 4.000,00.

Após manter-se no patamar de US$ 4.000,00 durante os três primeiros meses de 2019, o Bitcoin inicia, no mês de abril, uma forte valorização. Ao final do primeiro semestre do ano, período no qual o presente trabalho foi desenvolvido, a criptomoeda atingiu US$ 12.000,00, seu maior valor desde dezembro de 2017.

3 ANÁLISE DO BITCOIN

Realizada a contextualização histórica do Bitcoin, o próximo passo é a realização de uma análise mais aprofundada dos constituintes técnicos da criptomoeda. Este capítulo tratará das principais bases para o funcionamento do Bitcoin, familiarizando o leitor com as peculiaridades do sistema como um todo.

Entre os assuntos abordados estão o problema do gasto-duplo, as bases teóricas do *blockchain*, o processo de mineração, a carteira de Bitcoins, possíveis vantagens e desvantagens de seu uso e também a regulação de criptomoedas.

3.1 PROBLEMA DO GASTO-DUPLO

O surgimento das moedas digitais trouxe um novo desafio a ser superado. Diferentemente das moedas tradicionais, que possuem uma representação física, as moedas digitais consistem basicamente em arquivos de computador. Como qualquer outro tipo de arquivo, tais arquivos podem ser infinitamente copiados e distribuídos pela rede. Dessa forma, surge o problema do gasto-duplo (ULRICH, 2014).

O duplo gasto ocorre quando, após criar novas unidades da moeda digital a partir da cópia da unidade original, o indivíduo realiza múltiplas transações usando dinheiro que não deveria existir.

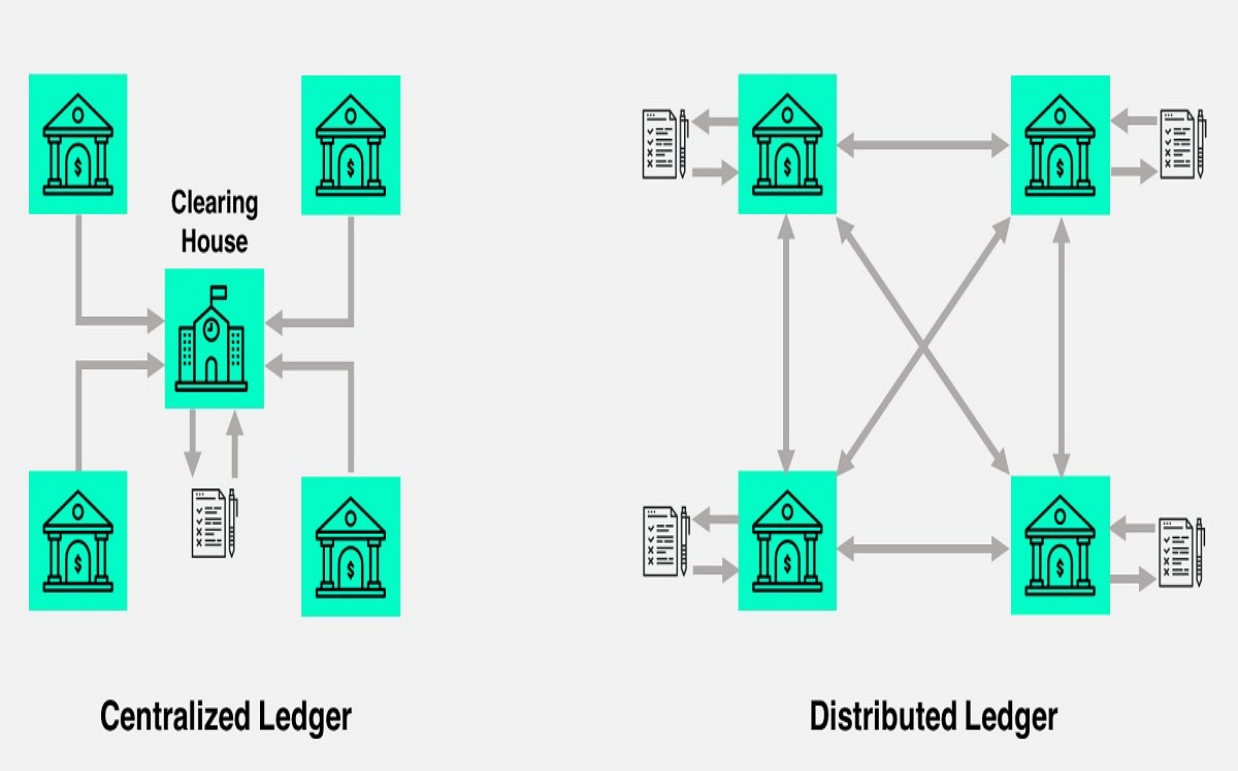
Tradicionalmente, o método utilizado para contornar o problema do gasto-duplo é a utilização de instituições financeiras, que atuam como nodos centrais de processamento, verificando a validade de cada transação realizada. É precisamente devido a esta grande concentração de poder que o sistema como um todo se torna vulnerável. Supondo que a segurança digital da instituição financeira seja comprometida, agentes mal-intencionados teriam completo controle sobre as transações ocorridas e sobre as informações privadas dos clientes (ULRICH, 2014).

Um exemplo prático da situação supracitada ocorreu em outubro de 2018. Após conseguirem invadir os sistemas do banco HSBC, *hackers* obtiveram acesso às informações pessoais - incluindo nome, data de nascimento, número de conta, saldo disponível e histórico de transações - de clientes do banco nos Estados Unidos.

Tal vulnerabilidade foi um dos principais motivadores para a criação de métodos descentralizados para a resolução do gasto duplo. Entre os métodos disponíveis, o de maior relevância é o *blockchain,* explicado com maiores detalhes abaixo.

A figura abaixo retrata de maneira gráfica as diferenças entre o fluxo de informações entre o método centralizado e o descentralizado para a solução do problema.

Figura 2: Comparação entre o método centralizado e o descentralizado.



Fonte: (BELIN). Disponível em: <https://tradeix.com/distributed-ledger-technology/>.

3.2 BLOCKCHAIN

Assim como já foi citado anteriormente, o *blockchain* é a principal inovação tecnológica presente no Bitcoin. O *blockchain* corresponde, de maneira resumida, a uma espécie de livro-registro onde todas as transações da criptomoeda são armazenadas. Como correspondem a uma rede descentralizada, as informações do *blockchain* não são armazenadas apenas em um lugar. Cada agente conectado à rede possui uma copia completa do arquivo (CROSBY *et al*, 2016).

O *blockchain* tem como uma de suas principais bases teóricas o conceito de funções *hash*, algoritmos matemáticos utilizados para transformar dados dos mais variados tamanhos (*inputs*) em dados com um tamanho fixo (*outputs*). A função *hash* utilizada pelo Bitcoin é unilateral, ou seja, não é possível determinar o *input* a partir do *output*. Dessa forma, o único modo de determinar o *input* correto para a função *hash* do Bitcoin é através de tentativa e erro, no processo chamado de mineração (CROSBY *et al*, 2016).

As informações do *blockchain* são armazenadas na forma de uma corrente de blocos, cada um contendo um determinado número de transações. Novos blocos são introduzidos ao final do último bloco já existente, garantindo a continuidade do sistema (CROSBY *et al*, 2016).

Para garantir a confiabilidade das informações contidas no *blockchain*, cada novo bloco é verificado através de um consenso entre os agentes envolvidos. Desta forma, o único modo possível de manipular as informações introduzidas na corrente é possuir 51% do poder de processamento total dos computadores conectados ao sistema, algo que, devido à grande quantidade de agentes envolvidos, torna-se inviável. Após serem introduzidas no sistema por meio dos blocos, as informações das transações realizadas não podem ser apagadas, tornando manipulações de registros passados impossíveis (NAKAMOTO, 2008).

Uma das principais características do *blockchain* é o elevado nível de anonimato por ele proporcionado. Cada agente é identificado apenas através de sua chave pública, uma sequência de caracteres que atua como uma forma de pseudônimo na rede (ULRICH, 2014). A chave pública não é associada a qualquer informação de pessoa física, impossibilitando a identificação de seu dono.

3.3 MINERAÇÃO

Mineração é o nome dado ao processo de introdução de novos blocos à corrente do *blockchain*. É através da mineração que a rede do Bitcoin é mantida em funcionamento e novas unidades da criptomoeda são criadas. A mineração ocorre de maneira descentralizada, de forma que todos podem participar do processo.

Cada novo bloco da criptomoeda contém a solução para um quebra-cabeça criptográfico envolvendo a função *hash* do último bloco, o *hash* das transações

contidas no novo bloco e um endereço (chave pública) a ser creditado com a recompensa pela mineração (EYAL E SIRER, 2018).

A figura abaixo corresponde aos últimos blocos criados até a data de consulta, no dia 04 de junho de 2019.

Figura 3: Últimos blocos minerados.

Height	Time	Relayed By	Hash	Size (kB)
579221 (Main Chain)	2019-06-04 16:59:52	BTC.com	00000000000000000001155da7809166b2500ad55fb631ad2f6c9ce39a1ec458e	1,257.17
579220 (Main Chain)	2019-06-04 16:50:43	Unknown	00000000000000000142c8473517358bfa43e37561d947b496a53ff62340dd9	1,196.9
579219 (Main Chain)	2019-06-04 16:44:36	Unknown	00000000000000000001b04a1783ee8266c61926faf016d3c42ae71478c96c71a	1,150.41
579218 (Main Chain)	2019-06-04 16:40:46	BTC.com	00000000000000000026aca9b062f1cffa3dde6087d8468060c2db2e1816758	1,326.63
579217 (Main Chain)	2019-06-04 16:40:02	ViaBTC	00000000000000000001f590b2d58a656078363a9c13884aa2c50b2c3f789f3c6	1,333.34
579216 (Main Chain)	2019-06-04 16:12:37	AntPool	00000000000000000000c30d728fb600eebb088d1a73c9029cc6e9d6426c9efe1	1,275.09
579215 (Main Chain)	2019-06-04 15:51:30	BTC.com	00000000000000000000068d30b0b296f7476ed43f37099f1ae2e2bec1dbb5b3d5	1,233.78
579214 (Main Chain)	2019-06-04 15:41:08	BTC.TOP	00000000000000000001386d22faf52a9f3990e0c5b2ecbbbdcbb98f12f3ffe60	1,228.26
579213 (Main Chain)	2019-06-04 15:33:34	AntPool	00000000000000000001dd1472fec7f4445793dcfad73ec938013966cf74e9ca1	1,184.06
579212 (Main Chain)	2019-06-04 15:32:36	SlushPool	00000000000000000010a00e9d79ca5798b3bea2ef67727c816f7a4c11eb7632	1,316.87
579211 (Main Chain)	2019-06-04 15:25:02	AntPool	00000000000000000001df1de6827211af0fd4001b58441e96766b3cdd95c0ab3	1,400.6

Fonte: BLOCKCHAIN. Disponível em: <https://www.blockchain.com/btc/blocks>.

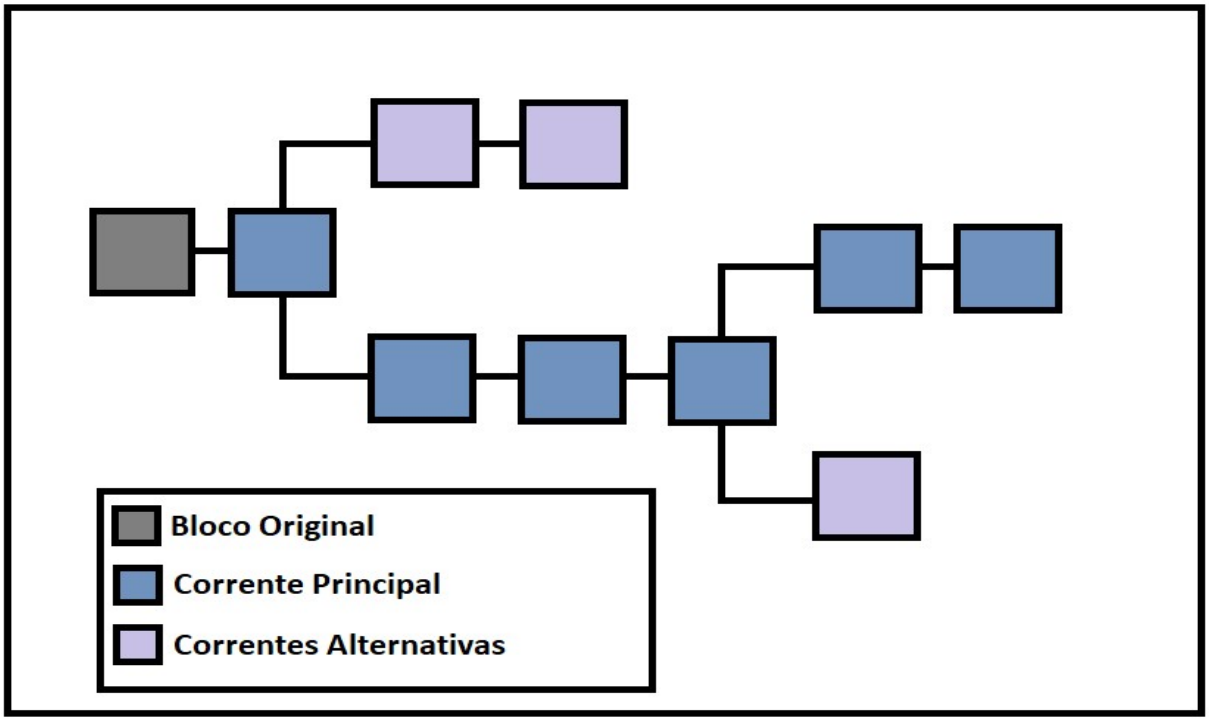
Para manter a oferta de Bitcoins em um ritmo constante de crescimento, a dificuldade do quebra-cabeça criptográfico é constantemente ajustada, baseando-se na velocidade de criação dos últimos blocos. Dessa maneira, mesmo com o expressivo avanço do poder de processamento dos computadores, o tempo entre os blocos se manterá constante em aproximadamente 10 minutos (CROSBY *et al*, 2016).

No caso de dois mineradores criarem simultaneamente blocos baseados no mesmo bloco anterior, a corrente sofre uma bifurcação, tornando possível a adição de novos blocos a ambas as pontas. Devido à necessidade de um consenso sobre a ordem das transações acontecidas, tal bifurcação representa algo a ser combatido pelo sistema. Para impedir a proliferação de correntes alternativas, o protocolo do Bitcoin obriga os mineradores a minerarem apenas a corrente com o maior número

de blocos. No caso de as correntes apresentarem o mesmo comprimento, a primeira a ser encontrada deve ser minerada. Dessa forma, as correntes alternativas são prontamente cortadas. As transações contidas nessas correntes são ignoradas (EYAL E SIRER, 2018).

A figura abaixo é uma representação gráfica simplificada do processo de bifurcação da corrente principal do *blockchain*.

Figura 4: Bifurcações no *blockchain*.



Fonte: Elaboração própria.

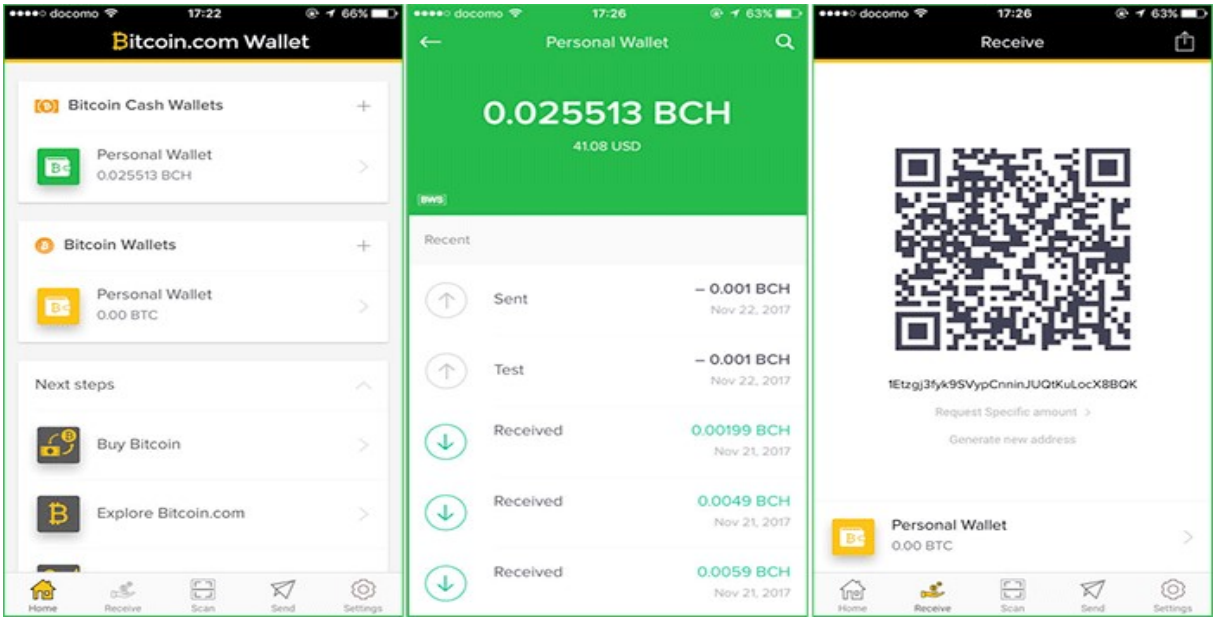
Como a probabilidade de um agente resolver o quebra-cabeça necessário para a mineração é diretamente proporcional ao poder de processamento empregado, torna-se conveniente aos envolvidos a formação de grupos de mineração. Nesses grupos, o poder de processamento de todos os seus constituintes é unido, aumentando consideravelmente as chances de resolução do quebra-cabeça. Ainda que o ganho esperado não seja alterado, devido à divisão igualitária dos rendimentos, o ingresso em grupos de mineração diminui consideravelmente a variância dos rendimentos, tornando a receita muito mais previsível (EYAL E SIRER, 2018).

3.4 CARTEIRA DIGITAL

A Carteira de Bitcoin é, basicamente, um programa de computador que possibilita ao usuário, além de enviar e receber unidades da moeda, ter acesso ao seu saldo e histórico de transações.

O download da carteira pode ser realizado de diversas fontes, apresentando algumas diferenças entre suas funcionalidades. Um exemplo de carteira de Bitcoin pode ser visto na figura abaixo:

Figura 5: Exemplo de carteira digital.



Fonte: (ADHIYA, 2019). Disponível em: <https://www.igeeksblog.com/best-iphone-ipad-bitcoin-wallet-apps/>.

Através do download da carteira, o usuário obtém acesso à sua chave pública, utilizada como método de identificação na rede, e à sua chave privada, utilizada para acessar a carteira em questão e validar as transações realizadas.

É importante ressaltar que tais chaves representam o único modo de ter acesso à carteira. Dessa forma, é imprescindível que o usuário as mantenha seguras, sob pena de perda do acesso aos seus fundos. Estima-se que aproximadamente 20% de todas as unidades do Bitcoin estejam em carteiras perdidas, fora de circulação no mercado (KRAUSE, 2018).

3.5 VANTAGENS

Supondo a ampla utilização do Bitcoin, na qual tanto grandes transações como compras corriqueiras são realizadas através de seu uso, considero pertinente citar uma série de vantagens obtidas pelos agentes econômicos quando contrastada com a utilização das moedas tradicionais:

3.5.1 Falta de inflação

Devido ao limite estabelecido ao número máximo de unidades monetárias imposto pelos algoritmos de criptografia, não há a possibilidade de inflação inesperada causada por um aumento da base monetária, como costumeiramente ocorre com moedas nacionais (IVASCHENKO, 2016).

3.5.2 Descentralização

Devido à ausência de um controle central, não há a possibilidade de imposição de regras aos donos das criptomoedas. Além disso, a rede de trocas continua ativa mesmo que seja perdida a conexão com algumas das partes (CROSBY *et al*, 2016).

3.5.3 Possibilidades ilimitadas de transações

Como as transações são realizadas a partir de um sistema descentralizado, não podem ser controladas ou canceladas de maneira exógena (IVASCHENKO, 2016).

3.5.4 Baixo custo de operação

Como as operações são realizadas sem a exigência de um intermediário financeiro, os custos de transação são extremamente reduzidos, figurando em média 0,1% do valor transacionado (IVASCHENKO, 2016), (ULRICH, 2014).

3.5.5 Anonimato e transparência

As operações de criptomoedas, ao mesmo tempo que são completamente transparentes, tendo em vista que todos os registros ficam disponíveis ao público através do uso do *blockchain*, são completamente anônimas, protegendo a identidade dos agentes envolvidos (ULRICH, 2014).

3.5.6 Velocidade de transação

Através do sistema ponto-a-ponto, onde as transações são mantidas através do processamento de mineradores, as trocas ocorrem e são validadas em minutos. Mais especificamente, estudos estatísticos através dos *logs* de transação são capazes de estimar que em mais de 90% dos casos as transações são confirmadas em menos de 30 minutos (IVASCHENKO, 2016).

3.5.7 Impossibilidade do uso de dados pessoais para fraude

Quando comparado aos outros métodos de realização de compras via internet, com especial enfoque nos cartões de crédito, as criptomoedas apresentam nível de segurança muito maior. Enquanto os meios tradicionais requerem uma série de dados pessoais do comprador para a validação da operação, o único dado requerido pelas criptomoedas é o número da carteira de onde os fundos serão retirados (IVASCHENKO, 2016).

3.5.8 Facilidade de uso

Quando comparado aos procedimentos necessários para a abertura de contas, tanto para pessoa física quanto jurídica, em bancos tradicionais, as criptomoedas são muito mais simples. Enquanto a abertura de contas em bancos é um procedimento burocratizado e demorado, um usuário pode criar uma carteira de criptomoedas e realizar sua primeira transação em meros minutos (IVASCHENKO, 2016).

3.6 DESVANTAGENS

Ainda que a lista de vantagens da utilização do Bitcoin seja extensa, é fantasioso esperar que qualquer método monetário seja completamente livre de riscos. Sendo assim, faz-se necessária também uma análise das possíveis desvantagens trazidas por sua utilização.

3.6.1 Grande nível de volatilidade

Devido aos poucos anos de existência e popularidade do Bitcoin, o mercado ainda necessita de maior nível de maturidade. Quando comparadas às principais divisas atualmente utilizadas, como o dólar americano e o euro, a criptomoeda apresenta flutuações de preço consideravelmente maiores. Somando-se a isso, decisões tomadas por governos centrais a respeito das regulações impostas ao sistema em seus territórios são capazes de influenciar fortemente o preço de venda da criptomoeda, como pode ser exemplificada pela proibição pelo governo chinês no final do ano de 2013 da utilização de Bitcoin pelas instituições financeiras oficiais (OLIVEIRA, TOTTI E NEY, 2014).

3.6.2 Maior risco nos investimentos e contratos de médio e longo prazo

Devido à supracitada volatilidade apresentada pelo Bitcoin, investimentos de médio e longo prazo tornam-se muito mais complicados, visto que não há como realizar projeções satisfatórias sobre seus valores. Além disso, contratos de longo prazo em Bitcoin tornam-se praticamente inviáveis, frequentemente exigindo a ancoragem em moedas tradicionais mais estáveis (IVASCHENKO, 2016).

3.6.3 Menor segurança frente a roubos virtuais

Como as operações de Bitcoin são realizadas sem um intermédio confiável e de maneira anônima, basta que o criminoso consiga acesso a uma carteira particular para que os fundos possam ser transferidos de maneira imediata e não-rastreável. Somando tal fato com a não existência de seguros de depósito, os riscos de *hacking* são consideráveis (YERMACK, 2013).

3.6.4 Incentivos a atividades ilícitas

Devido ao alto nível de anonimato oferecido pelo sistema de criptomoedas, neste caso o Bitcoin, sua utilização torna muito mais simples as transações relacionadas às transações ilícitas, como a compra de entorpecentes, encomenda de crimes e lavagem de dinheiro (YERMACK, 2013).

3.7 REGULAÇÃO DE CRIPTOMOEDAS

A descentralização apresentada pelo Bitcoin é, ao mesmo tempo, o fator mais forte e a maior origem de riscos do sistema. Ainda que possibilite uma maior agilidade no processamento das transações e maior nível de privacidade, essa descentralização, além de tornar o sistema mais suscetível a flutuações de mercado, gera insatisfação por parte de diversos governos, levando, em alguns casos, a restrições e proibições legais.

Um dos mais famosos exemplos dessa insatisfação ocorreu no final do ano de 2013 na China onde, subitamente, o governo decretou a proibição do uso de Bitcoin pelas instituições financeiras oficiais, acarretando em uma desvalorização de mais de 50% do preço da moeda em apenas duas semanas. A cotação de uma unidade do Bitcoin passou de US$ 1147,25 no dia 04 de dezembro para US$ 522,23 no dia 18 do mesmo mês (OLIVEIRA, TOTTI E NEY, 2014).

Entretanto, mesmo que exemplos como o exposto acima sejam abundantes, a moeda, após a perturbação inicial no nível de preços, volta a se estabilizar, atestando uma considerável solidez do mercado monetário em questão. No caso da intervenção chinesa, menos de um mês após alcançar o patamar de US$ 522,23, a cotação da moeda já atingia valores superiores a US$ 800,00 (OLIVEIRA, TOTTI E NEY, 2014).

Ainda que em países totalitários a decisões análogas à tomada pelo governo Chinês sejam uma possibilidade, um dos aspectos mais distintivos do Bitcoin, e das criptomoedas em geral, quando comparado com as moedas tradicionais, é a extrema dificuldade encontrada pelos governos de regulá-lo. Segundo Ulrich, as razões são:

> Isso ocorre porque o Bitcoin não se encaixa em definições regulamentares existentes de moeda ou outros instrumentos financeiros ou instituições, tornando complexo saber quais leis se aplicam a ele e de que forma.
>
> O Bitcoin tem as propriedades de um sistema eletrônico de pagamentos, uma moeda e uma commodity, entre outras. Dessa forma, estará certamente sujeito ao escrutínio de diversos reguladores. Vários países estão atualmente debatendo o Bitcoin em nível governamental. Alguns já emitiram pareceres ou pronunciamentos oficiais, estabelecendo diretrizes, orientações, etc. Uns com uma postura neutra, outros de forma mais cautelosa.
>
> Embora não seja o foco deste livro averiguar qual o tratamento legal adequado, é oportuno afirmar que as questões legais certamente afetarão a forma como o Bitcoin se desenvolve ao redor do mundo. Em países desenvolvidos, as incertezas sobre como o Bitcoin será regulado pouco a pouco se dissolvem. (ULRICH, 2014, p.33).

Figura 6: Situação legal do Bitcoin ao redor do mundo em 2018.

Fonte: (AMOROS, 2018). Disponível em: <https://howmuch.net/articles/bitcoin-legality-around-the-world>.

A partir da análise da figura acima, torna-se evidente a ampla legalidade do Bitcoin no mercado internacional. Restrições legais à sua utilização concentram-se

apenas em países tradicionalmente conhecidos pelo autoritarismo e reduzida liberdade econômica.

4 VALIDADE DO BITCOIN COMO MOEDA

O presente capítulo tem como objetivo específico realizar uma análise da atual validade do Bitcoin como moeda, visando a obter maior entendimento seu papel no sistema econômico.

Primeiramente, para que análise apresente o embasamento teórico necessário, é necessária uma definição mais rigorosa sobre o que uma moeda de fato representa. Em decorrência disso, a primeira sessão do capítulo tratará de aspectos técnicos relacionados à moeda, contemplando, além de sua definição básica, suas principais características e funções.

Em seguida, a análise se dará a partir do contraste entre as características e funções supracitadas e as atuais apresentadas pelo Bitcoin, buscando clarificar se a referida criptomoeda atende, ou não, os requisitos para que possa ser considerada como moeda.

4.1 CARACTERÍSTICAS DA MOEDA

Ainda que qualquer bem, supondo que exerça as funções básicas supracitadas, possa ser considerado como moeda, algumas características são essenciais:

4.1.1 Indestrutibilidade e Inalterabilidade

Um dos aspectos mais importantes para o bom funcionamento de uma moeda é sua durabilidade física. É imprescindível que a moeda não se deteriore ao ser manuseada pelos agentes econômicos durante a realização das trocas. Dessa forma, o material do qual a moeda é composto deve ser durável, possibilitando a manutenção de suas funções básicas por mais tempo (LOPES E ROSSETTI, 2005). Além disso, a indestrutibilidade e a inalterabilidade são de extrema importância no combate à falsificação, contribuindo para a manutenção da confiança dos agentes envolvidos e para a aceitação geral da moeda em questão (LOPES E ROSSETTI, 2005).

4.1.2 Homogeneidade

Para que os agentes econômicos envolvidos nas relações de troca possam chegar a um acordo sobre o valor representado pela moeda, diferentes unidades da moeda em questão devem ser indistinguíveis umas da outras. Supondo a utilização de moedas de ouro por uma determinada economia, cada unidade da moeda deve ser rigorosamente igual, possuindo a mesma composição, cunhagem e peso. Diferenças entre as unidades da moeda podem levar a desentendimentos sobre o valor representado. Por exemplo, na economia supracitada, caso uma moeda apresente uma quantidade maior de ouro do que outra, torna-se possível que, aos olhos dos agentes envolvidos, as duas unidades não possuam o mesmo valor (LOPES E ROSSETTI, 2005).

4.1.3 Divisibilidade

Para que possa ser utilizada em transações de diversos tamanhos, a moeda deve possuir uma quantidade suficientemente grande de múltiplos e submúltiplos (LOPES E ROSSETTI, 2005). Por exemplo, supondo que na economia brasileira menor unidade de valor fosse um real, qualquer transação de bens abaixo deste valor se tornaria impossível. Entretanto, o oposto também é verdadeiro. A moeda deve possuir múltiplos suficientemente grandes para que transações de grande porta não sejam prejudicadas. Voltando ao caso da economia brasileira, se a maior cédula disponível para os agentes econômicos fosse a de um real, transações corriqueiras passariam a requerer volumes consideráveis da moeda.

Como exemplo prático da última situação, pode-se citar a Alemanha da República de Weimar, onde, devido a uma hiperinflação criada pela turbulência do pós-guerra, as cédulas do Marco Alemão possuíam tão pouco valor que chegavam a ser varridas na rua como lixo. Na tentativa de corrigir a situação, o governo frequentemente aumentava o valor das cédulas impressas. No auge do processo de hiperinflação, cédulas com o valor nominal de 100 trilhões de Marcos Alemães foram impressas (FRENCH E CHRISTOFF-KURAPOVNA, 2015).

4.1.4 Transferibilidade

Uma característica essencial para o bom funcionamento da moeda é a facilidade com que suas unidades podem ser transferidas entre os agentes econômicos. Como é apontado por Lopes e Rossetti na citação abaixo, a moeda escolhida não deve apresentar identificações a respeito de seu dono, característica que acabaria por prejudicar a realização das transações monetárias.

> Se a moeda estiver materializada em uma mercadoria qualquer ou em uma cédula emitida e garantida pelo Estado, é desejável que tanto a mercadoria quanto a cédula não tragam quaisquer registros que identifiquem seu atual possuidor. Recorrendo mais uma vez ao clássico exemplo do gado, sua utilização como moeda-mercadoria ficaria prejudicada se cada um de seus sucessivos proprietários tivesse necessidade de gravar a fogo sua marca na pele do animal. Ao cabo de certo número de transações, não restariam mais espaços para novas marcas. O mesmo aconteceria caso as transferências de cédulas se processassem unicamente via endosso de um possuidor para outro. (LOPES E ROSSETI, 2005, p. 27).

4.1.5 Facilidade de Manuseio e Transporte

A última, e não menos importante, característica essencial a ser apresentada pela moeda é ser de fácil manuseio e transporte. Dessa forma, moedas demasiadamente pesadas ou que exijam volumes exagerados para a realização de transações acabam atuando como um empecilho à realização de transações. Novamente utilizando um exemplo de Lopes e Rossetti (2005), o principal motivo da substituição de metais não precisos pelo ouro e prata para uso como moeda esteve relacionado, basicamente, com o significativamente maior valor por unidade de peso apresentado pelos últimos dois metais.

4.2 FUNÇÕES DA MOEDA

4.2.1 Meio de Troca

A função mais importante da moeda é sua utilização como intermediária de trocas, tendo em vista que proporcionou uma resolução ao problema da coincidência

de interesses. Em economias marcadas pela prática do escambo, torna-se necessário, para que a troca aconteça, que ambos os envolvidos apresentem interesse na mercadoria em posse do outro. Por exemplo, suponha que o indivíduo A viva em uma economia de escambo e seja um produtor de leite, possuindo uma quantidade da mercadoria superior ao necessário para seu consumo. Para cada troca a ser realizada pelo indivíduo A, ele deverá encontrar algum outro indivíduo que possua um excesso da mercadoria desejada e aceite trocar uma determinada quantia desta por leite. Evidentemente, como o ser humano necessita de um número significativo de produtos para sua sobrevivência, o indivíduo A se encontraria em uma situação extremamente complicada.

A moeda como intermediária de trocas, ao introduzir uma mercadoria amplamente desejada por todos os agentes econômicos, possibilitou a surgimento de um maior grau de especialização e de divisão social do trabalho, ocasionando em significativos ganhos de produtividade econômica e aumento na qualidade de vida da sociedade em geral (LOPES E ROSSETTI, 2005).

Além disso, a possibilidade da realização de trocas indiretas, nas quais a compra e a venda ocorrem em momentos distintos, possibilitou uma significativa redução no tempo necessário para a realização das transações entre os agentes econômicos. Como os bens são trocados pela moeda, que é amplamente aceita, não é mais necessário o gasto de tempo com a procura de outros indivíduos com interesses coincidentes (LOPES E ROSSETTI, 2005).

4.2.2 Medida de Valor

Em economias de escambo, o único modo de obter o valor de um determinado produto é através da comparação com outros produtos no mercado. Este sistema de valoração se torna extremamente complicado à medida que o número de produtos disponíveis no mercado aumenta, devido ao aumento geométrico apresentado pelas possíveis relações de troca (LOPES E ROSSETTI, 2005).

O quadro abaixo exemplifica o expressivo crescimento apresentado pelas relações de troca a partir de variações nos produtos disponíveis no mercado:

Tabela 1: Número de relações de troca.

Produtos disponíveis (n)	Número de relações de troca (RT)
20	190
50	1.225
100	4.950
200	19.900
500	124.750
1.000	499.500

Fonte: (LOPES E ROSSETTI, 2005, p. 21).

Dessa forma, a criação de uma unidade padrão de medida para o valor das mercadorias torna-se de vital importância para o desenvolvimento do mercado e da economia como um todo. A existência de uma unidade de conta torna as informações essenciais para uma atuação econômica racional muito mais acessíveis, proporcionando elevados ganhos de eficiência aos envolvidos (LOPES E ROSSETTI, 2005).

Somando-se a isso, o uso da unidade de medida para o valor dos produtos possibilita a criação de sistemas de contabilidade nacional para o cálculo dos fluxos macroeconômicos, facilitando o planejamento e administração da economia (LOPES E ROSSETTI, 2005).

4.2.3 Reserva de Valor

A última função básica da moeda é a reserva de valor, através da qual a moeda preserva seu valor de compra ao longo do tempo. Com a separação entre a compra e a venda em decorrência das trocas indiretas, é importante que os agentes econômicos tenham a possibilidade de guardar para o futuro seus poderes de compra.

Ainda que tal função não seja exclusivamente realizada pela moeda, tendo em vista que ativos não monetários também preservam seu valor ao longo do tempo, a utilização da moeda apresenta consideráveis benefícios. Diferentemente dos outros ativos, que possuem níveis variados - e incertos - de liquidez, a moeda é plenamente líquida por definição (LOPES E ROSSETTI, 2005).

A importância da liquidez da moeda é trazida à tona a partir do lançamento da Teoria Geral do Emprego, dos Juros e da Moeda por John Maynard Keynes no ano de 1936. Devido à introdução pelo autor da incerteza como um componente essencial nas relações econômicas, a preferência pela liquidez, apresentada pelos agentes quando confrontados com um futuro incerto, toma papel de destaque nas análises econômicas (LOPES E ROSSETTI, 2005).

4.3 VALIDADE DO BITCOIN COMO MOEDA

A principal motivação por trás da criação do Bitcoin foi, segundo seu criador, introduzir ao mercado monetário uma alternativa às moedas tradicionais, que são suscetíveis às flutuações nas políticas econômicas dos países emissores. Ainda assim, antes que o Bitcoin realmente possa ser considerado como moeda, torna-se necessária uma análise a respeito do seu cumprimento das supracitadas características e funções básicas da moeda.

4.3.1 Características da Moeda

No que diz respeito às características básicas para o bom funcionamento de uma moeda, o Bitcoin é, sem dúvida alguma, exitoso.

Como não possui representação física, existindo apenas através dos registros no blockchain, cada unidade do Bitcoin é infinitamente durável, não podendo ser destruída ou danificada através de seu uso. Somando-se a isso, as unidades do Bitcoin são completamente indistinguíveis entre si, sendo plenamente homogêneas.

Sobre a divisibilidade, cada Bitcoin pode ser dividido em incontáveis partes. A menor subdivisão do Bitcoin é o Satoshi, que corresponde a uma unidade da criptomoeda dividida por cem milhões.

Como as transações de Bitcoin são realizadas puramente via internet, unidades da criptomoeda podem ser transacionadas por indivíduos em lados opostos do globo com extrema facilidade, eliminando a necessidade de transporte.

Como pode ser visto no quadro abaixo, presente no livro Bitcoin: A moeda da era digital, escrito por Fernando Ulrich no ano de 2014, o Bitcoin, ao menos no que diz respeito às suas características básicas, apresenta expressivas vantagens quando comparado ao ouro ou ao papel-moeda.

Quadro 2: Comparação das características do Bitcoin com ouro e papel-moeda.

Atributos	Ouro	Papel-moeda	Bitcoin
1. Durabilidade	Alta	Baixa	Perfeita
2. Divisibilidade	Média	Alta	Perfeita
3. Maleabilidade	Alta	Alta	Incorpóreo
4. Homogeneidade	Média	Alta	Perfeita
5. Oferta (Escassez)	Limitada pela natureza	Ilimitada e controlada politicamente	Limitada matematica-mente
6. Dependência de terceiros fiduciários	Alta	Alta	Baixa ou quase nula

Fonte: (ULRICH, 2014, p.67).

4.3.2 Funções da Moeda

Devido à sua natureza puramente digital, com total ausência de lastro, o valor do Bitcoin é puramente derivado de sua utilidade como instrumento de troca. Ainda que o número de transações de Bitcoin realizadas através de corretoras seja considerável, estima-se que a grande maioria seja composta por trocas entre especuladores (YERMACK, 2013). Em seu artigo, "*Is Bitcoin a Real Currency? an Economic Appraisal*", Yermack cita uma entrevista realizada por Fred Ersham, fundador de uma das maiores empresas de carteiras digitais, na qual o empresário afirma que aproximadamente 80% de todas as transações realizadas através de sua plataforma são relacionadas à especulação

O uso da referida criptomoeda para a realização de transações não especulativas pelos agentes econômicos é dificultado pelo reduzido número de comerciantes que a aceitam como moeda de troca. No dia a dia, nem mesmo os mais ferrenhos defensores do Bitcoin a utilizam a criptomoeda para a realização de suas transações corriqueiras (LUTHER E WHITE, 2014). Yermack aponta, ainda, que mesmo para os poucos comerciantes que aceitam realizar transações por meio

do Bitcoin - em sua maioria empresas relacionadas a serviços ligados ao próprio mercado das criptomoedas - as transações envolvendo a referida criptomoeda representam uma raridade.

Outro obstáculo para a ampla utilização do Bitcoin em transações diárias é a dificuldade de obtenção de unidades da criptomoeda. Como o processo de mineração é dominado por supercomputadores, o método mais fácil de obtenção de unidades do Bitcoin é através de corretoras, que frequentemente possuem baixa liquidez e *spreads* significativos (YERMACK, 2013)

Dessa forma, o Bitcoin não performa de maneira satisfatória a função básica de intermediar as trocas entre os agentes econômicos. Ainda que nos últimos anos o Bitcoin tenha passado por aumentos exponenciais em sua popularidade, a criptomoeda está longe de representar, como pretendia seu criador, um meio de troca universalmente aceito e capaz de substituir as moedas tradicionais.

Para que uma moeda possa atuar de maneira satisfatória como unidade de conta, um nível mínimo de estabilidade de preços é requerido. É necessário que os agentes econômicos tenham a capacidade de compreender o valor realmente expressado pelas unidades da moeda. No caso do Bitcoin, a grande volatilidade apresentada pela criptomoeda compromete essa compreensão.

Gráfico 3: Exemplo de volatilidade de preços do Bitcoin.

Fonte: COINBASE. Disponível em: <https://www.coinbase.com/price/bitcoin>.

O gráfico acima expressa as variações de preço do Bitcoin durante o período de uma semana, entre os dias 31 de maio de 2019 e 06 de junho de 2019. A partir de sua análise, torna-se evidente que o Bitcoin não é adequado para uso como unidade de conta. Por exemplo, suponha que um vendedor anuncie a venda de um determinado produto por 10 unidades de Bitcoin no dia 02 de junho. Menos de 24 horas mais tarde seu produto apresentaria um valor drasticamente diferente.

Outro fator que impede a utilização do Bitcoin como unidade de conta é o elevado valor nominal de cada unidade da criptomoeda. Quando cada unidade da moeda representa um valor na casa dos milhares de dólares, transações corriqueiras de baixo valor necessitarão do uso de várias casas decimais, dificultando o processo tanto para o vendedor quanto para o comprador (YERMACK, 2013).

Ainda que seja desconsiderada por grande parte das análises a respeito da função reserva de valor, a capacidade dos agentes econômicos protegerem, ou não, suas reservas monetárias é de vital importância. Em moedas tradicionais, essa proteção pode ser realizada através de seu armazenamento em locais seguros, como, por exemplo, em cofres.

No caso do Bitcoin, entretanto, a proteção contra roubos é significativamente mais complexa. O Bitcoin, assim como as outras criptomoedas, possui caráter puramente virtual, carecendo de qualquer representação física. Dessa forma, o único método de armazenamento é através das carteiras digitais, que, assim como qualquer sistema na internet, são passíveis de *hacking*. O exemplo mais relevante de roubo de carteiras digitais aconteceu em fevereiro de 2014, quando a corretora Mt. Gox, na época a maior corretora de criptomoedas do mundo, teve aproximadamente 750.000 unidades de Bitcoin roubadas.

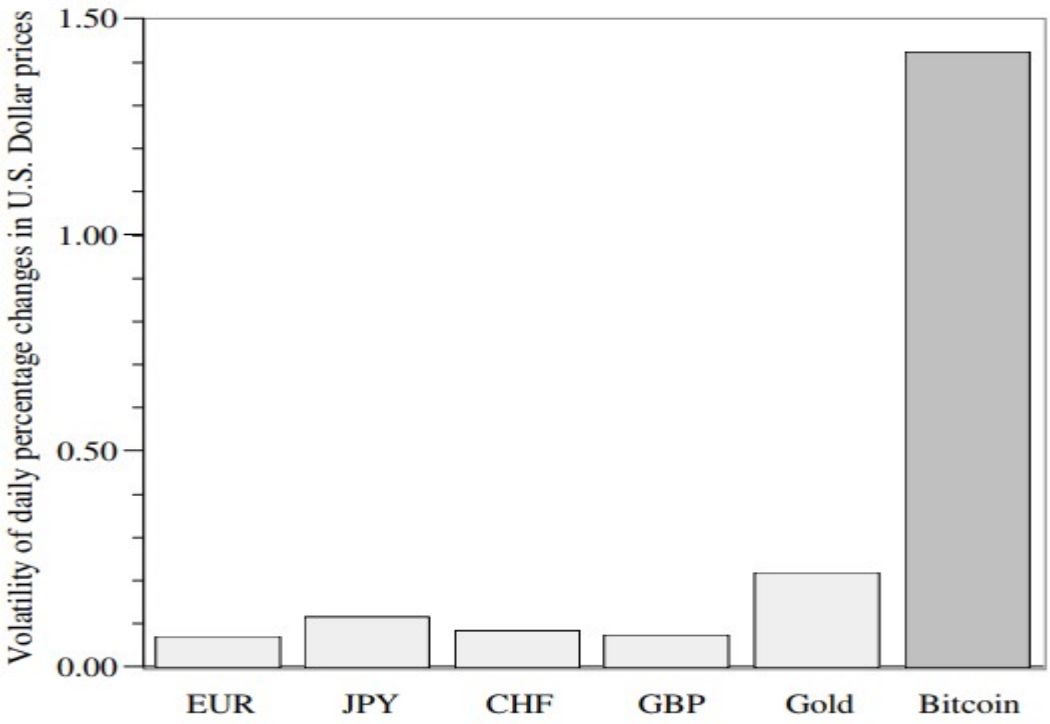
O gráfico abaixo retrata a variação de preço do Bitcoin logo após o Mt. Gox suspender todas as ordens de retirada da criptomoeda em sua plataforma. A expressiva desvalorização do preço de mercado do Bitcoin atesta a importância do evento ocorrido.

Gráfico 4: Variação de preços do Bitcoin após o fechamento de Mt. Gox.

Fonte: COINDESK. Disponível em: <https://www.coindesk.com>.

Somando-se à dificuldade de armazenamento seguro do Bitcoin, a expressiva volatilidade da criptomoeda gera considerável risco aos seus possuidores. As frequentes e drásticas flutuações de preço apresentadas pelo Bitcoin tornam a manutenção de seu valor incerta até mesmo no curto prazo.

Gráfico 5: Volatilidade do Bitcoin durante o ano de 2013.



Fonte: (YERMACK, 2013, p.21).

O gráfico acima, presente no artigo “Is *Bitcoin a Real Currency? An Economic Appraisal*”, escrito por David Yermack, ainda que possua dados relativamente antigos, aponta para a extrema diferença entre a volatilidade do Bitcoin quando comparada com as principais moedas tradicionais - Euro, Iene Japonês, Franco Suíço e Libra Esterlina - e o ouro quando comparado com o Dólar Americano. A partir da agregação de dados diários do ano de 2013, a volatilidade média do Bitcoin chegou ao patamar de 142%, enquanto as moedas se mantiveram na faixa de 7% a 12% e o ouro a 22%.

5 CONCLUSÃO

A concepção da moeda como instrumento facilitador de trocas foi, sem sombra de dúvidas, uma das maiores invenções da história humana. Resolvendo o problema da dupla incidência de interessas, a moeda possibilitou o desenvolvimento e aumento da complexidade dos mercados e, por consequência, das próprias sociedades que as utilizassem.

Ao longo da história econômica, a moeda tomou diversas formas, refletindo aspectos das sociedades pelas quais eram utilizadas. Mais recentemente, é possível notar um significativo processo de desmaterialização da moeda, na qual a importância sua representação física é fortemente diminuída.

O Bitcoin, surgido no ano de 2009, representa o início da mais recente etapa do processo de desmaterialização da moeda. Embora tenha apresentado um início conturbado, marcado por diversas bolhas especulativas, escândalos de segurança e uso em transações ilícitas, o Bitcoin experienciou um exponencial aumento em sua popularidade nos últimos anos. Nos dias atuais, apresenta uma capitalização de mercado na casa das centenas de bilhões de dólares, sendo transacionado ao redor de todo o mundo.

Baseando seu método de funcionamento no *blockchain*, uma espécie de livro registro público protegido através criptografia, o Bitcoin alia conceitos econômicos a um alto nível de sofisticação matemática e computacional, representando a possibilidade de um novo sistema monetário altamente descentralizado e independente.

Devido ao seu caráter puramente virtual, o uso do Bitcoin como moeda é capaz de conferir diversas vantagens como, por exemplo, maior agilidade nas transações, menores custos de transação, independência de políticas monetárias nacionais e um elevado nível de anonimato. Entretanto, assim como qualquer sistema monetário, também apresenta suas desvantagens. Entre elas é possível citar a elevada volatilidade apresentada pela referida criptomoeda e a possibilidade de roubos eletrônicos.

Ainda assim, sua própria validade como moeda está longe de representar um consenso entre a comunidade econômica. Ainda que apresente consideráveis vantagens quando comparado com moedas tradicionais no que diz respeito às suas

características básicas, o Bitcoin ainda não é capaz de atuar satisfatoriamente como intermediário de trocas, unidade de valor e reserva de valor. Dessa forma, ainda é demasiadamente cedo para que possa ser considerado como uma moeda. Em seus moldes atuais, o Bitcoin corresponde ao primeiro exemplo de uma nova classe de ativos financeiros formada pelas criptomoedas.

O futuro do Bitcoin dependerá da capacidade de adaptação da criptomoeda frente aos desafios encontrados. Para que possa se consolidar como moeda, necessitará de uma expressiva redução em sua volatilidade, aumento em seus níveis de segurança e maior aceitação pelo varejo.

REFERÊNCIAS

ADHIYA, D. **Best Bitcoin Wallet Apps for iPhone and iPad in 2019:** Get Complete Control of Your Private Keys, 2019. Disponível em: <https://www.igeeksblog.com/best-iphone-ipad-bitcoin-wallet-apps/>. Acesso em: 24 mai. 2019.

AMOROS, R. **Mapped:** Bitcoin's Legality Around The World. Disponível em: <https://howmuch.net/articles/bitcoin-legality-around-the-world>. Acesso em: 01 jun. 2019.

BELIN, O. **The Difference Between Blockchain & Distributed Ledger Technology.** Disponível em: <https://tradeix.com/distributed-ledger-technology/>. Acesso em: 10 jun. 2019.

BITCOINCHARTS. Disponível em: <https://commons.wikimedia.org/wiki/File:Bitcoin_October_2013.png>. Acesso em: 02 jun. 2019.

BLOCKCHAIN. Disponível em: <https://www.blockchain.com/btc/blocks>. Aceso em: 29 mai. 2019.

BOFF, S. O; FERREIRA, N. A. Análise dos benefícios sociais da bitcoin como moeda. **Anu. Mex. Der. Inter**, México , v. 16, p. 499-523, dic. 2016 . Disponível em <http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-46542016000100499&lng=es&nrm=iso>. Acesso em: 04 jun. 2019.

BRITO, J; CASTILLO, A. **Bitcoin**: A Primer for Policymakers. Arlington: Mercatus Center at George Mason University, 2016. Disponível em < https://www.mercatus.org/system/files/gmu_bitcoin_042516_webv3_0.pdf> Acesso em: 18 mai. 2019.

BUNTINX, J. P. **Top 4 Cryptocurrency Projects Created Before Bitcoin**, 2016. Disponível em: <https://themerkle.com/top-4-cryptocurrency-projects-created-ahead-of-bitcoin/>

CHAUM, D. Blind signatures for untraceable payments. **Advances in Cryptology**, p. 199-203, 1983. Disponível em: <https://sceweb.sce.uhcl.edu/yang/teaching/csci5234WebSecurityFall2011/Chaum-blind-signatures.PDF>. Acesso em: 25 mai. 2019.

COINBASE. Disponível em: <https://www.coinbase.com/price/bitcoin>. Acesso em: 14 mai. 2019.

COINDESK. Disponível em: <https://www.coindesk.com/>. Acesso em: 12 jun. 2019.

COINMARKETCAP. Disponível em:<https://coinmarketcap.com/>. Acesso em: 14 jun.2019.

CROSBY, M. *et al*. Blockchain Technology: Beyond Bitcoin. **Applied Innovation Review**, vol. 2, 2016. Disponível em <https://j2-capital.com/wp-content/uploads/2017/11/AIR-2016-Blockchain.pdf>. Acesso em: 17 mai. 2019.

D'ALFONSO, A; LANGER, P; VANDELIS, Z. **The Future of Cryptocurrency:** An Investor's Comparison of Bitcoin and Etherium, 2016. Disponível em <https://www.economist.com/sites/default/files/the_future_of_cryptocurrency.pdf>. Acesso em: 26 mai. 2019.

EYAL, I; SIRER, E. G. Majority is not enough: bitcoin mining is vulnerable. **Communications of the ACM**, vol. 61, no. 7, p. 95-102, 2018. Disponível em < https://dl.acm.org/citation.cfm?id=3212998>. Acesso em: 25 mai. 2019.

FRENCH, D; CHRISTOFF-KURAPOVNA, M. **Quando a moeda morreu na Alemanha,** 2015. Disponível em: <https://www.mises.org.br/Article.aspx?id=2077>. Acesso em: 03 jun. 2019. Acesso em: 19 de mai. 2019.

HILEMAN, G; RAUCHS, M. **Global Cryptocurrency Benchmarking Study**. 2017. Disponível em <https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf>. Acesso em: 22 mai. 2019.

IVASCHENKO, A.I..Using Cryptocurrency in the Activities of Ukrainian Small and Medium Enterprises in order to Improve their Investment Attractiveness. **Problemi Ekonomiki,** n.03, p. 267-273, 2016. Disponível em <http://oaji.net/articles/2016/728-1479730699.pdf>. Acesso em: 10 mai. 2019.

KRAUSE, E. **A Fifth of All Bitcoin Is Missing. These Crypto Hunters Can Help,** 2018**.** Disponível em: <https://www.wsj.com/articles/a-fifth-of-all-bitcoin-is-missing-these-crypto-hunters-can-help-1530798731?mod=rss_Technology>. Acesso em: 03 jun. 2019.

LI, X; CHONG, A. W. The technology and economic determinants of cryptocurrency exchange rates: The case of Bitcoin. **Decision Support Systems**, vol. 95, p. 49-60. 2017. Disponível em <https://www.sciencedirect.com/science/article/pii/S0167923616302111>. Acesso em: 01 jun. 2019.

LOPES, J. do C.; ROSSETTI, J. P. **Economia Monetária.** 9. ed. São Paulo:Atlas, 2005.

LUTHER, W. J; WHITE, L. H. **Can Bitcoin Become a Major Currency?.** George Mason University, Department of Economics, Working Paper No. 14-17, 2013. Disponível em: <https://poseidon01.ssrn.com/delivery.php?ID=545088089111020077027123127126094120039012007068065003094083108117029101126100118093035043107025020012109114030003117103113013033055024073042105002084000117095083089003009036118085118121004087070087114106029000109067064011114118108093103014120026031089&EXT=pdf>. Acesso em: 17 mai. 2019.

NAKAMOTO, S. **Bitcoin:** A Peer-to-Peer Electronic Cash System, 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 24 mai. 2019.

OLIVEIRA, F. M.; TOTTI, M. E. F.; NEY, V. de S. P. BITCOIN: O DINHEIRO COM TECNOLOGIA DE FONTE ABERTA EM REDE PONTO-A-PONTO. **Anais do Encontro Virtual de Documentação em Software Livre e Congresso Internacional de Linguagem e Tecnologia Online**, [S.l.], v. 3, n. 1, jun. 2014. Disponível em: <http://www.periodicos.letras.ufmg.br/index.php/anais_linguagem_tecnologia/article/view/5879>. Acesso em: 28 mai. 2019.

ORRELL, D; CHLUPATÝ, R. **The evolution of money.** Nova York: Columbia University Press, 2016.

PIRES, H. Bitcoin: a moeda do ciberespaço. **GEOUSP Espaço e Tempo (Online)**, v. 21, n. 2, p. 407-424, 19 out. 2017. Disponível em: <http://www.revistas.usp.br/geousp/article/view/134538>. Acesso em: 14 mai. 2019.

RICCI, S; *et al*. Dinâmica das transações do Bitcoin: uma abordagem quantitativa. In: 15º WPERFORMANCE - WORKSHOP EM DESEMPENHO DE SISTEMAS COMPUTACIONAIS E DE COMUNICAÇÃO, 06, 2016, Porto Alegre. **Anais [...]**. Porto Alegre, Pontifícia Universidade Católica do Rio Grande do Sul, 2016. Disponível em <www.lbd.dcc.ufmg.br/bdbcomp/servlet/Trabalho?id=23967>. Acesso em 18 mai. 2019.

SICHEL, R. L; CALIXTO, S. R. Criptomoedas: impactos na economia global. Perspectivas / Cryptocurrency: impacts in the global economy. Perspectives. **Revista de Direito da Cidade**, [S.l.], v. 10, n. 3, p. 1622-1641, ago. 2018. Disponível em: <https://www.e-publicacoes.uerj.br/index.php/rdc/article/view/33096>. Acesso em: 19 mai. 2019.

ULRICH, F. **Bitcoin**: A moeda na era digital. São Paulo: Instituto Ludwig Von Mises Brasil, 2014.

VICENTE, R. J. A criptomoeda como método alternativo para realizar transações financeiras. **Revista Maiêutica**, Indaial, v. 2, n. 01, p. 85 - 94, 2017. Disponível em <https://publicacao.uniasselvi.com.br/index.php/TI_EaD/article/view/1692>. Acesso em: 21 mai. 2019.

YERMACK, D**. Is Bitcoin a Real Currency? An Economic Appraisal.** National Bureau of Economic Research, Working Paper no.19747, 2013. Disponível em < https://www.nber.org/papers/w19747.pdf>. Acesso em: 17 mai. 2019.