UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
INSTITUTO DE ECONOMIA
MONOGRAFIA DE BACHARELADO

CRIPTOMOEDAS - SERIAM ESSAS FORMAS VIÁVEIS DE DINHEIRO?

Pablo Diego de Albuquerque Pereira
Matrícula n°: 110052628

Orientador: Prof. João Felippe Cury Marinho Mathias

SETEMBRO 2019

UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
INSTITUTO DE ECONOMIA
MONOGRAFIA DE BACHARELADO

CRIPTOMOEDAS - SERIAM ESSAS FORMAS VIÁVEIS DE DINHEIRO?

Pablo Diego de Albuquerque Pereira
Matrícula n°: 110052628

Orientador: Prof. João Felippe Cury Marinho Mathias

SETEMBRO 2019

As opiniões expressas neste trabalho são da exclusiva responsabilidade do autor

Dedico este trabalho a Tatiana, mulher essencial e adorável que acreditou e me apoiou imensamente em toda essa jornada.

AGRADECIMENTOS

Agradeço à Deus, minha mãe, que muito investiu na minha educação e meu irmão, que esteve lado a lado grande parte dessa jornada acreditando em mim.

Agradeço ao João Felippe Cury Marinho Mathias, que acreditou e aceitou orientar esse trabalho, dando toda atenção que demandei nesse breve e intenso percurso.

Agradeço aos amigos que me mantiveram crente na conclusão desse curso e não me deixaram fugir desse propósito, especialmente a cada um dos amigos do Sujeira, onde sem dúvida há de habitar o espírito imortal do Instituto de Economia.

Agradeço aos meus sócios, que entenderam minha ausência, apoiaram e acreditaram que eu jogaria duro essa partida.

Agradeço a Anna Lucia Braga Salles: Sem sua atitude eu não estaria escrevendo essas linhas. Muito obrigado pela confiança.

E por último agradeço ao Instituto de Economia, seus professores, alunos e técnicos, pela pluralidade de pensamentos que foram apresentadas, a qualidade de ensino que foi disponibilizada e o desenvolvimento e aprendizado que tive como profissional e pessoa, que sem dúvida levarei pelo resto dessa breve existência.

RESUMO

Essa monografia irá analisar o processo de origem e desenvolvimento da moeda ao longo do tempo. Após isso, abordará a estrutura que sustenta o universo das criptomoedas, em especial o Bitcoin. Com isso, de maneira descritiva, será abordado sobre sua origem, funcionamento e com uma discussão sobre as vantagens e riscos ligados ao sistema. Como Após isso, será seguida de uma análise das características e funções clássicas da moeda em comparação a moeda eletrônica.

ÍNDICE

INTRODUÇÃO

"A boa reputação vale mais que grandes riquezas; desfrutar de boa estima vale mais que prata e ouro".
Provérbios 22:1

As moedas eletrônicas (ou criptomoedas) representam uma inovação que pode ser observada em ampla escala. No que diz respeito aos aspectos que representam uma perspectiva mais superficial, é possível constatar sua considerável e crescente utilização no sistema de pagamentos. Quanto ao que engloba o sistema monetário como um todo, nota-se uma espécie de reformulação dos potenciais agentes, assim como um grande impacto, inclusive, no ambiente jurídico. O fluxo de inovações estimulado por esta concepção digital de valor tem sido tão grande e acelerado, que alguns autores o qualificam como uma "revolução".

> "Você lembra como a internet e o e-mail revolucionaram a comunicação? Antes, para enviar uma mensagem a uma pessoa do outro lado da Terra, era necessário fazer isso pelos correios. Nada mais antiquado. Você dependia de um intermediário para, fisicamente, entregar uma mensagem. Pois é, retornar a essa realidade é inimaginável. O que o e-mail fez com a informação, o Bitcoin fará com o dinheiro. Com o Bitcoin você pode transferir fundos de A para B em qualquer parte do mundo sem jamais precisar confiar em um terceiro para essa simples tarefa." (ULRICH, 2014, p.112)

O objetivo deste trabalho é traçar um panorama geral sobre o surgimento da moeda e seu desenvolvimento, até o surgimento da versão mais primitiva de moeda fiduciária, que deu poder aos bancos e estados de emissão de dinheiro não lastreado. A má execução desse poder ocasionou graves consequências, como a fome e o desabastecimento (MISES, 2008). Por esse motivo, é importante destacar que "não há maneira mais sutil nem mais segura de derrubar a base da sociedade do que perverter a moeda. O processo engrena todas as forças ocultas da lei econômica no lado da destruição e o faz de tal forma que nem um homem dentre um milhão é capaz de diagnosticar" (KEYNES, 2002). Seguido desse ponto, será dada a estruturação e a operação do sistema de moedas virtuais. Também, serão desenvolvidas algumas questões que serão propostas no decorrer do trabalho, tomando como referência a definição clássica da moeda, apresentada nos manuais de economia. Dessa maneira, sucede que para que uma moeda eletrônica seja considerada efetivamente moeda, é preciso que ela atue como reserva de valor, meio de troca e unidade de conta.

Diante do exposto, surgem algumas importantes questões iniciais: Esse grupo de ativos pode atender essas funções? Até que ponto? Caso atenda, isso implicaria na sua utilização como

dinheiro? Quais seriam os pontos que poderíamos citar como possivelmente vantajosos, visto que provavelmente não haverá resguardo legal ou regulatório? É possível que a confiança ("*fiducia*") seja estruturada sem um agente responsável pelo bom funcionamento do sistema? Parte desses dois últimos questionamentos são pontuados pelo próprio criador do Bitcoin, Satoshi Nakamoto:

> "The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts. Their massive overhead costs make micropayments impossible." [1] (NAKAMOTO, 2011)

A desestatização do dinheiro vem sendo discutida como uma possível alternativa para evitar a manipulação da moeda, pois a concorrência entre moedas privadas pode resultar numa espécie de "antipolítica" monetária (HAYEK, 2011). Essa proposta abre espaço para uma discussão que abrange a aplicação das criptomoedas como uma ferramenta para a descentralização do dinheiro. Isso se dá porque algumas delas, como o Bitcoin por exemplo, não demandam o mesmo tipo de confiança em instituições, visto que é descentralizada. Inclusive, a literatura aponta que sua demanda por confiança é exclusivamente técnica, baseada no projeto de governança embutido e no comportamento da rede de usuários que a utiliza. Em vista disso, caso as moedas eletrônicas assumam todas as características e funções básicas de moedas e, além disso, também sejam capazes de desempenhar todos os requisitos técnicos, ainda fica uma pergunta essencial que buscaremos responder no desenvolvimento dos próximos capítulos: *Seriam as criptomoedas formas viáveis de dinheiro?*

Esse questionamento se aproxima da hipótese que sustenta esse trabalho, pois foi levantada a possibilidade de que o Bitcoin esteja próximo a uma moeda-mercadoria, dado sua vulnerabilidade frente ao mercado devido à inexistência de um agente regulador. Na tentativa de responder essa questão, será apresentada no primeiro capítulo uma breve história da origem do dinheiro, discutindo basicamente as razões que impulsionaram os agentes. Também serão

1 Tradução livre: "O problema chave da moeda convencional é toda a confiança que é necessária para fazê-la funcionar. Deve-se confiar que o banco central não prejudique a base monetária corrente, mas a história das moedas fiduciárias expõe graves falhas nessa confiança. Deve-se confiar nos bancos, onde depositamos nosso dinheiro e transferimos eletronicamente, mas eles emprestam-lo em ondas de bolhas de crédito com apenas uma fração da reserva. Temos que confiar com nossa privacidade, confiar que não irão drenar nossas contas. Com suas sobrecargas de custos massivos, fazem micropagamentos impossíveis."

apresentadas as melhorias ocorridas no processo até o surgimento das moedas fiduciárias, assim como serão indicadas as funções que uma moeda deve cumprir. No segundo capítulo será abordada uma perspectiva da origem das moedas eletrônicas, como uma nova forma de moeda, e o blockchain, como uma cadeia aberta de informações registradas e descentralizada, além dos principais conceitos que envolvem ambos e uma discussão do seu funcionamento. A partir daí, surgem outras questões: Por quê o Bitcoin foi criado? O que há de errado com a forma de pagamento tradicional online? Onde estão as tentativas precedentes ao Bitcoin? Como ele solucionou os problemas que foram previamente apresentados em outras tentativas de moeda eletrônica? No terceiro capítulo aprofundaremos a discussão a respeito das criptomoedas, e utilizando o bitcoin[2] (BTC) como referência, serão abordadas cada uma das características desejáveis da moeda (divisibilidade, transferibilidade, facilidade de manuseio e transporte, indestrutibilidade, inalterabilidade e homogeneidade) e as funções que essa moeda deve assumir (unidade de conta, meio de troca e reserva de valor).

2 Será usado BTC e bitcoin em caixa baixa para referir a unidade monetária e Bitcoin em caixa alta para referir ao sistema

CAPÍTULO I - SOBRE A MOEDA

> *"Qualquer pessoa, menos um economista, sabe o que quer dizer 'dinheiro', e até mesmo um economista é capaz de descrevê-lo ao longo de um capítulo ou mais."*
> *A. H. Quigging, a survey of primitive money: the beginnings of currency [uma pesquisa sobre o dinheiro primitivo: o começo da moeda], p. 1.*

I.1 - Desenvolvimento

As sociedades pré monetárias tinham como seu método de negociação a troca direta de bens. Esse processo era resultado da busca de uma "coincidência de desejos", aspecto que evidencia, inicialmente, um problema ligado à necessidade do indivíduo demandante: a procura por uma dada mercadoria ou serviço, ou seja, é necessário encontrar um ofertante que precise de algo que o primeiro faça ou produza. Essa busca poderia ser extremamente desgastante, forçando que núcleos produtivos (como famílias e grupos nômades) fossem extremamente auto-suficientes, e presos a necessidades muito básicas, como segurança e alimentação. Outro problema que surge a partir desse método de negociação, é a indivisibilidade de certos bens, fator que dificulta negociações de porte menor. Portanto, mesmo dado que agentes interessados em realizar uma troca se encontrem, e decidam transacionar em comum acordo, é possível que não consigam pulverizar sua mercadoria sem prejudicar o valor de uso da mesma. Nesse arranjo de trocas diretas, é impossível a existência de uma economia moderna (CARVALHO et al., 2007; ROTHBARD, 2013).

Na medida em que tais grupos nômades começaram a migrar para um modelo mais sedentário e complexo, tal arranjo de trocas diretas acabou sendo sobrecarregado diante do crescimento das populações. Esse arranjo é explicado da seguinte maneira:

> "As trocas diretas somente seriam eficazes em sociedades com economias primitivas, onde os indivíduos e/ou grupos familiares fossem basicamente auto suficientes; isto é, onde a divisão do trabalho praticamente inexistisse: uma sociedade em que cada indivíduo produzisse o que necessita e transacionasse somente quando houvesse um excedente, eventual, não planejado da sua produção. Nessa sociedade, um indivíduo não necessita realizar transações para se proteger do frio, para comer, para acender o fogo. Quando (e se) a transação do seu excedente produtivo ocorrer, ele pode obter uma satisfação extra, além das suas necessidades básicas. O agente não depende da realização de uma transação para atender as suas necessidades. A produção individual ou familiar garante a satisfação de necessidades. As transações, quando realizadas, gerariam satisfação extra. Assim, no regime de trocas diretas, uma transação é, ao

> mesmo tempo, venda de uma mercadoria e compra de uma outra." (CARVALHO et al., 2007, p.2)

I.1.1 – Origem

O surgimento das formas mais primitivas de dinheiro se dá, através de trocas indiretas, na intenção de aumentar a eficiência das trocas numa dada economia. De maneira bem diferente da que ocorre nos dias de hoje, o dinheiro não surgia como fruto de homens engajados com a melhoria de atividades econômicas ou com legisladores, e sim, a partir de indivíduos em pequenas economias locais que buscavam melhorias em suas atividades comerciais. Eles notaram que, ao trocarem mercadorias menos comercializadas por outras com maior intensidade, ganhavam potenciais de otimização na busca dos seus próprios interesses econômicos. Dessa forma, pode-se supor que a origem do dinheiro, na sua forma mais primitiva, é descentralizada. Sendo assim, trata-se de um "produto natural da economia". Esse espaço, ao longo do tempo, foi ocupado por diversas mercadorias, tais como: gado, sal, cevada, arroz, ouro e outros. Todas as mercadorias, fundamentalmente, possuíam valor de uso e eram racionalizadas em medidas de peso ou volume. (MENGER, 1985)

> "A mercadoria transformada em dinheiro (na ausência de obstáculos impostos pelas características da respectiva mercadoria) é, ao mesmo tempo, aquela que melhor se presta para a avaliação dos objetivos práticos das pessoas economicamente ativas e, ao mesmo tempo, para a comercialização dos estoques de mercadorias destinadas à permuta; do exposto conclui-se também que o dinheiro-metal - precisamente o que os pesquisadores de Economia Política têm em mente quando falam de dinheiro em geral - atende de fato e em alto grau a essas finalidades. Todavia, parece-nos igualmente certo que ao dinheiro como ta! não se pode atribuir a função de "parâmetro de valor" e de "conservador de valores", pois essas características são de natureza acidental, não estando contidas intrinsecamente no próprio conceito de dinheiro." (MENGER, 1985, p. 388)

Então, na sua forma mais primitiva, o nascimento do dinheiro ocorre maneira bem espontânea, como unidades de uma dada mercadoria que era melhor aceita. Sendo assim, se tratava de uma forma mais eficiente de se movimentar financeiramente em economias de escambos. Dessa forma, pode-se concluir que o dinheiro é uma mercadoria que permite a avaliação de todas as outras demais mercadorias dentro de um ambiente econômico (MENGER, 1985).

Inicialmente, essa demanda por uma moeda poderia ser lida como uma busca pelo aumento da liberdade das escolhas dos indivíduos. Tal ótica é explicada da seguinte maneira:

> “Se lutamos pelo dinheiro, é porque ele nos permite escolher da forma mais ampla como melhor desfrutar os resultados de nossos esforços. Visto que, na sociedade moderna, as restrições ainda impostas por nossa relativa pobreza se refletem na limitação da nossa renda pecuniária, muitos passaram a odiar o dinheiro como símbolo dessas restrições. Mas isso significa confundir com a sua causa o meio pelo qual uma força se faz sentir. Seria muito mais certo dizer que o dinheiro é um dos maiores instrumentos de liberdade já inventados pelo homem. É o dinheiro que, na sociedade atual, oferece ao homem pobre uma gama de escolhas extraordinariamente vasta, bem maior do que aquela que há poucas gerações se oferecia aos ricos. Compreenderemos melhor a importância desse serviço prestado pelo dinheiro se considerarmos o que de fato aconteceria se, como propõem muitos socialistas, o “incentivo pecuniário” fosse em grande parte substituído por “incentivos não-econômicos”. Se, em vez de serem oferecidas em dinheiro, todas as recompensas o fossem sob a forma de distinções públicas ou privilégios, posições de poder, melhores condições de moradia ou alimentação, oportunidade de viajar ou educar-se, isso significaria apenas que o beneficiário já não teria liberdade de escolha e que o dispensador das recompensas determinaria não somente o seu valor mas também a forma específica em que elas seriam desfrutadas." (HAYEK, 2010, P.102)

Da mesma forma, Ferguson (2009) diz que o dinheiro é um meio de troca que suprime as ineficiências do escambo, facilitando a valoração e o cálculo de preços, permitindo que transações econômicas sejam conduzidas durante longos períodos e também a partir de grandes distâncias geográficas. Ele também nota que a necessidade de ser durável, fungível, portátil e confiável é a melhor maneira de assumir essas funções, dadas as circunstâncias. Dito isso, metais preciosos se tornaram uma ótima mercadoria para ocupar essa lacuna, pois assumem essas características. No entanto, o ponto a ser problemático nessa equação seria a confiabilidade da qualidade do metal envolvido na troca. O autor também cita outras formas de dinheiro locais, que ocorreram sem a necessidade de que a mercadoria fosse rara ou tivesse valor de uso relevante, como conchas, pedras e folhas. Nesses casos, o que diferenciava essa forma da citada anteriormente, era uma relação de confiança que ancorava aquela negociação. Essa confiança era possível de ser reproduzida em diversas transações dentro de uma mesma pequena economia local, mas dificultava muito a negociação caso aquele povoado procurasse realizar alguma transação com outros povos e cidades. Isso se daria tendo em vista que algo que tenha valor simbólico para um povoado, não necessariamente teria para outro.

Ferguson (2009) mostra que, mesmo que um bem tenha sido tomado como uma moeda-mercadoria localmente, na tentativa de expansão das redes comerciais, nada garantiria que as negociações continuariam sendo aceitas com aquela determinada unidade - seja pela ausência de valor simbólico naquela região ou por não possuir valor de uso percebido. Fato que acabaria gerando um empecilho nessas expansões, dado que, na medida em que fossem crescendo, maior seria a demanda por confiança ou por garantia, caso as negociações com tal moeda-mercadoria continuem sendo aceitas. Esse problema se agrava diante da possibilidade de, em alguns casos,

tal mercadoria, mesmo possuindo grande aceitação, pudesse literalmente morrer no caminho, como escravos ou gado.

Smith (1996) indica que, no processo de escolha da moeda-mercadoria nas aplicações regionais, ao que tudo indica, evidenciou-se que tal produto não era necessariamente único. No entanto, ainda era possível que tivesse algumas predileções ao longo do tempo. Assim, ele explica que:

> "Provavelmente, muitas foram as mercadorias sucessivas a serem cogitadas e também utilizadas para esse fim. Nas épocas de sociedade primitiva, afirma-se que o instrumento generalizado para trocas comerciais foi o gado. E embora se trate de uma mercadoria que apresenta muitos inconvenientes, constatamos que, entre os antigos, com freqüência os bens eram avaliados com base no número de cabeças de gado cedidas para comprá-los. A couraça de Diomedes, afirma Homero, custou somente 9 bois, ao passo que a de Glauco custou 100 bois. Na Abissínia, afirma-se que o instrumento comum para comércio e trocas era o sal; em algumas regiões da costa da Índia, o instrumento era um determinado tipo de conchas; na Terra Nova era o bacalhau seco; na Virgínia, o fumo; em algumas das nossas colônias do oeste da Índia, o açúcar; em alguns outros países, peles ou couros preparados; ainda hoje — segundo fui informado — existe na Escócia uma aldeia em que não é raro um trabalhador levar pregos em vez de dinheiro, quando vai ao padeiro ou à cervejaria; Entretanto, ao que parece, em todos os países as pessoas acabaram sendo levadas por motivos irresistíveis a atribuir essa função de instrumento de troca preferivelmente aos metais, acima de qualquer outra mercadoria..". (SMITH, 1996, p.82)

A durabilidade dos metais acaba sendo um fator primordial na sua escolha. Essa vantagem proporciona ao material uma possibilidade de, sendo mercadoria, conservar seu valor ao longo de um tempo mais longo frente a outras mercadorias que ocupem essa mesma posição. A divisibilidade, que é possível nesse tipo de bem, também é um atrativo, já que mesmo que seja partido em frações pequenas, não perde suas características, e, além disso, ao se fragmentar, esse bem pode facilmente se recuperar novamente com um processo de fusão, que é uma característica única, apresentada apenas nos metais preciosos. Sua facilidade de manuseio e transporte é razoável, mas fica questionável na medida em que crescem os volumes de negociação e os riscos envolvidos no transporte de grandes quantidades de metais em uma caravana. Tais pontos desenham algumas das quais seriam as características físicas desejáveis de uma moeda. Essas mercadorias acabaram sendo um dos primeiros métodos de pagamentos aceitos em várias regiões do mundo. Seu uso e aplicações serão retratados na próxima sessão. (SMITH, 1996; CARVALHO et al., 2007)

I.1.2 - Da cunhagem até a moeda fiduciária

A verificação da autenticidade dos metais precioso nas negociações foi o primeiro ponto a ser eliminado, dado que era mais um custo acrescentado na operação, pois seria necessária a

atuação de um especialista para garantir a pureza do metal. A solução encontrada foi a marcação das barras de metal por uma autoridade oficial ou por um pessoa que tivesse a confiança nessa dada avaliação. Essa certificação não garantiria o peso da barra, já que ocorria um problema de confiança na balança dos comerciantes, mas atestaria a qualidade para quem estivesse recebendo. O problema com a pesagem seria resolvido na medida que essa necessidade de atestar o peso também começou a se mostrar mais latente, fato que ocorreu em alguns casos simultaneamente a solução da garantia de pureza. Para isso, a melhor forma seria dividir o metal em peças pequenas, o que permitiria a identificação deles como autênticos, assim como seria facilmente notada qualquer fraude aplicada nesse mesmo material. Desse arranjo, surge o processo de cunhagem do metal, que deu origem as moedas, que tinham proporções e purezas que as protegiam de fraudes. Esse movimento proporcionou uma imensa praticidade nas negociações (MENGER, 1985).

Rothbard (2013) retratou que essa padronização através da cunhagem também foi a causa de uma transformadora revolução no comércio.

> "O surgimento do dinheiro foi uma grande dádiva para a humanidade. Sem o dinheiro – sem um meio geral de troca – seria impossível haver uma genuína especialização, uma genuína divisão do trabalho. Consequentemente, seria impossível a economia avançar para além de seu nível mais simples e primitivo. Com o dinheiro, todos os problemas de indivisibilidade e da "coincidência de desejos", que atormentavam a sociedade baseada no escambo, são eliminados. Agora, João pode contratar trabalhadores e pagá-los em... dinheiro. O senhor Silva pode vender seu arado por unidades de... dinheiro." (ROTHBARD, 2013, p.17)

O processo de cunhagem demandava que a autoridade fosse reconhecida e, teoricamente, tivesse total interesse na não corrupção do sistema. Sobre esse aspecto, Menger (1985) relata o seguinte:

> "Não há como negar que a melhor garantia em relação ao peso e à composição das moedas é aquela que o Estado pode oferecer, porque essa autoridade é de todos conhecida e por todos reconhecida, e, ao mesmo tempo, o Estado tem condições de coibir e punir crimes no tocante a essa matéria. Eis por que geralmente os governos têm considerado seu dever cunhar as moedas necessárias para o comércio; em muitos casos, porém, abusaram tanto desse poder, que os indivíduos quase chegaram a esquecer que uma moeda não passa de uma peça de metal nobre com peso e composição específicos, elementos garantidos pela retidão do cunhador, chegando-se até a duvidar de que a moeda seja, em última análise, uma mercadoria, e ao ponto de, ao final, se qualificar a moeda como ato puramente imaginário e baseado apenas na conveniência humana. Assim, o fato de os governos dispensarem à moeda esse tratamento - como se ela fosse efetivamente apenas um produto da conveniência humana em geral e do arbítrio legislativo do Estado -, esse fato, dizíamos, contribuiu não pouco para induzir aos erros vigentes acerca da natureza do dinheiro." (MENGER, 1985, p.390)

Registros do século VI A.C. mostram a prerrogativa do governo sobre a cunhagem de moedas de metais preciosos. A partir desse momento, para que essa prerrogativa tivesse valor,

era fundamental a aceitação irrestrita dessa moeda. Essa necessidade foi o aspecto que deu origem ao curso forçado da moeda, por parte do Estado. Esse processo de cunhagem, assim como a mineração e os impostos alfandegários, vieram a se tornar regalias, ou seja, direitos e privilégios da realeza (HAYEK, 2011).

Tais moedas vieram a se tornar o principal meio de pagamento em várias regiões do mundo, onde teriam diferentes percepções de valor, mas ainda assim aceitas de maneira semelhante. A única forma, até então, de se atestar propriedade de uma quantidade de metal precioso era portar ele, assim como a única garantia de pagamento era a transferência física do mesmo, isto é, quando um comprador entregava uma quantidade de moeda para o vendedor. Dado isso, a constante necessidade de transportar quantidades relevantes de moedas em caravanas comerciais se tornou um problema. Tanto pelo custo do transporte, quanto pelos custos referentes aos roubos e a proteção necessária em longas jornadas. Para solucionar esse fato, foram criados locais de armazenamento que custodiavam esses metais, e entregavam em troca, aos seus portadores, certificados que serviam como moedas representativas, que muito se assemelhavam à letras de câmbio (SMITH, 1996).

Inicialmente, toda letra de câmbio era 100% lastreada em metais preciosos, porém, com a popularização e o enraizamento da confiança na probidade e prudência de um dado banco nessas emissões, era natural que tais papéis tivessem o mesmo valor que moedas. Nesse ponto, abriu-se espaço para criação de moedas bancárias, onde os bancos poderiam criar moeda através da emissão de notas com fins de empréstimos, assumindo, a partir desse momento, que os empréstimos não seriam 100% lastreados. Esse é o início do viria a ser a moeda fiduciária (WRAY, 2002).

I.2 - Definição e Funções da Moeda

> *"E disse: Que me quereis dar, e eu vo-lo entregarei? E eles lhe pesaram trinta moedas de prata"*
> *Mateus 26:15*

É possível indicar que a moeda é um objeto que atua na direção de facilitar as trocas no contexto da divisão social do trabalho - onde indivíduos optam por se especializar na produção de uma dada mercadoria ou serviço e usam outra mercadoria como referência de valor na hora da troca, em vez de buscar alguém que queira especificamente a sua produção como no mercado de escambo. Essa modernização nas trocas acaba sendo fundamental em uma economia capitalista, já que os agentes se tornam extremamente interdependentes e, sem ela, ocorreria grande lentidão e desgaste na conclusão de cada negociação, inviabilizando o dinamismo moderno da economia (CARVALHO et al., 2007).

Agentes demandam a moeda como remuneração, o que possibilita maior liberdade nas suas decisões de compra. Para que a moeda cumpra esse uso, é preciso que ela assuma um conjunto de funções que, baseado em Carvalho et al. (2007), podem ser os seguintes:

1) Meio de troca: Nessa função, se supõe que vários agentes dentro daquele ambiente econômico aceitam e usam a moeda como uma forma de pagamento por um serviço. Sem essa função, se perde a liberdade nas decisões de compra e a moeda se descaracteriza, perdendo sua característica essencial, já que sem ela, a economia de escambo não teria sido superada.
2) Unidade de conta: Essa função pretende que se tenha como mensurar uma produção ou o valor como um todo em uma economia em unidades do ativo. Com essa função, se pretende ser possível indexar todos as mercadorias disponíveis em valores relativos ao ativo que se propõe ser uma moeda, escapando do problema das economias de escambo, onde cada mercadoria teria seu valor expresso em quantidades de outra mercadoria de interesse. Uma das importâncias da existência desse instrumento é para que permita-se a coordenação das decisões de produção dos agentes dentro daquele ambiente econômico
3) Reserva de valor: Tal função dispõe da crença de que se possa reservar parte do poder de compra em um período, para ser consumido em um período seguinte (poupar), sem um custo de carregamento. Dessa forma, seria possível operar como um estoque de riqueza. A reserva de valor basicamente opera como uma versão estendida da unidade de conta, mas para longo prazo.

Os princípios que acompanham o surgimento da moeda - desde a sua construção inicial através do uso de moedas-mercadorias, seguido de um desenvolvimento que resultou em uma padronização na cunhagem, até a adoção das letras de câmbio - permitem depreender que, tais funções amadureceram na medida em que se potencializou a necessidade de ampliação da aceitação da moeda de uma maneira mais simples, dinâmica e segura. Esse ponto, que pode ser observado ao longo do tempo, ainda é passível de ser percebido até mesmo nos dias de hoje - a partir da desmaterialização da moeda, atributo que trouxe novos formatos e outras possibilidades.

Por esse motivo, esse ciclo de desenvolvimento da economia monetária, assim como as funções básicas de uma moeda, foram apreendidos como a base de construção deste trabalho. Portanto, para que os próximos andares sejam construídos, se faz necessário um melhor entendimento das características dispostas na rede Bitcoin - elemento central desta monografia

- tal qual a sua construção interna e os aspectos que poderão ancorar a confiança nessa nova moeda.

CAPÍTULO II - SOBRE CRIPTOMOEDAS E BLOCKCHAIN

> *"Os males desesperados são aliviados com remédio desesperados ou, então, não têm alívio."*
> *William Shakespeare (Hamlet, ato IV, cena III)*

As criptomoedas (ou moedas eletrônicas) podem ser definidas como ativos virtuais que, inicialmente, se propuseram a cumprir basicamente o papel da moeda - como o dólar, o real ou o euro, mas, principalmente, no meio eletrônico. No princípio, as principais diferenças das criptomoedas em relação à moeda convencionais, se deram a partir de uma descentralização tanto na emissão, quanto na administração do sistema como um todo (ULRICH, 2014). Essas diferenças vêm se expandindo continuamente à medida que ocorrem, tanto as bifurcações do desenvolvimento, quanto os lançamento de novos ativos, que apresentam novas características e usabilidades, oferecendo um escopo enorme e em constante expansão para esse trabalho. Em razão disso, o trabalho se aterá, na maior parte do tempo, ao Bitcoin, que corresponde, em grande parte do tempo, à base teórica para a maior parte dos sistemas posteriores. No que diz respeito, especificamente ao Bitcoin, pode-se tomar o seguinte conceito:

> "Bitcoin é uma moeda, um meio de troca, embora ainda pouco líquida quando comparada às demais moedas existentes no mundo. Em algumas regiões de opressão monetária[3], é cada vez mais usada como reserva de valor. Uma característica peculiar é a sua oferta limitada em 21 milhões de unidades, a qual crescerá paulatinamente a uma taxa decrescente até alcançar esse limite máximo. Embora intangível, o protocolo do Bitcoin garante, assim, uma escassez autêntica. Como unidade de conta, pode-se afirmar que ainda não é empregada como tal, devido, especialmente, à sua volatilidade recente. Ademais, Bitcoin é também um sistema de pagamentos, o que significa que, pela primeira vez na história da humanidade, a unidade monetária está aliada ao sistema bancário e de pagamento e é parte intrínseca dele." (ULRICH, 2014 p.113).

A jornada se inicia a partir de uma série de questionamentos - feitos por um grupo de criptógrafos a partir da década de 80 - aos meios tradicionais de pagamento. Eles pontuavam que esses métodos exigiam o envolvimento de intermediários, onde alguém se responsabilizava por administrar os débitos e créditos das contas, assim como os requerimentos de pagamentos, inclusive, cobrando altas taxas. Esse movimento estava centrado em uma série de limitações

[3] O Autor trata opressão monetária como zonas que sofrem grande impacto negativo de fenômenos monetários, como inflação, deflação, manipulação cambial, etc. Ver Mises (2008)

técnicas que obrigavam, justamente por esse motivo, a existência desses intermediários (CHAUM, 1982).

II.1 - Sobre a origem das moedas eletrônicas

"As liberdades não se concedem, conquistam-se."
Piotr Kropotkin

O sistema de dinheiro eletrônico evidencia algumas dificuldades no âmbito da sua implementação: Como definir, eletronicamente, moedas? Como seria sua distribuição? Como provar sua posse? Como prevenir o gasto duplo? Como fazer as transações privadas? Como garantir a segurança do sistema? De acordo com Nakamoto (2018), alguns profissionais tentaram encontrar respostas para essas perguntas, e a partir de então, o surgimento do Bitcoin se tornou possível.

II.1.1 - eCash

Um dos mais antigos precursores desse universo é David Chaum, matemático e criptógrafo americano, que a apartir 1982 lançou uma série de papers e iniciativas a respeito do tema (GREENBERG, 2012). Em 1990 fundou o DigiCash, e acabou lançando em 1994 o eCash, a primeira tentativa de moeda eletrônica e, também, a espinha dorsal do que viria se tornar o Bitcoin.

> "David Chaum preceded me by almost twenty years, but with his paper Untraceable Electronic Cash he explored the possibility of anonymous transactions using a number of cryptographic protocols. Its inherent flaw however, was that it was centralized. And like all things, people can lose trust in something that is controlled by one authority." [4] (NAKAMOTO, 2018, p.1)

Sua principal contribuição para o Bitcoin e todos os sistemas subsequentes foi a introdução da assinatura digital, que protegia por meio de criptografia os dados da mensagem, conduzindo ao anonimato (CHAUM, 1983). Apesar de essencial para o desenvolvimento do Bitcoin, acabou apresentando fragilidades que a inviabilizaram em larga escala, pois era muito

[4] Tradução livre: "David Chaum me precedeu quase 20 anos, mas com seu trabalho "Untraceable Electronic Cash" explorou a possibilidade de fazer transações anônimas usando alguns protocolos criptográficos. Sua falha inerente, no entanto, era a centralização em algo que era controlado por uma autoridade"

centralizada e apresentava uma considerável fragilidade ao maior adversário do universo das moedas digitais: o gasto duplo.

II.1.2 - HashCash

Um outro expoente nessa jornada é Adam Back, um criptógrafo britânico, que em 1997 propôs um sistema de hash criptografado como forma de proteger abusos sistemáticos, como o spam de email e o ataque DoS - chamado de HashCash. Basicamente, ele introduz um sistema de prova de trabalho (Proof of Work - POW), com o objetivo de verificar se um computador ou alguém trabalhou em uma determinada atividade. É importante ressaltar que tal sistema nunca teve a pretensão de ser utilizado como moeda. No entanto, o próprio Adam Back (2002), ao formalizar o conceito por meio de um paper, não deixou de esclarecer que a aplicação desse conceito foi muito além do que ele imaginava:

> "Hashcash was originally proposed as a mechanism to throttle systematic abuse of un-metered internet resources such as email, and anonymous remailers in May 1997. Five years on, this paper captures in one place the various applications, improvements suggested and related subsequent publications, and describes initial experience from experiments using hashcash." 5 (BACK, 2002, p.1)

II.1.3 - B-money

Nesse universo do dinheiro eletrônico, também é de extrema relevância citar Wei Dai, um engenheiro de computação chinês, que em 1998 introduziu o b-money, um sistema de pagamento via "contratos", que estabeleceu uma forma de definir eletronicamente a moeda. Esse programa foi baseado na proposta Hashcash do Adam Back.

> "I am fascinated by Tim May's crypto-anarchy. Unlike the communities traditionally associated with the word "anarchy", in a crypto-anarchy the government is not temporarily destroyed but permanently forbidden and permanently unnecessary. It's a community where the threat of violence is impotent because violence is impossible, and violence is impossible because its participants cannot be linked to their true names or physical locations (...); Until now it's not clear, even theoretically, how such a community could operate. A community is defined by the cooperation of its participants, and efficient cooperation requires a medium of exchange (money) and a way to enforce contracts. Traditionally these services have been provided by the government or government sponsored institutions and only to legal entities. In this article I describe a protocol by which these services can be provided to and by

[5] Tradução livre: "Hashcash foi originalmente proposto como um mecanismo para dificultar o abuso sistemático de recursos não medidos da internet, como e-mail e remailer anônimo em maio de 1997. Cinco anos depois, este artigo captura em um único local as várias aplicações, melhorias sugeridas e publicações subsequentes relacionadas, e descreve a experiência inicial dos usos experimentais do Hashcash."

> untraceable entities(...);The protocol proposed in this article allows untraceable pseudonymous entities to cooperate with each other more efficiently, by providing them with a medium of exchange and a method of enforcing contracts. The protocol can probably be made more efficient and secure, but I hope this is a step toward making crypto-anarchy a practical as well as theoretical possibility." 6 (DAI, 1998)

A contribuição do trabalho desenvolvido pelo engenheiro foi considerável e apresentou, dentre outros aspectos, um amplo grau de completude, pois continha um elaborado sistema de prova de trabalho para a geração de moeda, uma transmissão das transações realizadas, assim como uma assinatura digital que utilizava chave pública de criptografia. Embora essa estrutura tivesse uma falha fatal de gasto duplo - o que a inviabilizou como um sistema de dinheiro -, ela pôde servir de incentivo para o Bitcoin, sendo considerada a inspiração crucial de Satoshi. Contudo, vale salientar que esse sistema dificilmente existiria sem seus predecessores (NAKAMOTO, 2018).

II.1.4 - RPOW

Harrold Finney foi um engenheiro americano, citado em diversas ocasiões por Nakamoto como o primeiro "*beliver*". Além disso, ele trabalhou diretamente no próprio desenvolvimento do Bitcoin, sendo, inclusive, participante das primeiras transações executadas e, até mesmo, apresentou outros incrementos fundamentais para a existência da moeda eletrônica em questão. Sua proximidade com Nakamoto foi amplamente divulgada, fato que resultou na suposição de que Dorian Satoshi Nakamoto seria o autor por trás do famoso pseudônimo "Satoshi Nakamoto", pois ambos moraram na mesma cidade por 10 anos (GREENBERG, 2012).

> "People may forget about this fact now but for the first year, it really was mostly myself who was the sole and active participant in the network. I was both maintaining it, using

---

6 Tradução por ULRICH 2014, p.42: "Eu estou fascinado com a cripto-anarchia do Tim May [membro fundador da lista de discussão Cypherpunk].Ao contrário das comunidades tradicionalmente associadas à palavra 'anarquia', em uma cripto-anarquia o governo não é temporariamente destruído, mas permanentemente proibido e permanentemente desnecessário. É uma comunidade em que a ameaça de violência é impotente porque é impossível, e a violência é impossível porque os participantes não podem ser vinculados aos seus nomes verdadeiros ou às localidades físicas (...); Até agora não está claro, até mesmo teoricamente, como tal comunidade poderia operar. Uma comunidade é definida pela cooperação de seus participantes e cooperação eficiente requer um meio de troca (dinheiro) e uma forma de fazer cumprir contratos. Tradicionalmente esses serviços têm sido providos pelo governo ou por instituições patrocinadas pelo governo e somente a entidades jurídicas. Neste artigo eu descrevo um protocolo pelo qual esses serviços podem ser providos para e por entidades não rastreáveis(…);O protocolo proposto neste artigo permite que entidades pseudônimas não rastreáveis cooperem umas com as outras mais eficientemente, por meio da provisão de um meio de troca e um método de fazer cumprir contratos. Provavelmente o protocolo pode ser aprimorado, mas espero que isso seja um passo à frente do sentido de tornar a cripto-anarquia uma possibilidade prática e teórica

> it, making changes to the code, fixing bugs, and promoting its use. Most people in the beginning were in fact just installing bitcoin once and never using it again, circumventing its intended use. The only person that really chugged away and stayed with it that first year, was Hal Finney" [7] (NAKAMOTO, 2018, p.4)

Hal, abreviação muito utilizada por Nakamoto sobre Harrold Finney, desenvolve em 2004 o mecanismo de prova de trabalho reutilizável (NAKAMOTO, 2018, p.18), onde *tokens* (ou fichas) - que seriam chamados de RPOW - Reusable Proof of Work - eram criados ao se provar trabalho e esses poderiam ser transferidos pela internet - assim como moedas sendo transferidas de carteiras (Finney, 2004). A estrutura de verificação era baseada no uso de servidores remotos, resolvendo assim o problema em relação ao gasto duplo, embora, teoricamente, abrisse uma brecha para vulnerabilidades. Então, apesar de solucionar uma adversidade relevante, definindo a moeda, o sistema não apresentou um processo claro de controle de inflação, o que inviabilizou seu uso em larga escala.

II.1.5 - Bit Gold

Nick Szabo, jurista e criptógrafo americano, talvez tenha sido aquele que chegou mais próximo nessa corrida pela criação da moeda digital. Szabo escreveu diversos papers, de 1998 até 2005, delineando o que seria o bitgold - muito similar ao que seria o Bitcoin - utilizando o sistema de prova de trabalho para gerar token, agregado a um livro razão global de operações para a prevenção de fraudes na cadeia, utilizando assinaturas digitais (SZABO, 2005). O uso de tal livro razão (*"ledger"*) é a grande contribuição de Szabo para o que estaria por vir. Apesar da completude da proposta, Szabo enfrentou um grande problema, pois não encontrou uma solução prática de implementação e acabou não tendo êxito.

> "Precious metals and collectibles have an unforgeable scarcity due to the costliness of their creation. This once provided money the value of which was largely independent of any trusted third party. Precious metals have problems, however. It's too costly to assay metals repeatedly for common transactions(...);Thus, it would be very nice if there were a protocol whereby unforgeably costly bits could be created online with minimal dependence on trusted third parties, and then securely stored, transferred, and assayed with similar minimal trust. Bit gold." [8] (Szabo, 2005)

---

[7] Tradução livre: "As pessoas podem esquecer esse fato agora, mas no primeiro ano, fui eu quem foi o único e ativo participante da rede. Eu estava fazendo manutenção, usando, alterando o código, corrigindo bugs e promovendo o uso. A maioria das pessoas no começo estava apenas instalando bitcoin e nunca mais o usando, evitando o uso pretendido. A única pessoa que realmente se divertiu e ficou naquele primeiro ano, foi Hal[Harrold] Finney"

8 Tradução livre: "Metais preciosos e itens colecionáveis tem uma escassez inevitável devido aos seus custos de criação. Isso acabou provendo um valor de dinheiro que acaba sendo largamente independente da confiança de terceiros. Metais preciosos têm problemas, no entanto. É caro analisar metais repetidamente para

II.2 - Bitcoin

"Ora, havendo Deus completado no dia sétimo a obra que tinha feito, descansou nesse dia de toda a obra que fizera".
Gênesis 2:2

II.2.1 - Definição

Em 2008, Satoshi Nakamoto, um pseudônimo usado em fóruns de cypherpunks e listas de email de criptografia, ao unir os conceitos explorados por todos os seus predecessores - expostos anteriormente neste trabalho - lança um paper em uma lista de email. Neste paper, ele desenhou um sistema que enquadrava todas as respostas para os problemas apresentados no capítulo anterior: uma clara definição de moedas eletrônicas, com um modelo simples de distribuição e prova de posse, mecanismos sólidos de prevenção ao gasto duplo, ampla segurança devido ao alto grau de descentralização. Além disso, o sistema não apresentou nenhum mecanismo que possibilitasse a quebra de privacidade, superando as principais barreiras notadas no decorrer do desenvolvimento da tecnologia (NAKAMOTO, 2008).

O lançamento desse sistema aconteceu no dia 3 de janeiro de 2009. O bloco 0 - ou gênesis - começou a ser minerado no dia 3 de janeiro e o bloco 1 dia 9 de janeiro. O dia 3 é considerado, de fato, a data de criação do sistema, porém, foi somente a partir da conclusão do bloco 1 que vieram os primeiros bitcoins utilizáveis (NAKAMOTO, 2009).

É curioso que o prazo de 6 dias - prazo da criação do primeiro bloco - tenha gerado diversas teorias, e que, devido à identidade desconhecida do criador, o surgimento de teorias a seu respeito tenham se tornado praticamente um padrão. No caso das teorias que envolvem a data da criação, foram feitas, inclusive, alusões da gênesis bíblica à gênesis do Bitcoin[9]. A identidade da pessoa ou grupo que está por trás do pseudônimo Satoshi Nakamoto nunca foi revelada[10]. Desde 2010, ao que tudo indica, Satoshi se ausentou do desenvolvimento do sistema - suas últimas interações foram em 2014[11] e, em 2018 lançou um pequeno livro[12].

---

transações comuns(…); Assim, seria muito bom se tivesse um protocolo em que bits inesgotáveis pudessem ser criados online com dependência mínima de terceiros confiáveis e assim possam ser seguramente armazenados, analisado com confiança mínima. Bit gold"

9 Ver https://bitcointalk.org/index.php?topic=172009.0; https://www.blockchain.com/btc/blocks/1231000000001 e https://www.blockchain.com/btc/blocks/1231518400001

10 Ver https://www.coindesk.com/information/who-is-satoshi-nakamoto e https://nakamotostudies.org/forums/

11 Ver https://nakamotostudies.org/forums/

12 Ver https://www.wired.com/story/did-satoshi-nakamoto-write-this-book-excerpt-a-wired-investigation/

Aqui, surge uma possível resposta da pergunta que foi feita no início do capítulo: Porque o Bitcoin foi criado? Muitos aspectos da comunicação deixada por Nakamoto em seu tempo oficial de atividade, permitem a observação de um viés anárquico no seu posicionamento - tanto no artigo que explica a estrutura do Bitcoin em 2008 e no seu livro de 2018, quanto na sua participação na comunidade cypherpunk de 2008 até 2014. Além disso, um ponto sutil, que deixará isso transcrito enquanto o sistema funcionar, é a notação que ele deixou gravada no bloco gênesis, que contém o seguinte trecho: “The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.”. Essa citação faz referência à uma matéria publicada no mesmo dia da transação, sobre os resgates feitos pelo banco central europeu aos bancos ingleses que estavam em risco por conta da crise de 2008 que ainda se desenrolava. Por esse motivo, “a alusão à manchete do jornal britânico The Times daquele dia não é acidental. É, na verdade, um claro indicativo da visão crítica de Satoshi sobre o sistema bancário e a desordem financeira reinante” (ULRICH, 2014, p.34).

Sendo assim, o Bitcoin é a primeira e, até o momento, a maior moeda digital em funcionamento. Nakamoto (2008) a define como “uma versão puramente ponto-a-ponto de dinheiro eletrônico que pode permitir o envio de pagamentos online diretamente de uma parte a outra sem ser através de uma instituição financeira". Seria uma tentativa de proporcionar uma forma de pagamentos online e dinâmica, muitas vezes tão rápida quanto enviar um email - sem intermediários centralizadores - e com taxas muito baixas quando comparadas às opções que o mercado tradicional oferece. Todos esses aspectos, permitem que transações milionárias internacionais sejam feitas com extrema praticidade e velocidade. De acordo com Ulrich (2014), o Bitcoin:

> “...é como um grande livro-razão, único e compartilhado por todos os usuários simultaneamente. Nele, todas as transações são registradas, sendo verificadas e validadas por usuários especializados, de modo a evitar o gasto duplo e que usuários gastem saldos que não possuem ou de terceiros. Esse registro público universal e único não pode ser forjado. Lá estão devidamente protocoladas todas as transações já realizadas na história do Bitcoin, bem como os saldos atualizados de cada usuário. O livro-razão é, assim, um registro fidedigno, estando sempre atualizado e conciliado. Por sinal, o nome dado a esse livro-razão é blockchain.” (ULRICH, 2014, p.112)

II.2.2 - Blockchain

O Blockchain é o ponto de disrupção desse sistema, ou seja, a nova tecnologia. Da mesma forma que pendrives, folhas de papel ou discos rígidos, o blockchain nada mais é que uma forma de armazenamento, semelhante a um grande livro razão. Tal livro serve como um registro público de transações, que está disposto em uma rede de computadores, totalmente descentralizada e encriptada. Ele contém o histórico completo, com todas as movimentações já

feitas dentro do sistema e, por consequência, todos os saldos atualizados de cada um dos integrantes. Essa estrutura foi fundamental para a viabilidade técnica do Bitcoin e, também para estruturar, de maneira sólida, com mecanismos redundantes de proteção, um sistema de prevenção ao gasto duplo e demais fraudes (ULRICH, 2014).

Já que a finalidade da criação do Bitcoin é realizar transações, o blockchain acaba sendo o grande meio por onde se registra e garante o funcionamento dessas transações - é a espinha dorsal que, tanto explica, quando sustenta o sistema. Essa proposta vai de encontro com basicamente todas as tentativas prévias de criar uma moeda eletrônica, já que pela primeira vez não haveria uma autoridade central envolvida, registrando e aprovando todas as transações executadas (NAKAMOTO, 2008). Nele pode-se notar algumas características fundamentais: descentralização, pseudonimato, irreversibilidade, irrestritibilidade técnica e transparência.

II.2.3 - Características Fundamentais

A descentralização garante que nenhuma entidade única controle a rede e possa alterar transações. Essa característica aumenta a segurança e garante que quando uma transação é concluída, sua conclusão seja transmitida para toda a rede. Além disso, o objetivo do desenho do funcionamento do Blockchain é incentivar a descentralização como medida de segurança e redundância no funcionamento da rede, desencorajando atacantes gananciosos ou desonestos (NAKAMOTO, 2008).

Outro ponto de destaque que a descentralização influencia, é na complexidade regulatória, já que qualquer política do sistema acaba sendo altamente discricionária, rígida, e qualquer mudança no funcionamento do sistema depende de um consenso, ou seja, depende que os integrantes adotem uma mudança em massa (ULRICH, 2014).

A privacidade foi um ponto de extrema relevância trabalhado por todos os criptógrafos que serviram de inspiração para Nakamoto, e não ao acaso, a rede atingiu um alto grau de privacidade. Seu funcionamento é pseudônimo, onde se tem como identificação apenas um endereço bitcoin, e nenhuma conexão direta com as informações do mundo real do usuário. Seu rastreamento continuará sendo possível na medida em que se interaja com outras pessoas e instituições - como por exemplo, lojas. Já que as transações são facilmente rastreáveis entre si, o usuário poderá ser identificado por meio de investigações, ou empresas que exijam uma identificação mais detalhada, como no caso das corretoras que hoje adotam políticas de "conheça seu cliente" como um mecanismo de combate à lavagem de dinheiro. Portanto, podemos afirmar que o Bitcoin não se propõe a ser uma rede anônima (NAKAMOTO, 2008).

A irreversibilidade é uma característica inerente a estruturação em blocos do blockchain. Ao se fazer uma transação, o sistema de verificação assegura aquela transação, incluindo ela na

corrente de blocos, registrando a transferência dos recursos do pagador para o recipiente. A garantia da integridade do registro desses pagamentos é a chave para a impossibilidade de fraudes. Dessa forma, a rede checa a cadeia de negociações feitas anteriormente para garantir que a negociação foi legítima. Caso não seja legítima ou contenha algum erro, ela será descartada. Do contrário, o próximo bloco da cadeia será trabalhado para que o registro continue íntegro e dê continuidade para a corrente. Esse novo bloco inicia uma camada de verificação, e a cada bloco, novas camadas se formam, assegurando à cada verificação concluída, uma maior garantia da irreversibilidade (NAKAMOTO, 2008).

A importância dessa característica é, principalmente, viabilizar garantias de recebimento de pagamento, acabando com os gastos duplos e, em tese, viabilizando custos menores de transações, já que dispensa uma autoridade intermediando o processo. Nesse caso, não há possibilidade de inadimplência por parte do sistema ou fraudes com solicitações de reembolso, como nos cartões de créditos, proporcionando mais certeza referente ao recebimento da parte dos comerciantes que aceitem o meio como pagamento (ANTONOPOULOS, 2017).

Outro ponto que se torna uma qualidade poderosa do sistema, é ela ser tecnicamente irrestrita, visto que a rede é aberta para ser utilizada por qualquer usuário ou empresa que se integre ao sistema, funcionando em qualquer lugar, a qualquer hora, possibilitando transações milionárias ou pequenas com a mesma simplicidade - mas, ainda assim, podendo enfrentar restrições regulatórias, que independem das suas características técnicas. Além disso, o blockchain tem capacidade de acoplar melhorias, como “módulos”, que permitem um aperfeiçoamento contínuo no sistema (ULRICH, 2014).

A última característica do Blockchain para verificação de alguns dos pontos anteriores é a transparência do sistema. O registro das transações que são feitas no sistema é pública, de fácil acesso e global. Esses aspectos, permitem novas e extremamente dinâmicas formas de auditoria, possibilitando inclusive que a solvência e as reservas de uma empresa ou pessoa sejam facilmente provadas. Essa característica permite, dada a descentralização e transparência dos registros de transação, provar a posse ou a veracidade de uma informação (NAKAMOTO, 2008).

II.2.4 - Mineração, Transações e Armazenamento

Dada a profunda tecnicidade desse trecho, será abordado de maneira mais pontual, expondo os principais conceitos explorados por Nakamoto (2008) para a estruturação da rede.

Todo sistema de pagamento minimamente eficiente precisa de um método para registrar as transações, seja pela transferência de moeda manualmente entre pessoas ou o um registro feito em um sistema eletrônico. No caso do Bitcoin, esse registro, que é universal e público, é

preenchido na medida em que as negociações são verificadas como autênticas. “Ao invés de uma autoridade central confiável, no Bitcoin a confiança é alcançada como uma propriedade emergente das interações dos diferentes participantes no sistema bitcoin” (ANTONOPOULOS, 2017, p.22). Esse processo de verificação, que é chamado de mineração, é semelhante à execução de um exercício matemático extremamente complexo por computadores. O minerador que conclui o exercício, recebe um prêmio em bitcoin, que é composto, em parte referente aos custos de verificar a transação pagos pelos usuários e, em parte referente à uma emissão feita pelo próprio sistema, conforme segue citação a seguir:

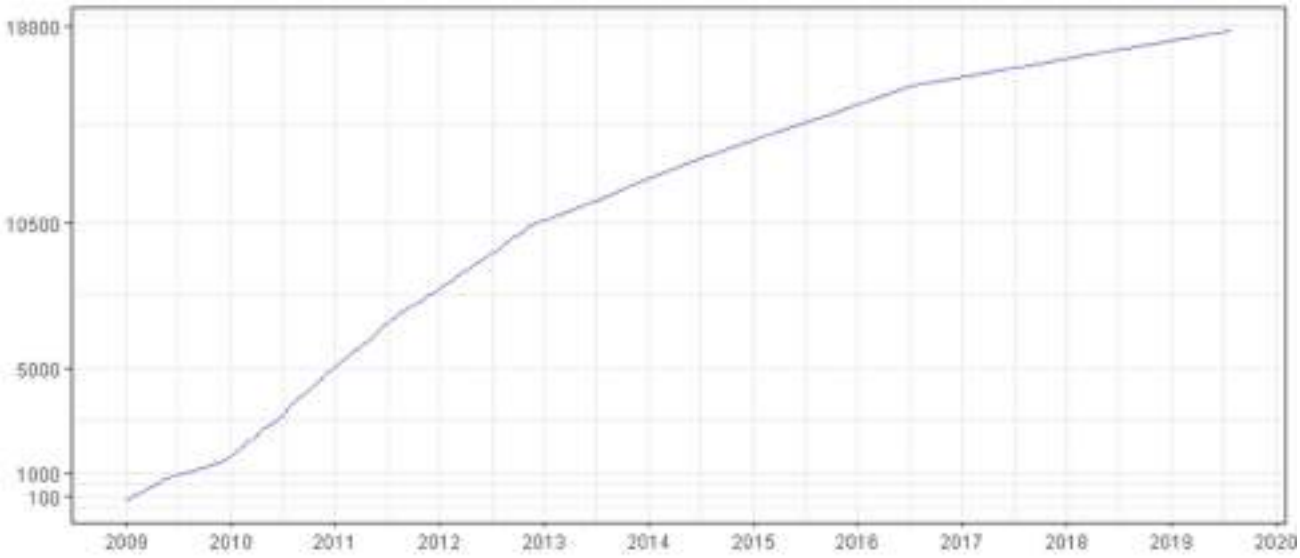
> “A real mineração de bitcoins é puramente um processo matemático. Uma analogia útil é a procura de números primos: costumava ser relativamente fácil achar os menores (Erastóstenes, na Grécia Antiga, produziu o primeiro algoritmo para encontrá-los). Mas à medida que eles eram encontrados, ficava mais difícil encontrar os maiores. Hoje em dia, pesquisadores usam computadores avançados de alto desempenho para encontrá-los, e suas façanhas são observadas pela comunidade da matemática(...); No caso do Bitcoin, a busca não é, na verdade, por números primos, mas por encontrar a sequência de dados (chamada de “bloco”) que produz certo padrão quando o algoritmo “hash” do Bitcoin é aplicado aos dados. Quando uma combinação ocorre, o minerador obtém um prêmio de bitcoins (e também uma taxa de serviço, em bitcoins, no caso de o mesmo bloco ter sido usado para verificar uma transação). O tamanho do prêmio é reduzido ao passo que bitcoins são minerados(...); A dificuldade da busca também aumenta, fazendo com que seja computacionalmente mais difícil encontrar uma combinação. Esses dois efeitos combinados acabam por reduzir ao longo do tempo a taxa com que bitcoins são produzidos, imitando a taxa de produção de uma commodity como o ouro. Em um momento futuro, novos bitcoins não serão produzidos, e o único incentivo aos mineradores serão as taxas de serviços pela verificação de transações”. (ULRICH, 2014, p.19-20)

Antonopoulos (2017) encontra uma maneira muito interessante de explicar a mineração, onde faz uma analogia a um gigantesco e competitivo jogo de sudoku. Ao ser concluído, ele é automaticamente reiniciado com seu nível de dificuldade reajustado para que a próxima solução demore cerca de 10 minutos para ser encontrada. Essa comparação acaba sendo muito pertinente, já que, apesar de ser potencialmente difícil seu preenchimento, é muito fácil que todos os participantes verifiquem que foi corretamente preenchido e reajustar o nível de dificuldade. O primeiro competidor a concluir corretamente o exercício é premiado, e todos os outros competidores descartam suas soluções e se inicia um novo turno de competição.

A mineração, portanto, além de ser o meio que garante a legitimidade dos registros de transações, acaba sendo também o processo por onde se emitem novas moedas para o sistema (ANTONOPOULOS, 2017). Esse processo de emissão, funciona através de uma regra discricionária, extremamente rígida e decrescente ao longo dos anos, como pode ser observado no gráfico I.1, com um limite máximo de 21 milhões de unidades, previsto para ser alcançado em 2140. No entanto, em 2032 já teria quase todas as unidades mineradas. Nakamoto (2008), elucida o processo, ao afirmar que “a adição estável de uma quantidade constante de novas

moedas é análogo a garimpeiros despender recursos para colocar mais ouro em circulação. No nosso caso, tempo de CPU e eletricidade que estão sendo consumidos" (NAKAMOTO, 2008, p.4).

Gráfico I.1: Quantidade BTC Emitidos de 03/01/2008 até 28/07/2019 em milhares de unidades. Escala Logarítmica.



Fonte: Blockchain; Elaboração: Própria

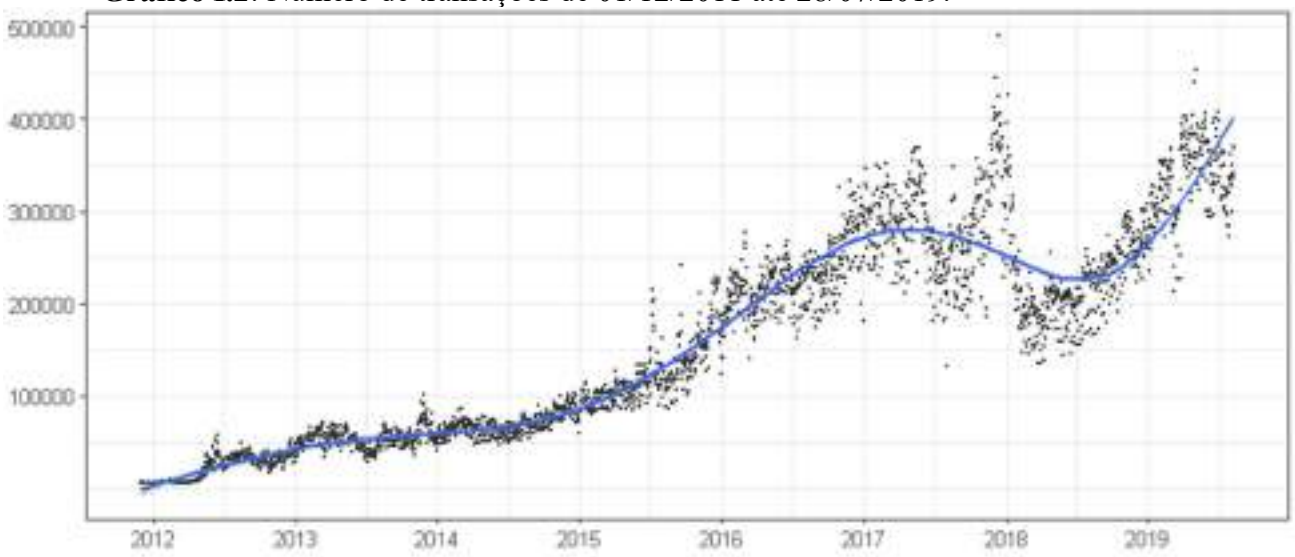
A transação de bitcoins pode ser considerada uma assinatura digital, onde um usuário aceita enviar para outro - por meio das suas chaves públicas (ou endereços bitcoin) - uma dada quantia. Após o envio, os mineradores, ao cobrarem uma tarifa, verificam a autenticidade daquela troca e conectam a cadeia de blocos do blockchain. Essa verificação se dá a partir do envio de chaves privadas - como uma assinatura ou senha - que garantem que o pagador é o dono da determinada quantia de bitcoins que estão conectados àquela conta. Isso significa que, feita a verificação, o usuário tem direitos de realocação, e pode passar o controle daqueles ativos para terceiros. Dessa forma, uma "mensagem" é enviada - com tal assinatura - para a rede, com a instrução de transferir a determinada quantia da carteira identificada para uma outra, mantendo o restante na carteira original (ANTONOPOULOS, 2017). Em outras palavras, esse processo pode ser descrito da seguinte maneira:

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

> registrada, carimbada com data e hora e exposta em um "bloco" do blockchain (o grande banco de dados, ou livro-razão da rede Bitcoin). A criptografia de chave pública garante que todos os computadores na rede tenham um registro constantemente atualizado e verificado de todas as transações dentro da rede Bitcoin, o que impede o gasto duplo e qualquer tipo de fraude." (ULRICH, 2014, p.18-19)

Devido a grande adesão ao bitcoin, o número de transações vem crescendo de maneira exponencial, e hoje ocorrem uma média de 300 mil transações diárias registradas na rede, conforme o gráfico I.2. Apesar do amplo crescimento, ainda é pequeno frente às 65 mil transações por segundo que as operadoras de cartão de crédito, como a Visa, conseguem suportar em seus testes de stress[13]. Isso aponta para a magnitude na imaturidade da tecnologia, visto que apesar do pouco uso, ainda assim enfrentou congestionamentos em sua rede em alguns momentos[14]. Outro dado que também deixa clara essa diferença, é o fato da visa ter 3.3 bilhões de cartões em circulação, enquanto o número de carteiras blockchain chegou a 40 milhões, deixando claro que ainda há muito espaço para amadurecimento, e que muito ainda precisa ser tecnicamente aperfeiçoado para chegar aos níveis competitivos frente às grandes operadoras e demais meios de pagamento. É válido ressaltar que os custos de transações proporcionam um entrave a larga adesão, mas trataremos do tema no item III.2, a respeito das funções da moeda e do uso do bitcoin como meio de troca.

Gráfico I.2: Número de transações de 01/12/2011 até 28/07/2019.



Fonte: Blockchain; Elaboração: Própria

13 Ver https://www.visa.gr/dam/VCOM/download/corporate/media/visanet-technology/aboutvisafactsheet.pdf

14 Ver https://guiadobitcoin.com.br/crise-na-blockchain-mais-de-140-000-transacoes-na-fila/

Esse registro atualizado de transações, somado as assinaturas digitais, faz com que sejam possíveis as movimentações dos valores depositados nessas chaves públicas, dispensando a existência de arquivos de bitcoin, bastando sua chave como recurso para movimentar esse saldo. O armazenamento dessas chaves privadas de acesso são chamados de carteiras, que podem ser "quentes" ou "hot wallets", quando conectadas diretamente com a internet, permitindo um dinamismo maior nas transações. Porém, esse aspecto aponta para uma menor segurança, já que são dispositivos capazes de serem hackeados. Essas carteiras, também podem ser "frias" ou "cold wallets", onde as mesmas chaves são armazenadas em dispositivos ou meios desconectados com a internet, como pendrives ou até uma folha de papel. Enquanto o problema das carteiras quentes é a vulnerabilidade da segurança por ataques cibernéticos, nas frias o problema se torna puramente mecânico: tais objetos podem ser danificados, extraviados ou destruídos, impedindo o acesso, descartando completamente e permanentemente os ativos ligados a ela (ANTONOPOULOS, 2017).

II.3 - Usos e desafios da tecnologia

"Ao infinito e além"
Buzz Lightyear

II.3.1 - Outras aplicações

O potencial de uma nova tecnologia dificilmente é explorado na introdução da mesma no mercado. Bitcoin é um projeto aberto, onde qualquer pessoa pode basicamente fazer algumas mudanças no protocolo inicial - renomear e lançar como de sua autoria, novas aplicações ou usos. Tecnicamente é fácil criar uma nova moeda, mas é muito difícil obter o efeito de rede. O desdobramento das aplicações da tecnologia que surge com o bitcoin é um ponto válido a ser abordado, já que permite repensar também novos caminhos para as tecnologias usadas atualmente. Como citado por Ulrich (2014):

> "Uma das aplicações mais promissoras do Bitcoin é como uma plataforma à inovação financeira. O protocolo do Bitcoin contém o modelo de referência digital para uma quantidade de serviços financeiros e legais úteis que programadores podem desenvolver facilmente. Como bitcoins são, no seu cerne, simplesmente pacotes de dados, eles podem ser usados para transferir não somente moedas, mas também ações de empresas, apostas e informações delicadas[15]. Alguns dos atributos que estão embutidos no protocolo do Bitcoin incluem micropagamentos, mediações de litígios,

15 Nota do autor: BRITO, Jerry. The Top 3 Things I Learned at the Bitcoin Conference. Reason, 20 mai. 2013. Disponível em: . Acesso em: 12 dez. 2013.

> contratos de garantia e propriedade inteligente[16]. Esses atributos permitiriam o fácil desenvolvimento de serviços de tradução via internet, processamento instantâneo de transações pequenas (como medição automática de acesso Wi-Fi) e serviços de crowdfunding[17].” (ULRICH, 2014, p.27)

Hoje pode-se contar com registros financeiros eletrônicos de ativos como ações, empréstimos, derivativos e títulos. Todos esses registros ficam sob posse das autoridades e intermediários envolvidos no processo, como os bancos e corretoras que mantêm os dados referentes às posses que um determinado cliente possui sobre certos ativos. A extensão do impacto das criptomoedas na economia real é uma grande incógnita. De fato esses impactos ocorreram, mas a magnitude pode ser muito maior do que a que pode-se observar atualmente, visto que, de maneira bem simplista, é possível afirmar que cada um desses registros estão “vulneráveis” a serem alvos dessa inovação. Todos podem ser facilmente migrados para plataformas como o blockchain, e permitir que sua negociação se dê de maneira eletrônica, dinâmica e independente.

A utilização do Bitcoin como meio de pagamento é um dos principais temas abordado neste trabalho. Dessa afirmação, podemos derivar outras possibilidades. Sendo o BTC um registro imutável, toda transação de bens e serviços é passível de utilizar um protocolo semelhante de registro como forma de assegurar a transação como feita. Tendo isso em vista que as criptomoedas podem assumir o papel de um contrato - podendo ser chamadas de *tokens* ou moedas coloridas - onde as partes envolvidas assumem uma premissa de valor para aquele ativo, ao trocar de mãos, o novo proprietário se torna detentor daquele direito (ANTONOPOULOS, 2017). Isso ocorre com a separação de uma quantidade de bitcoin para outro propósito:

> “Imagine, por exemplo, pegar uma nota de R$ 1 e colocar um selo que diz "Esse é 1 certificado de ações de uma ação da Acme Ltda." Agora a nota de R$1 serve para dois propósitos: É uma nota de dinheiro e também um certificado de ações. Como ela é mais valiosa como uma ação, você não vai querer usá-la para comprar bala, de forma que ela

16 Nota do autor: HEARN, Mike. Bitcoin 2012 London: Mike Hearn. YouTube video, 28:19, publicado por “QueuePolitely,” 27 set. 2012. Disponível em: . Acesso em: 13 dez. 2013. Propriedade inteligente (smart property) é um conceito para controlar propriedade de um item por meio de acordos feitos no blockchain do Bitcoin. A propriedade inteligente permite que as pessoas intercambiem propriedade de um produto ou serviço uma vez que uma condição é atingida usando a criptografia. Embora a propriedade inteligente seja ainda teórica, os mecanismos básicos já estão incorporados ao protocolo do Bitcoin. Ver Bitcoin wiki “Smart Property”. Disponível em https://en.bitcoin.it/wiki/Smart_Property. Acesso em: 13 dez. 2013.

17 Nota do autor: O financiamento coletivo (crowdfunding) consiste na obtenção de capital para iniciativas de interesse coletivo por meio da agregação de múltiplas fontes de financiamento, em geral, pessoas físicas interessadas na iniciativa. O termo é muitas vezes usado para descrever especificamente ações na internet com o objetivo de arrecadar dinheiro para artistas, jornalismo cidadão, pequenos negócios e startups, campanhas políticas, iniciativas de software livre, filantropia e ajuda a regiões atingidas por desastres, entre outras.

> não é mais útil como dinheiro. Moedas coloridas funcionam da mesma forma, convertendo uma pequena e específica quantidade de bitcoin em um certificado negociável que representa outro ativo. O termo "color" ou "cor" refere à ideia de dar um significado especial através da adição de um atributo tal como uma cor — é uma metáfora, não uma associação a uma cor real. Não há cores nas moedas coloridas." (ANTONOPOULOS, 2017, p. 236)

Um exemplo de token que simplifica a comunicação da economia internacional com o universo das criptomoedas são as stable coins, ou moedas estáveis. Tais moedas tem como característica única seu pareamento de preços com uma moeda real, mantendo um lastro de proporção idêntica ao número de moedas em circulação. Por exemplo, o Theter é uma moeda que tem essa característica e durante muito tempo foi a única moeda estável relevante, que tinha sua versão pareada com o Dólar e com o Euro. Nessa modalidade de criptomoeda, é possível espelhar uma moeda com todas as funções perfeitamente assumidas e, é através dela que algumas empresas de cartão de crédito tem feito a ponte com a economia real, aceitando transações em moeda eletrônica como forma de pagamento (ANTONOPOULOS, 2017).

Como citado anteriormente, da mesma forma que criptomoedas podem ser lastreadas em moedas reais, assumindo seu valor, também podem assumir valor de ações de empresas e outros ativos da economia real, como imóveis. Um exemplo é a Mastercoin, que "não é primariamente uma moeda. Ao invés disso, é uma plataforma para construir outras coisas, como moedas de usuário, tokens de propriedade smart, meios descentralizados de troca de ativos, e contratos" (ANTONOPOULOS, 2017, p. 238). Basicamente, tal moeda irá atuar como um registro, arquivado dentro da blockchain do Bitcoin, mas usando uma camada de protocolo sobre o bitcoin (ANTONOPOULOS, 2017).

O universo das aplicações das criptomoedas é muito amplo, mas dividido basicamente em dois grandes nichos além das colored coins. As altcoins - versões de criptomoedas primariamente usadas como moedas - e as altchains - que assumem outras propostas, mas são moedas primariamente. As altcoins costumam apresentar diferenças relevantes do bitcoin em três áreas: política monetária, mecanismo de consenso/prova de trabalho e características muito específicas, como a anonimidade (ANTONOPOULOS, 2017). Já as Alt Chain podem ter como definição o seguinte ponto:

> "Alt chains são implementações alternativas do padrão de design da blockchain, que não são primariamente utilizadas como moeda. Muitas incluem uma moeda, mas a moeda é usada como um token para alocar alguma outra coisa, como um recurso ou um contrato. A moeda, em outras palavras, não é o ponto principal da plataforma; ela é uma funcionalidade secundária." (ANTONOPOULOS, 2017, p. 246)

Como exemplo de altchain, de acordo com Antonopoulos (2017), serão citadados dois casos. O primeiro é o Namecoin, a primeira bifurcação do código do bitcoin, que surge em

2012. Ela tem como objetivo dar suporte ao registro de domínios globais, não tendo como principal foco servir de meio de pagamento, apesar de seu chain incluir uma moeda (NMC). O Segundo caso é o Ethereum, lançado em 2014 pelo russo Vitalik Buterin, que é uma forma de processar contratos em linguagem Turing completa dentro de uma plataforma semelhante ao blockchain, mas com uma mecânica muito diferente do bitcoin. Tanto o bitcoin quanto o Ethereum possuem moedas disponíveis em sua rede (bitcoin e ether - ETH), mas o primeiro é feito em uma língua de programação bem simples, enquanto o segundo, pode registrar contrato em uma linguagem turing completa. Esses contratos são capazes de guardar informações, enviar, armazenar e receber pagamentos em ETH e uma série ilimitada de ações computáveis.

Detalhar muitas dessas altcoin e altchain estenderá o trabalho além do necessário, sendo a função desse trecho unicamente expor que a tecnologia, feita há pouco mais de 10 anos, já tem características interessantes o suficiente para impactar qualquer setor altamente conectado a registros: meios de pagamento, imóveis, pessoas (nascimento, casamento, certificações, óbito, etc), mercado acionário, mercado de crédito, registro de posse de bens e raridades (como diamantes, artes e outros), contratos (com cláusulas automáticas de execução de garantias), veículos de remessas ou transmissão de herança e muito mais (ANTONOPOULOS, 2017).

II.3.2 - Riscos e Mal uso

O uso do Bitcoin, tanto como meio de pagamento ou como protocolo de registro, é crescente. Um dos principais pilares desse movimento é a confiança, que é fundamental, assim como vem sendo no desenvolvimento de toda economia monetária. Sendo esse seu principal ativo, os riscos que possam abalar essa confiança precisam ser melhor detalhados. O sistema, em sua estrutura, apresenta alguns riscos que podem, ao longo do tempo, não só minar o seu uso, mas também extinguir sua viabilidade. Cada ponto é muito extenso e pode ser melhor discutido em literatura especializada[18], sendo assim, esse tópico irá abordar alguns pontos críticos que se destacam no sistema e compreenderá uma discussão a respeito do mal uso por parte da comunidade. Os riscos que envolvem o Bitcoin podem basicamente ser divididos em 4 tipos: técnicos, de custódia, regulatórios e de adoção (ANTONOPOULOS, 2017).

Dentre os riscos que assombram a rede, os mais críticos são os técnicos. Devido a sua estrutura de criptografia, uma falha no uso das chaves públicas/privadas da rede, deixaria elas abertas ou acessíveis, o que seria fatal. Existe uma possibilidade de ocorrência, devido a uma

18 Ver Antonopoulos (2017)

perda de efetividade do padrão de criptografia atual: esse atual se tornaria vulnerável, tendo em vista as constantes melhorias no poder computacional. Isso forçaria uma atualização no núcleo de criptografia da estrutura do bitcoin, não sem antes provavelmente arruinar a confiança no sistema. Apesar do risco, o protocolo de segurança que protege o bitcoin já foi testado diversas vezes por especialistas em segurança e hackers e é considerado muito robusto. O risco criptográfico do bitcoin é muito pouco provável, mas ainda é possível e crítico (ULRICH, 2014).

Além deste, podem ocorrer riscos de defeito na própria programação do bitcoin, ou seja, bugs. Programas podem ter bugs, é muito comum que ocorra. Um defeito desse tipo poderia afetar qualquer aspecto do bitcoin, mas poderia ser especialmente grave se ocorresse afetando, por exemplo, o consenso da rede como um todo, permitindo resultados completamente fora do esperado. Apesar da possibilidade, o núcleo do Bitcoin, ou *Bitcoin core*[19], é um dos códigos mais revisados do mundo. Porém, não é impossível que ainda existam bugs não detectados. Essa possibilidade, ao afetar o consenso, cria um problema que é o risco de bifurcações no sistema, onde mineradores trabalhariam em diferentes correntes do blockchain, desenvolvendo de maneira independente uma nova cadeia de registro. Essas bifurcações ocorrem normalmente, mas em tamanho muito reduzido com duração de poucos minutos - um bug como esse poderia levar a longas cadeias de bifurcação. Em 11 de março de 2013 ocorreu um bug desse tipo que durou 6 horas até ser resolvido, gerando uma bifurcação e uma "corrida" de venda de bitcoins[20] (TRACHSLER, 2019).

Atualmente, o desenvolvimento do núcleo do bitcoin é lento, mas muito cuidadoso para proteger a integridade do sistema. No entanto, existe a possibilidade de que problemas como esses possam ocorrer novamente em um futuro, e o dano possível de acontecer, tanto técnico quanto de confiança, até o momento é desconhecido (ULRICH, 2014; ANTONOPOULOS, 2017).

Outro risco no sistema é um risco teórico, chamado de ataque de consenso ou ataque dos 51%. Nele um minerador ou um grupo de mineradores pode, via consenso, ao assumir mais de 50% do poder computacional, permitir o gasto duplo na rede. Esse ponto é mais simples, já que tecnicamente é recuperável, além de não apresentar risco de roubo de bitcoins. Ele também pode ter seu risco mitigado através de alterações na programação do bitcoin, mas

19 Forma como é chamado a estrutura central de programação onde foi e é desenvolvido o bitcoin e suas melhorias.

20 Ver https://bitcoin.org/en/alert/2013-03-11-chain-fork

potencialmente diminuiria o grau de descentralização do sistema. O risco do ataque de consenso é tecnicamente recuperável, mas seu dano de imagem é difícil de prever (WOO, 2013; ANTONOPOULOS, 2017).

Além dos riscos técnicos, também se apresentam os riscos exógenos ao sistema. Um desses é o risco de custódia. Muitos bitcoins ficam depositados em carteiras virtuais e corretoras, ou seja, com intermediadores responsáveis pela custódia. Caso algum desses perca ou seja roubado, nenhuma agência reguladora ou entidade governamental teria jurisdição direta para exigir a devolução dos valores. Isso faz com que qualquer depósito nesse tipo de instituição seja um voto absoluto de confiança, pois não há nenhuma garantia de recuperação em caso de perda ou outro tipo de dano. Essa estrutura em muito se difere do modelo tradicional, que tem grandes reguladores, como é o caso do Banco Central, que aqui no Brasil tem uma série de mecanismos para garantir a solvência dos bancos e instituições relacionadas. Então, qualquer evento que prejudique o intermediário, automaticamente faria com que as criptomoedas custodiadas estejam potencialmente perdidas ou vulneráveis. Reguladores vem tentando atuar muito mais na questão de proteção ao consumidor nesse caso, do que propriamente de proteção financeira. O risco de custódia vem caindo drasticamente com o amadurecimento do mercado, mas ele ainda é uma possibilidade, e um erro pode afetar de maneira muito profunda a confiança no sistema como um todo (WOO, 2013; ECB, 2012).

Um ponto que fragiliza demais o sistema como um todo é o risco regulatório. Estudos apontam que, além de ser um fator que pode potencialmente mitigar[21] ou encerrar[22] o uso da criptomoeda em determinada região, é também um causador de intenso aumento de volatilidade[23], o que acaba prejudicando a expansão do ativo. Esse fato é resultado da grande incerteza e do pouco consenso acerca de como tratar o ativo a nível internacional[24]. O risco regulatório, por hora, existe e ainda existirá por algum tempo, enquanto as autoridades não tomarem um direcionamento mais claro.

O último ponto é mais abrangente: o risco de adoção da moeda. Nesse ponto se enquadra tanto o risco de deixarem de usar a moeda, quanto o risco de usarem o desconhecimento ou a pouca regulação do sistema como um meio de praticar atividades criminosas. O mercado de criptomoedas tem sido canal de fraudes, esquemas ponzi[25], lavagem de dinheiro e muitos

21 Ver https://www.cftc.gov/PressRoom/PressReleases/pr7231-15

22 Ver https://www.theverge.com/2017/9/18/16326078/chinese-regulators-ban-cryptocurrency-platforms-bitcoin

23 Ver https://www.fxcm.com/uk/insights/what-causes-volatility-in-bitcoin/

24 Ver https://www.loc.gov/law/help/cryptocurrency/world-survey.php

25 Ver ECB (2012)

outros. Ulrich (2014) relata o famoso caso do Silk Road[26], um conhecido site da *deep web*[27], onde ocorriam diversos tipos de transações ilegais, como vendas de drogas e outros produtos ilícitos e até lícitos. Além desse caso, diversas outras operações notaram o uso do ativo como meio para lavagem de dinheiro, até mesmo no Brasil[28]. Esse uso controverso do sistema foi e vem sendo razão para uma caçada ao sistema como um todo[29], em vez de focar nos usuários mal intencionados. Outro ponto que embasou as autoridades nessa corrida foi o caso do Liberty Reserve, uma moeda digital centralizada, que teve sua operação encerrada após alegações do uso para lavagem de dinheiro[30] (ULRICH, 2014). O desmembramento de esquemas ponzi e pirâmides financeiras também tem sido uma constante nesse mercado. Inclusive, a nível nacional, diversos casos estão sendo investigados e denunciados[31]. O crescimento da prática tem sido tanto[32] que a CVM publicou recentemente uma página para auxiliar na identificação desse tipo de iniciativa, visando mitigar a atuação de criminosos no mercado brasileiro[33]. É válido pontuar que quase a totalidade dos riscos de adoção que atingem o bitcoin são perfeitamente passíveis de ocorrerem com o papel moeda. O pseudonimato proposto pelo sistema pouco difere no mal uso de cédulas para aquisição de serviços ou produtos ilícitos, onde as partes podem efetuar transações sem necessariamente se identificarem umas às outras. O ponto é que no blockchain ocorrem registros públicos dessas transações, dificultando o anonimato, já que permitem o rastreamento dos envolvidos. Diferente do rastreio do dinheiro espécie que só é possível em caso de cédulas marcadas (ECB, 2012).

---

26 Nota do autor: O site Silk Road foi fechado pelas autoridades americanas no final de 2013, mas a associação do Bitcoin ao uso para fins criminosos é algo recorrente. Isso nos remete a um ponto fundamental: o Bitcoin é uma tecnologia e, portanto, não é boa nem má. É neutra. O crime está na ação do infrator, jamais na tecnologia empregada para tal. O Bitcoin, ou qualquer outra forma de dinheiro, pode ser usado para o bem ou para o mal. Além disso, a compra e venda de drogas, dependendo do país, já é algo normal e perfeitamente lícito. Isso quer dizer que a proibição das drogas é uma questão política que independe por completo do Bitcoin. Ademais, a experiência sugere que a guerra às drogas é muito mais nefasta do que qualquer consequência derivada de seu uso por cidadãos honestos.

27 Nota do autor: Wikipedia "Deep Web". Disponível em http://en.wikipedia.org/wiki/Deep_Web. Acesso em: 30 jul. 2013.

28 Ver https://canaltech.com.br/criptomoedas/policia-encontra-laboratorio-de-bitcoins-usado-para-lavagem-de-dinheiro-no-rs-137833/

29 WOLF, Brett. Senators Seek Crackdown on 'Bitcoin' Currency, Reuters, 8 jun. 2011. Disponível em: <http://www.reuters.com/article/2011/06/08/us-financial-bitcoins-idUSTRE7573T320110608>. Acesso em: 14 dez. 2013.

30 Liberty Reserve Digital Money Service Forced Offline, BBC News—Technology, 27 mai. 2013. Disponível em: <http://www.bbc.co.uk/news/technology-22680297> . Acesso em: 14 dez. 2013.

31 Ver http://www.cvm.gov.br/noticias/arquivos/2018/20180322-1.html

32 Ver https://www.gazetadopovo.com.br/economia/cvm-recorde-investigacoes-irregularidades-piramides/

33 Ver http://www.cvm.gov.br/menu/investidor/alertas/ofertas_atuacoes_irregulares.html

CAPÍTULO III - CARACTERÍSTICAS E FUNÇÕES DA MOEDA NAS CRIPTOMOEDAS

"Qualquer um pode criar dinheiro; o problema está em fazer as pessoas aceitarem ele."
Hyman Minsky

O ponto guia da terceira parte desse trabalho é uma abordagem mais quantitativa. A tentativa é se afastar um pouco dos fatos históricos na elaboração e no desenvolvimento do sistema, e focar principalmente na discussão e no comportamento que os dados apresentam. Apesar do Bitcoin ser uma inovação no sistema de pagamento, para que ele assuma de fato o papel de moeda, na forma que apontam os manuais de economia, há uma série de pressupostos. Para que sejam cumpridos, o bitcoin precisa servir como reserva de valor, meio de troca e unidade de conta. Independente de um ativo assumir essas característica, não há garantia de que ele necessariamente seja aceito como dinheiro para fins regulatórios ou legais. O debate tratado nesse capítulo se aterá às funções das características da moeda, sem pretensão de definir necessariamente que esse ativo de fato é dinheiro. Além das funções da moeda, serão discutidas as características desejáveis da moeda no bitcoin, onde ela deve apresentar as seguintes características: *divisibilidade, transferibilidade, facilidade de manuseio e transporte, indestrutibilidade, inalterabilidade e homogeneidade*, como definido por CARVALHO et al. (2007).

III.1 - Características desejáveis da moeda nas criptomoedas

"Quando não temos nada, não temos nada a perder"
Bob Dylan

Todo bitcoin precisa ser transacionado com auxílio direto ou indireto do meio eletrônico, visto que o uso do blockchain é essencial para o registro da transação. Essa característica torna, inicialmente, essa análise fundamentalmente diferente do direcionamento clássico das características desejáveis da moeda no papel moeda, frente a essas mesmas características na moeda eletrônica. Hoje a maior parte das transações financeiras do planeta se dá via meios eletrônicos. Além disso, é possível afirmar que quase toda custódia desses ativos nada mais são do que informações inseridas em balanços financeiros de bancos, armazenados em computadores. Outro ponto que se pode enumerar é que a gestão e movimentação de grande

parte desses ativos é feita eletronicamente, sem nenhuma ou quase nenhuma materialização do capital envolvido. Sabendo disso, a realidade em que está submerso o bitcoin - no qual é impossível negociar sem seu sistema eletrônico - é semelhante e, potencialmente, poderá ser a mesma realidade de todo sistema de pagamento futuramente, afinal, o dinheiro como é conhecido hoje, já é basicamente um ativo digital. Se for tomada essa última afirmação como verdadeira, pode-se olhar as características desejáveis de uma outra forma nas criptomoedas.

A primeira que se pode abordar é a *divisibilidade*. Nakamoto (2008) em seu protocolo, traz um limite total de emissão de 21 milhões de unidades. Esse limite seria um problema no uso comercial, já que tiveram momentos de cada unidade valer aproximadamente 20 mil dólares, o que teria dificultado o uso como meio de pagamento. O grande ponto dessa característica é que cada unidade de BTC tem a possibilidade de divisão em até 8 casas decimais, que traz uma disponibilidade de $21x10^{14}$ unidades de satoshi[34]. Esse fracionamento da unidade de BTC permite negociações de todos os tamanhos, inclusive micro pagamentos. Além disso, o protocolo permite que esse número de casas decimais se expanda indefinidamente, se necessário, somente necessitando passar pelo consenso da rede (CARVALHO et al., 2007; ULRICH, 2014).

Três características se aproximam ao serem explicadas no bitcoin, o que não necessariamente se aplica em moedas antigas: *facilidade de manuseio e transporte, indestrutibilidade e transferibilidade*. Por conta de diversas experiências com moedas de tamanhos e formas exóticas[35], a logística desses ativos se tornou uma característica extremamente desejável.

A *facilidade de manuseio e transporte*, por conta de se tratar de dinheiro eletrônico, tem como único entrave essa necessidade de comunicação dos usuários com um canal que se comunique com o blockchain, seja por uma via de aplicação no seu próprio dispositivo eletrônico ou por outra em que tenha um intermediário que faça a solicitação. Sendo hoje o dinheiro basicamente um ativo digital, esse não é um entrave para a maior parte dos volumes financeiros que circulam o planeta (CARVALHO et al., 2007; ULRICH, 2014).

A *indestrutibilidade* estava atrelada ao fato do ativo não perder facilmente suas características físicas - como seria se fossem usados guardanapos como forma de pagamento. O Bitcoin, por ser uma rede eletrônica com seus registros descentralizados, acaba possuindo

34 Satoshi é o nome que se dá a menor fração atual do bitcoin que equivale a 1/100000000 da unidade de BTC

35 Ver https://www.bbc.com/portuguese/vert-tra-44374327

um poder de durabilidade, ou indestrutibilidade, muito superior a maior parte, senão totalidade, das entidades do setor financeiro. Enquanto o usuário tiver sua chave privada armazenada em algum lugar, e a rede continuar funcionando de maneira íntegra, ele terá como recuperar seus ativos (CARVALHO et al., 2007; ULRICH, 2014).

Outro ponto importante é a *transferibilidade*, que é outra característica facilmente observável, já que, com uma chave pública, uma privada e uma ordem enviada para a rede, é possível transferir qualquer quantidade monetária que se tenha para qualquer pessoa no planeta sem nenhum entrave ou barreira burocrática (CARVALHO et al., 2007; NAKAMOTO, 2008).

Além desses pontos, restam as características de verificabilidade do ativo, que são a *homogeneidade* e *inalterabilidade*. Nelas se atém pontos que permitem a fácil verificação da autenticidade, que também dificultam a falsificação daquele ativo ao longo do tempo, dando a ele uma característica escassa. Isto é, na medida que ocorre um controle de emissão, seja natural, como foi o caso da era metalista, que dependia da mineração do ouro e da prata, ou burocrático, onde um governo influencia no volume do papel moeda em circulação, seja indiretamente, com a mudança da taxa de compulsório, como no caso brasileiro, ou diretamente, através da emissão primária.

A *inalterabilidade* está intimamente ligada à possibilidade de falsificação e alteração de um ativo - como, por exemplo, ao misturar ouro com outros metais para assegurar mais peso em uma negociação. Esse processo é, a princípio, impossível. A rede não permite a criação de novos bitcoins que não seja pela via mineração. É possível, teoricamente, apenas adulterar negociações para que bitcoins sejam roubados de terceiros ou, também, que se pratique o gasto duplo através do ataque dos 51%. Essa é uma característica muito forte da rede e é intrínseca a sua constituição. Da mesma maneira, a *homogeneidade* é uma característica inerente ao sistema, desejável para fácil identificação de um ativo como legítimo e válido. Já que o bitcoin é uma informação eletrônica dentro de uma rede, acaba sendo perfeitamente homogêneo, podendo armazenar centavos ou milhões sem nenhuma diferença técnica (CARVALHO et al., 2007; ULRICH, 2014).

III.2 - Funções clássicas da moeda nas criptomoedas

"Nenhuma árvore pode crescer até o céu sem ter suas raízes no inferno."
Carl Gustav Jung

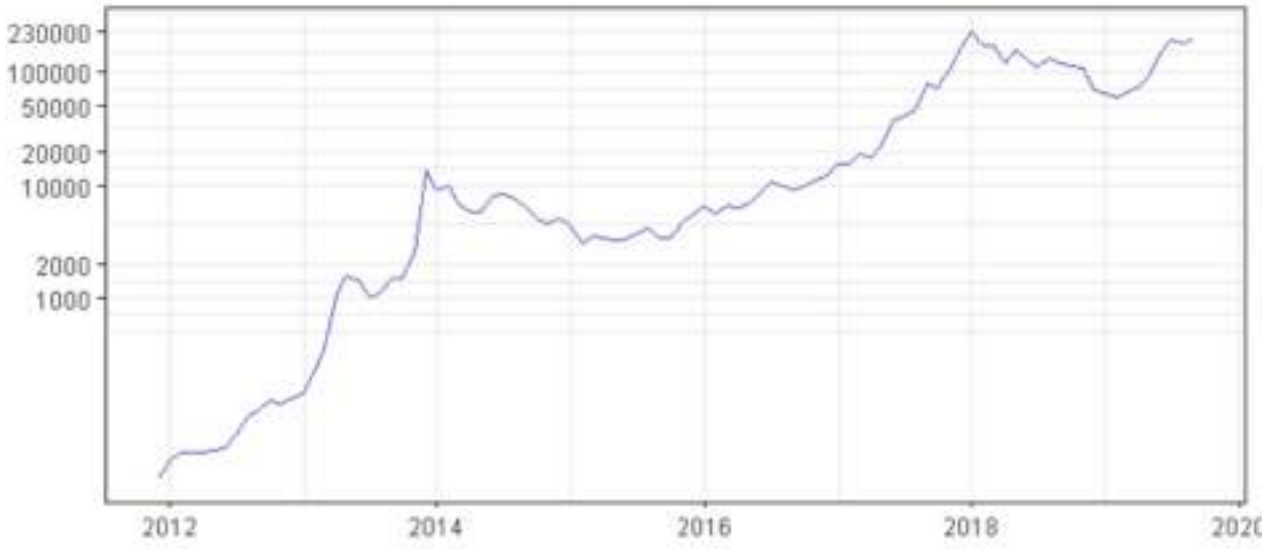
A estruturação das funções da moeda pode ser vista como uma grande hierarquia de grandeza, onde primeiro um ativo atinge a função de reserva de valor para várias pessoas, como por exemplo obras de arte e casas. Para que estes possam assumir a função de meio de troca, é

necessário que pelo menos duas pessoas, que vejam esse item como reserva de valor, queiram fazer uma permuta usando aquele ativo como referência de pagamento naquela dada situação. Para assumir a função de unidade de conta, é necessário que um espectro muito variado de serviços e itens naquela sociedade que estão inseridas essas pessoas possam ser precificados usando unidades daquele ativo. Dado isso, será abordardada neste tópico cada uma das funções, discutindo-as, tentando compreender o que influencia esse processo.

III.2.1 - Reserva de valor

Sendo a mais ampla das funções da moeda, a reserva de valor consiste simplesmente em entender o comportamento do preço do ativo, crendo que o mesmo é estável a nível de manutenção de poder de compra ao longo do tempo. Um dos principais recursos que se tem é o histórico do valor total do Market Cap[36] desde sua origem. Tal valor vem em uma crescente muito acelerada, mas com muita volatilidade, onde o mercado saiu de um valor de poucos centavos em sua origem e hoje possui uma capitalização de pouco mais de 200 milhões de dólares, como pode ser visto no gráfico seguinte:

Gráfico II.1: Valor total do Market Cap do BTC em Milhares de Dólares. Escala logarítmica



Fonte Blockchain em 12 ago 2019; Elaboração: Própria

36 Soma dos valores de todos os bitcoins em circulação.

Esse movimento de preços, por ser voluntário e sem nenhuma demanda intrínseca do sistema que está inserido - como por exemplo no uso de produção de bens ou consumo - merece destaque por seu caráter espontâneo. Mas, da mesma forma, a ausência dessa demanda intrínseca ou uma autoridade regulando, não proporciona certeza na manutenção dessa característica de reserva de valor, tendo como ponto favorável a escassez extremamente rígida do sistema. Dessa forma, a referência da valorização do preço de negociação do BTC não é suficiente para ser determinada como uma reserva de valor ou não. Ainda assim, é importante a discussão de outros possíveis mecanismos de medição de valor ao longo do tempo, das utilidades propostas pelo sistema, e se existem múltiplos de outras instituições que se possa tomar como referência na hora de traçar um possível *valuation*[37] para a rede como um todo.

Na busca de respostas para esse valor, Woo (2013), apresenta uma discussão onde evidencia a possibilidade do bitcoin não possuir um valor fundamental, mas sim, um valor referente às propriedades relacionadas a sua semelhança ao dinheiro ou uma commodity escassa. O autor conclui que o bitcoin pode se tornar um meio de pagamento relevante e com um claro potencial de crescimento, sendo uma possível ameaça a todos os provedores tradicionais de transferência, como a Western Union e o Paypal. A possibilidade de evasão de taxações foi também outro ponto favorável, mas ainda especulativo, para a adoção da tecnologia, porém, com um certo limite nesse uso, dado que é possível a identificação dos integrantes envolvidos. Como ponto paradoxal ele vê que há um problema grave no fato de que quanto mais se toma o BTC como reserva de valor, pior seria para o seu uso como meio de troca, já que agregaria uma alta volatilidade ao ativo, dificultando sua aceitação geral como meio de pagamento (WOO, 2013).

Na tentativa de entender o valor do Bitcoin, Bouoiyour e Selmi (2015) fazem um extenso estudo econométrico a respeito dos dados disponíveis no mercado de criptomoedas com variáveis independentes, como o mercado do ouro e, inclusive, pesquisas no google usando o termo "bitcoin". Os resultados dessas regressões não foram significativos, e os autores concluem:

> "So, is Bitcoin a long-term promise? Given our obtained findings, it is difficult to reach clearer, solid and unambiguous evidence into Bitcoin phenomenon, since it is uncertain. This nascent digital money can remain as it can disappear, especially when considering that Bitcoin faces a structural economic problem regarding its limited amount recording 21 million units in 2140, implying that the money supply cannot continue to rise after this date. There are, up to now, 12 million Bitcoin in circulation. If this famous crypto-

37 Termo que refere a valoração, ou seja, prática na qual se calcula um suposto preço justo de um determinado ativo ou empresa.

> currency successfully displace fiat currencies (euro, dollar and yen), it will exert sizable deflationary pressures. Without definitely tackling the causes, the virtual currency seems highly correlated to the speculative behaviors of investors or people who hold it. This digital money is not issued by banking system and even less by any government, but by a computing algorithm. Unfortunately, the majority of users have not acknowledged about mathematical programs, and it is therefore unknown for them how far it can go. In sum, no one can predict the precise value and the specific form crypto-urrency will take since the technological development is heavily unpredictable. As technology becomes increasingly integrated into our everyday lives, crypto-currencies will obviously continue to grow and Bitcoin may probably be displaced by better digital currencies."38 (BOUOIYOUR E SELMI, 2015, p. 469)

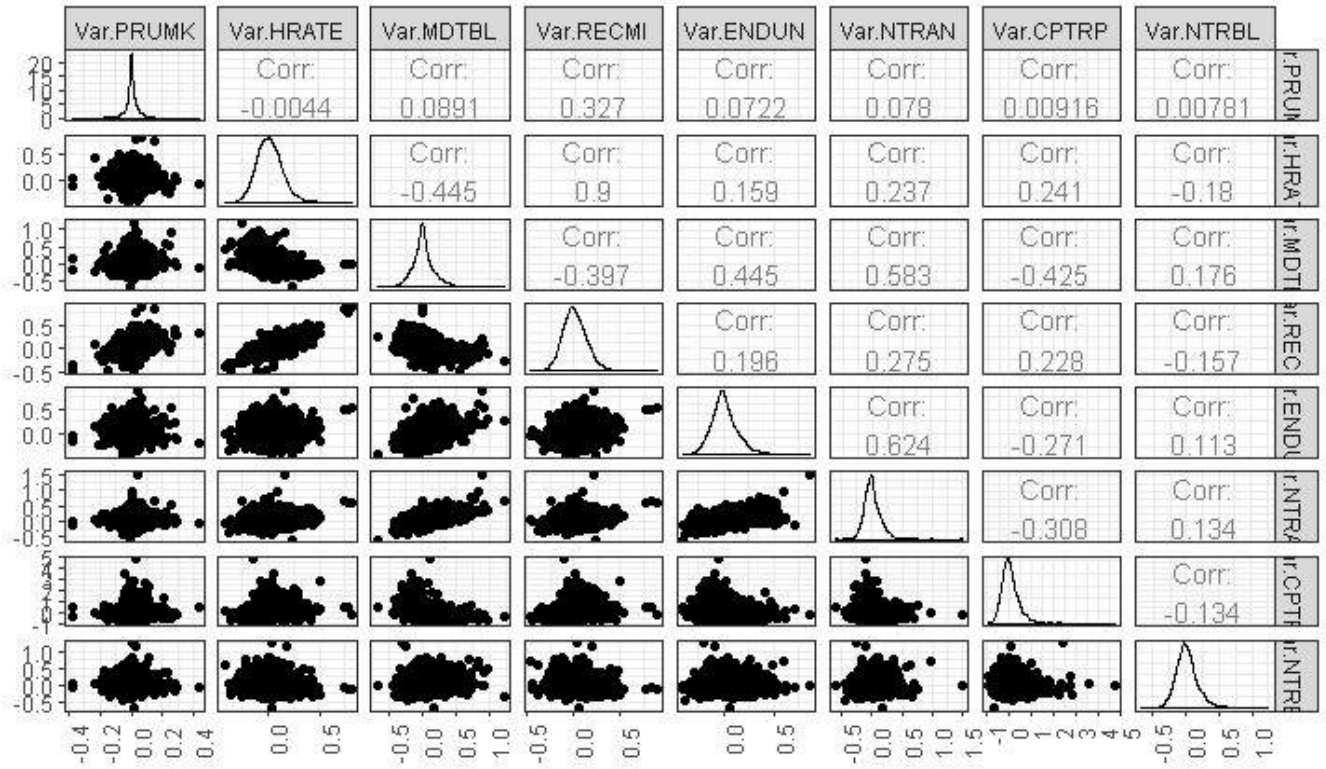
Além disso, Bouoiyour e Selmi (2015), ao encontrarem alguns dados interessantes de regressões, notam que devido ao alto grau de disrupção do segmento e constantes modernizações, a projeção de futuro de maneira sólida do bitcoin, se torna delicada. Para os autores, é uma tecnologia nascente, com uma existência muito curta, sendo extremamente vulnerável as novidades que possam substituí-lo. Ou seja, nada ancora a possibilidade de que, caso haja uma nova moeda, o bitcoin não venha a ser abandonado. Além disso, existe uma intensa busca eufórica sem o devido conhecimento por parte do ativo. Isso quer dizer que "há mais chances de que o Bitcoin entre em colapso e desapareça amanhã, em vez de se tornar repentinamente reconhecido internacionalmente" (BOUOIYOUR E SELMI, p. 469), e que o movimento dos regulares em volta do bitcoin e do ingresso contínuo de investidores inexperientes, possibilita o reforço da evidência de que essa seria uma oportunidade de proteção de curto prazo e investimento de alto risco, do que uma promessa de longo prazo (BOUOIYOUR E SELMI, 2015).

Sendo assim, há uma ambiguidade nas leituras do dados apresentados. Ao mesmo tempo em que é possível que o ativo se torne uma reserva de valor, nada impede que ele seja abandonado. É válido frisar que mesmo que o bitcoin sofra com uma rejeição no futuro, é perfeitamente possível que isso ocorra a partir da sua substituição por outra moeda virtual,

38 Tradução Livre: "Então, o bitcoin é uma promessa de longo prazo? Visto nossas conclusões, é difícil alcançar essa resposta de maneira clara, sólida e inequívoca sobre o fenômeno Bitcoin, uma vez que ele é incerto. Esse dinheiro digital que nasce pode permanecer como pode desaparecer, especialmente quando se considera que o Bitcoin enfrente uma um problema econômico estrutural dada a limitação de suas 21 milhões de unidade em 2140, implicando que não terá aumento da oferta monetária a partir desta data. Até o momento existem mais de 12 milhões de bitcoins em circulação. Se essa famosa criptomoeda despor com sucesso as moedas fiduciárias (euro, dólar e yen) ela exercerá pressões deflacionárias consideráveis. Sem abordar definitivamente as causas, essa moeda virtual parece altamente correlacionada com movimento especulação de investidores e pessoas que detêm ela. Esse dinheiro virtual não é emitido pelo sistema bancário e muito menos por qualquer governo, mas sim por um algoritmo de computador. Lamentavelmente, a maioria dos usuários não tem tanto conhecimento sobre programas matemáticos e, portanto, não sabem até onde que podem ir. Em suma, ninguém pode prever o valor preciso e a forma específica que uma criptomoeda irá tomar, uma vez que seu desenvolvimento tecnológico é altamente imprevisível. A medida que a tecnologia se torna cada vez mais integrada ao nosso cotidiano, criptomoedas obviamente irão continuar a crescer e o bitcoin provavelmente poderá ser deposto por moedas digitais melhores."

anulando as possibilidades do bitcoin, mas mantendo essa função viável para o sistema de moedas eletrônicas como um todo. O fato do bitcoin não estar atrelado a nenhum outro ativo ou instituição que garanta a demanda, é um problema grave para a garantia de valoração do ativo no longo prazo. Também, nenhuma correlação clara da variação do preço é vista nas variáveis diretamente ligadas ao sistema, dificultando sua previsibilidade como reserva de valor - como uma característica intrínseca ao sistema.

Figura II.1: Correlação da variação % das variáveis do Bitcoin.[39]



Fonte: Blockchain em 18/08/2019, Elaboração Própria

Como se pode observar na figura acima, superficialmente não há correlação interna que sustenta a proposta de que um BTC possa assumir ao longo do tempo uma reserva de valor, deixando em aberto essa função, e crendo que apenas teria a espontaneidade dos seus usuários como sustento dessa função. A evolução da aceitação do mercado como um todo pode ser tomada como evidência positiva nesse caso. Porém, como discutido por Bouoiyour e Selmi (2015), há o revés da volatilidade na medida em que o ativo é tomado como reserva de valor,

39 Siglas na imagem: Var.PRUMK: Variação do preço unitário no mercado; Var.HRATE; Variação do Hashrate/Dificuldade; Var.MDTBL: Variação do Tamanho médio do bloco; Var.RECMI: Variação da receita dos mineradores; Var.ENDUN: Variação do número de endereços únicos ativos; Var.NTRAN: Variação do número de transações; Var.CPTRP: Variação do custo percentual por transação; Var.NTRBL: Variação do número de transação por bloco.

fato que pode ser suavizado na medida em que frações das suas unidades se normalizem como uso principal.

Tendo em vista que a decisão de demandar bitcoins é exógena ao sistema, volta-se à discussão dos sistemas de valoração propostos por Woo (2013). Para isso, pode-se ver o bitcoin como um ativo que carrega as mesmas propriedades de uma moeda fiduciária sem curso forçado ou commodity escassa sem utilidade significativa, e que basicamente depende da aceitação da sociedade como um todo, ou seja, uma crença coletiva que leva ao seu uso como reserva de valor. Para avaliar, toma-se qualquer ativo comparável, como ouro ou prata, no caso das commodities, ou o volume convertido em dólares do M2 de países em que se possa supor o bitcoin assumindo o papel de moeda naquela dada economia. Pegando o exemplo do Ouro, o valor total das reservas mundiais de ouro é de aproximadamente 8 trilhões de dólares. Supondo que o bitcoin absorva apenas 5% dessa função de hedge que é ocupada pelo ouro, o valor de cada unidade de BTC seria de aproximadamente 22 mil dólares. É válido ressaltar que essa é apenas uma discussão superficial de valoração e existem literaturas muito extensas a respeito do tema[40].

Além da valoração tomando como referência os preços das commodities, Woo (2013) sugere a avaliação frente ao volume em dólares do M2. A demonstração a seguir será adaptada, já que para ser feita na profundidade adequada seria fundamental debater inúmeros pontos, como as taxas de desconto na valoração para uma dada comparação, já que o bitcoin provavelmente terá uma capacidade técnica mais lenta de atender as negociações, do que uma economia que, além de diversos canais eletrônicos, tem o papel moeda como forma de efetuar pagamentos. Sendo assim, tomando o volume em dólares que compõe o M2 de alguns países, pode-se extrair a tabela a seguir, onde na última coluna será o M2 do país em questão, dividido pela quantidade atual aproximada de bitcoins em circulação, que será arredondado para 18 milhões a fim de simplificar o exercício

Tabela II.1: Comparação de valores de M2 e preços equivalente do BTC em dólar.

País	M2 USD Em Milhões	Preço equivalente do BTC	País	M2 USD Em Milhões	Preço equivalente do BTC
China	$27.196.059,87	$1.510.892,22	Israel	$241.954,34	$13.441,91
Estados Unidos	$14.872.100,00	$826.227,78	Chile	$199.184,51	$11.065,81
Zona do Euro	$13.371.855,23	$742.880,85	Qatar	$153.577,47	$8.532,08

40 Ver BOUOIYOUR E SELMI, 2015

Japão	$9.695.079,93	$538.615,55	Colômbia	$136.885,42	$7.604,75
Alemanha	$3.437.965,40	$190.998,08	Argentina	$37.274,07	$2.070,78
Brasil	$718.627,70	$39.923,76	Bahamas	$6.761,00	$375,61
Portugal	$255.778,19	$14.209,90	Tunísia	$27,17	$1,51

Fonte: Trading Economics[41] em 19/08/2019, Elaboração própria

É válido ressaltar que não há a pretensão de discutir um "valor justo" para o bitcoin nesse trabalho, mas apenas apresentar alguns múltiplos comparáveis para fins de calcular uma possível reserva de valor que o ativo venha assumir.

Portanto, seguindo a tese de Buouiyour e Selmi (2015), pode-se concluir que a possibilidade do bitcoin se tornar uma reserva de valor no longo prazo carece de evidências, deixando em aberto as possibilidades. Dessa maneira, além de não existir nenhuma promessa clara pro longo prazo, o ativo atende muito mais a função de hedge de curto prazo. Isso acaba corroborando com o pensamento de Woo (2014), que indica um grave entrave entre a possibilidade do ativo - ao assumir a função de meio de troca - ser tomado como reserva de valor e acabar trazendo uma grande volatilidade como consequência da sua escassez. Esse processo, potencialmente, condenaria a função de reserva de valor.

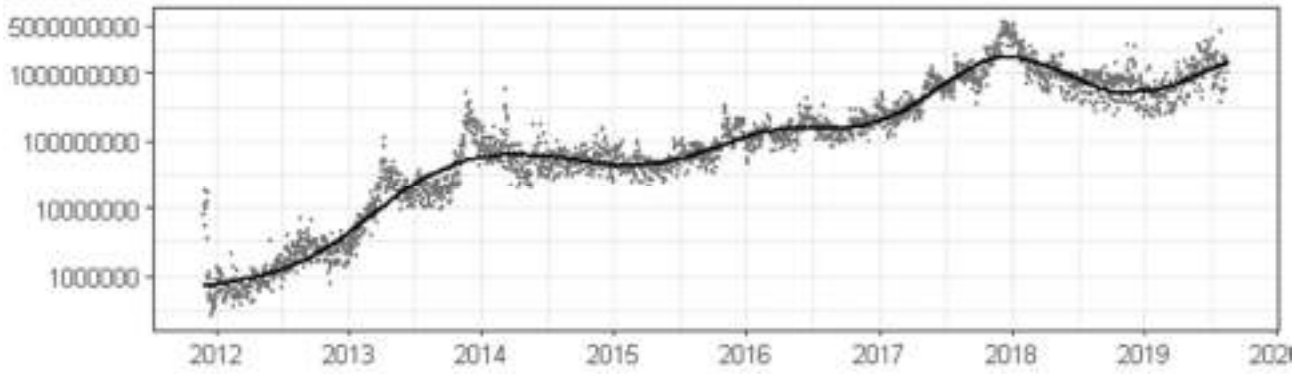
III.2.2 - Meio de troca

A função de meio de troca, é o sinal mais importante do ativo nesse processo de se tornar uma moeda. Nele pode-se captar a percepção de valor que aquele ativo teria para um dado grupo de indivíduos, que ao efetuar negociações, utilizariam aquele bem como referência de pagamento. Esse, inclusive, foi o principal propósito da criação do bitcoin. Nakamoto (2008) deixa claro esse aspecto, ao afirmar que o bitcoin seria um ativo virtual que "permitiria que pagamentos on-line fossem enviados diretamente de uma parte para outra, sem passar por uma instituição financeira" (NAKAMOTO, 2008, p.1). Sendo assim, já que moedas eletrônicas tem, atualmente, estruturas baseadas em uso voluntário - diferente da moeda tradicional que tem curso forçado dentro de um determinado território - surge uma necessidade de atrativos intrínsecos desses ativos, isto é, estruturas e regras técnicas implantadas na estrutura da criptomoeda, já que não teria uma grande instituição garantindo sua validade ou obrigando seu

[41] Ver https://tradingeconomics.com/country-list/money-supply-m2

uso. Para observar melhor, serão discutidas as características do próprio sistema para mensurar uma possível atratividade no longo prazo.

Gráfico II.2 - Volume de transações em dólares. Escala Logarítimica.



Fonte Blockchain em 19/08/2019; Elaboração: Própria

O Crescimento do volume de transações BTC, quando se calcula em dólares, é crescente. Diferente do comportamento que se vê em números absolutos de bitcoins, dada sua natureza escassa, que acaba sendo constante. Tal comportamento crescente seria uma ótima chancela para se concluir uma expansão contínua no número de integrantes e logo consolidando o papel do ativo como meio de troca. O que se destaca como contraponto é o contínuo uso do bitcoin meramente como ativo especulativo[42], tendo menos de 1,5% das suas transações envolvendo o comércio de algum produto ou serviço, e nos últimos 3 anos aproximadamente 90% das transações foram voltadas apenas para especulação ou investimento em corretoras. Para fins de comparação, ao pegar 2% de todas as transações feitas pela rede do BTC, totalizando pouco menos de 9 milhões, e for multiplicado por uma cotação hipotética de 20 mil dólares, resultaria um volume financeiro de 180 bilhões de dólares negociados pelo sistema, muito abaixo do volume diário da Visa de 11 trilhões de dólares[43]. Tal comportamento acaba sendo nocivo, já que atrai cada vez mais volatilidade para o ativo, e consequentemente acaba afastando os comerciantes, que não tiram proveito desse tipo de oscilação em seus planejamentos comerciais[44]. Esse é mais um ponto que corrobora com o argumento de Woo

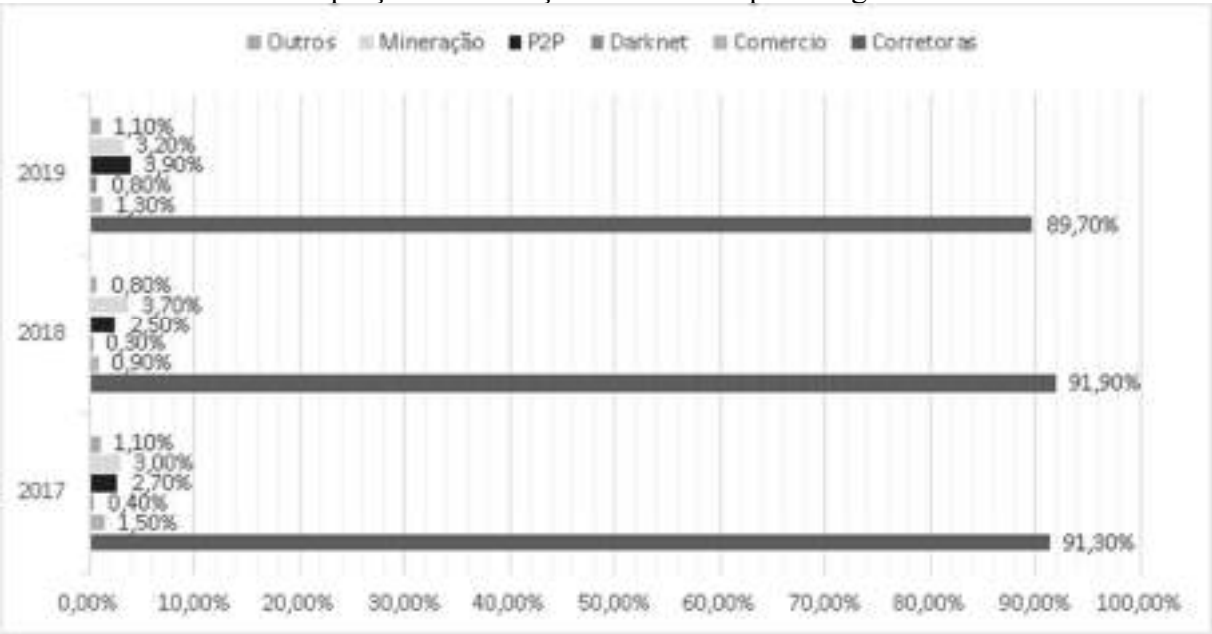
42 Ver https://cointelegraph.com/news/chainalysis-research-speculation-remains-bitcoins-prim

43 Ver https://www.visa.gr/dam/VCOM/download/corporate/media/visanet-technology/aboutvisafactsheet.pdf

44 Ver https://www.bloomberg.com/news/articles/2019-05-31/bitcoin-s-rally-masks-uncomfortable-fact-almost-nobody-uses-it

(2013), onde, ao buscar extrair valor do entesouramento do BTC, aumenta volatilidade do mesmo.

Gráfico II.3 - Proporção de transações em bitcoin por categoria.

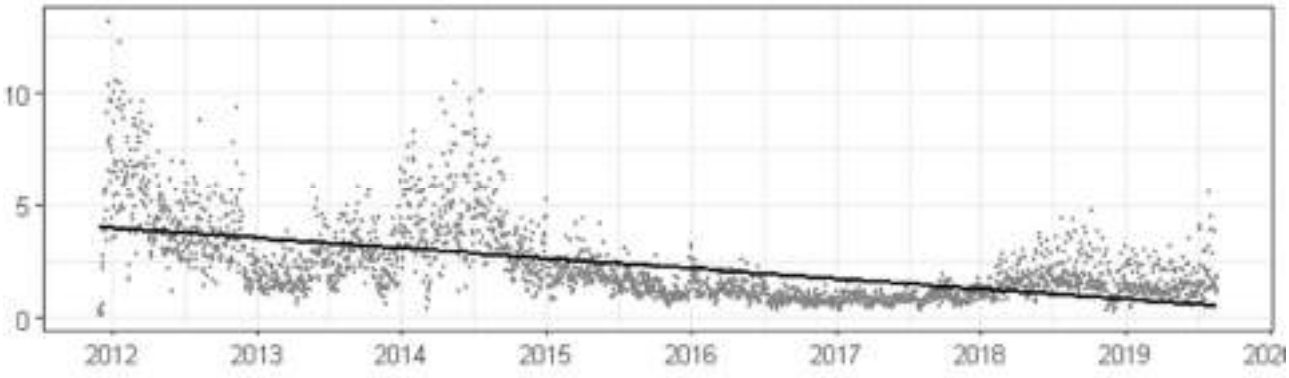


Fonte: https://cointelegraph.com/news/chainalysis-research-speculation-remains-bitcoins-primary-use-case
Acesso 19/08/2019; Elaboração: Própria

Abordando pela ótica dos quesitos técnicos, o Bitcoin se apresenta como uma poderosa alternativa de remessas internacionais (WOO, 2013). Dado seu custo médio abaixo de 2,3% por transação[45], mesmo somado a um custo de intermediação de 1%[46], totalizando aproximadamente 3,3%, acaba sendo extremamente competitivo frente aos demais canais de remessa, que tem um custo médio de 6,84%[47]. Essa característica traz um nicho inteiro que pode impactar de maneira a diminuir os custos de transação de mercado já maduros, como o de remessas internacionais. Uma estratégia factível seria a aproximação desse nicho, como forma de consolidar seu papel como meio de troca, mas a volatilidade citada acaba sendo um risco operacional na consolidação desse tipo de negócio para grandes empresas, dada a escassez e pouca liquidez dos ativos[48]. Mesmo com custos competitivos, esses pontos proporcionariam resistência ao avanço da tecnologia nesse mercado.

45 Média calculada dos dados disponíveis em https://www.blockchain.com/pt/charts/cost-per-transaction-percent
46 Ver https://bitpay.com/
47Ver https://remittanceprices.worldbank.org/sites/default/files/rpw_report_june_2019.pdf
48 Ver https://www.compareremit.com/money-transfer-guide/bitcoin-affect-remittance-industry/

Gráfico II.4 - Custo percentual por transação na rede Bitcoin.



Fonte:Blockchain; Elaboração: Própria

Além dos pontos citados, pode-se discutir o bitcoin como alternativa para bancarização de regiões mais pobres . Apesar da contradição de um sistema tão disruptivo ser um possível meio de solução na expansão da malha de serviços bancários, algumas experiências na Tanzânia, Quênia e Afeganistão têm se mostrado particularmente exitosa, pois permite que populações mais pobres tenham acesso a serviços complexos de maneira muito barata e em escala global (ULRICH, 2014). Isso também é possível por conta da irreversibilidade das negociações, que dão a certeza aos participantes do sistema do recebimento de um pagamento e do seu direito sobre o valor recebido.

A ampliação do número de estabelecimentos que aceitem o bitcoin como forma de pagamento é parte fundamental da estruturação dessa função de maneira sólida a nível global (WOO, 2014). Essa aceitação, hoje, atinge proporções realmente relevantes, mas não diretamente apenas, ou seja, através da aceitação direta de bitcoins como forma de pagamento. Por conta de mecanismos de conversão rápida por meio de corretoras - como o *BitPay*[49] - mercadores e grandes empresas passaram a aceitar pagamento em BTC, só que sem manter o ativo, somente usando-o como canal de pagamentos para o recebimento em moedas comuns, como dólares ou reais.

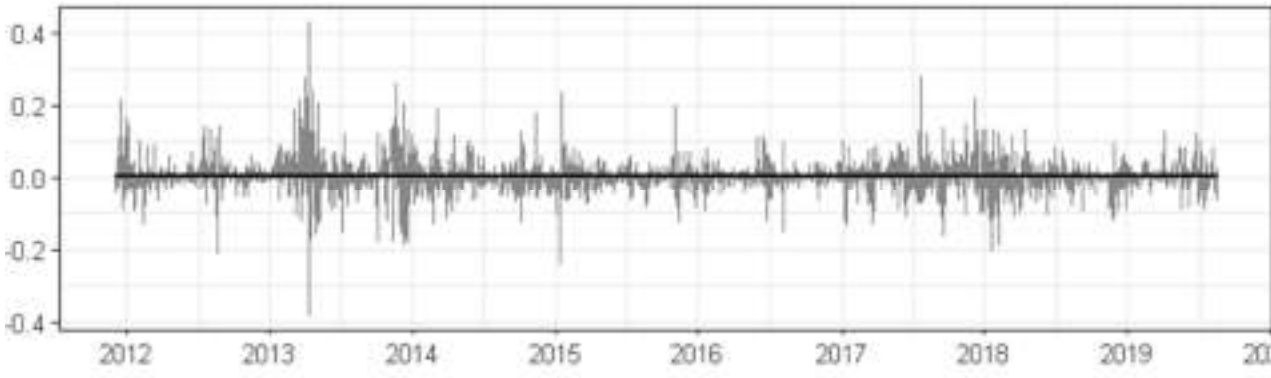
Devido aos dados apresentados, pode-se tomar o bitcoin como, atualmente, um meio de troca, mas com subutilização e muita volatilidade, - aspecto que basicamente condena o próximo passo da função da moeda, que é a possibilidade de ser tomada como unidade de conta.

49 Empresa que se propõe a receber pagamentos em BTC e converter em moeda local. Ver mais em: https://bitpay.com/

III.2.3 - Unidade de conta

Servir como unidade de conta, no caso do BTC, é uma função que apresenta um grande e sólido número de barreiras sistêmicas. Para que um ativo assuma essa função, é fundamental que haja alguma estabilidade da paridade dele frente aos preços de uma economia. Sem isso, é impossível enumerar preços em uma economia dinâmica ou planejar contratos com prazos longos, já que até durante o mesmo dia é possível ocorrer várias cotações com grandes amplitudes para um mesmo produto. Esse fato dificulta o funcionamento da economia e a expõe à riscos cambiais muito altos, o que inviabilizaria a adoção de tal ativo como moeda.

Gráfico II.5 - Variação diária da cotação BTCUSD[50]

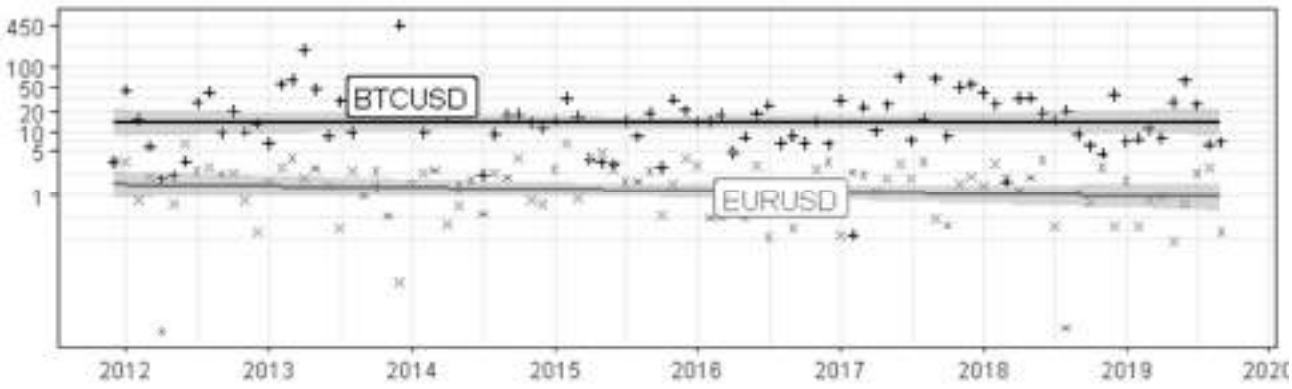


Fonte:Blockchain; Elaboração: Própria

A amplitude da volatilidade do BTC é extremamente elevada, sendo um dos ativo mais voláteis em negociação constante atualmente[51]. Isso se dá, em parte, devido a sua escassez definida matematicamente em uma época de dinamismo muito acelerado. Tal característica leva o ativo a sofrer variações com médias mensais superiores a 25%, basicamente incomparável a volatilidade do par EURUSD[52], com volatilidade média semanal de pouco menos de 1,8%. Esse ponto já demonstra um possível problema, dada a distância que o ativo teria que percorrer para de fato ser considerado uma unidade de conta. Para melhor ilustrar essa amplitude, será feita uma comparação da volatilidade semanal do par BTCUSD frente ao par EURUSD.

Gráfico II.5 - Volatilidade mensal comparada do BTCUSD x EURUSD. Escala Logarítimica

50 Preço da unidade de BTC em dólares
51 Ver https://br.investing.com/tools/forex-volatility-calculator
52 Preço da unidade de EUR em dólares



Fonte:Blockchain; Elaboração: Própria

Nota-se claramente uma disparidade grave entre a volatilidade do BTC frente às moedas tradicionais, representando um grave risco cambial para o portador. Isso impossibilita qualquer tipo de precificação, já usando o BTC como unidade de conta, inclusive para contratos de curto prazo. Potencialmente, seria possível indicar variações severas, além do custo de cardápio[53] constante para que os preços se mantenham atualizados. Apesar disso, é possível afirmar, dado o gráfico exposto, que a tendência de volatilidade está em queda e na medida em que se aproxima da média dos demais ativos (até o máximo de 5% em 60 dias), surge a possibilidade de que em alguns anos o quadro seja mais estável e possa apresentar uma situação diferente (WOO, 2014).

Como já foi falado, a volatilidade que o BTC enfrenta é fruto do desenho da sua arquitetura. Dada a predeterminação da oferta monetária existente no sistema, governada por um algoritmo, isso acaba removendo qualquer medida discricionária possível de contornar esse ciclo. Como observou Woo (2013), o ato de poupar nessa moeda, tende a gerar aumento de volatilidade, já que seu desenho a torna muito escassa, diminuindo ainda mais o espaço amostral em circulação. Da mesma forma que traz volatilidade ao ativo, esse desenho do sistema também acaba impactando em uma tendência deflacionária do ativo. Mesmo em menores níveis de entesouramento, a tendência é que no longo prazo, com o ampliação da adoção e com novos entrantes, o nível da atividade econômica se acelere. Porém, dado a inelasticidade absoluta da oferta monetária, forçaria um ciclo deflacionário sem perspectivas de fim, variando os preços dos bens e serviços da economia e provavelmente afetando negativamente o nível de atividade econômica.

53 Custo referente às alterações dos preços dispostos em um estabelecimento, como anúncios, etiquetas, encartes, etc.

CONCLUSÃO

O objetivo deste trabalho foi analisar o Bitcoin como uma forma viável de dinheiro. Na tentativa de discutir essa questão, buscou-se evidenciar as principais características e funções da moeda e atribuí-las ao bitcoin - utilizando análises empíricas dos dados disponíveis e bibliografia referente ao tema.

Primeiro, foi apresentada a origem da moeda, seu amadurecimento e modernização. Em seguida, foram indicados os precursores, assim como a construção técnica do bitcoin - para isso, foi necessário apresentar as principais características da rede, listar os potenciais e os riscos diante do mal uso dos integrantes da rede. Por último, foi feita uma análise das características desejáveis e das funções clássicas da moeda frente ao bitcoin.

A base teórica e a estrutura criptográfica que sustenta o Bitcoin dá muita segurança ao usuário da posse dos seus BTC, com risco muito baixo de qualquer extravio ou dano. Sua característica de emissão de moedas proporciona ao usuário a segurança de que não ocorrerá um grande derramamento de ativos na rede, impactando diretamente na valoração do ativo. Muito da sua estrutura é aproveitada para diversas outras aplicações, já que, além de um sistema de pagamento, o bitcoin vem com uma poderosa forma de armazenamento, podendo ser utilizada para fazer qualquer registro com bastante facilidade A estrutura do sistema detém uma série de qualidades técnicas que não a deixa imune ao mal uso. Práticas criminosas e lavagem de dinheiro vem sendo cada dia mais comuns e, pela ausência de uma autoridade reguladora, resulta numa grande dificuldade de controle.

A análise das características da moeda mostrou que o bitcoin as cumpre com bastante facilidade, desde que tenha disponibilidade de meios eletrônicos. Essa demanda por telecomunicações e energia, em tese, seria um ponto de extrema fragilidade, mas dado que a maioria absoluta das transações do sistema bancário atual também ocorrem assim, essa fragilidade se torna superável.

Ao se ponderar a respeito da sua viabilidade como meio de troca, foi constatado que é possível que o bitcoin assuma essa função, ou seja, ele tem mecanismos e condições que permitem que essa função seja atendida. Essa oportunidade fica clara principalmente para o mercado de remessas de câmbio, que tem uma diferença bem clara entre o custo das duas operações. O volume de negociações é crescente e bem acelerado, assim como a adesão de novos entrantes na rede. Porém, os usuários que fazem uso dessa função de meio de pagamento acabam sendo uma parcela pequena. A maior parte das transações de BTC são especulativas. O valor do custo percentual das transações é relativamente alto para transações comuns, mas é

menor do que os custos médios de remessas internacionais, sendo que vêm apresentando uma tendência a diminuir ainda mais ao longo do tempo.

A análise da unidade de conta mostrou um grave problema. Quando feita uma análise comparativa, o par BTC/USD apresentou uma volatilidade basicamente 10 vezes maior que o par EUR/USD. Essa diferença impossibilita a medição, mesmo no curto prazo, de preços de uma economia, anulando completamente essa função - dado o cenário atual. Hoje, uma grande parte das empresas que aceitam o BTC como forma de pagamento, fazem isso já executando a conversão instantânea do ativo em moeda local, que calcula o valor em BTC pro cliente, dada uma cotação instantânea da internet. A variedade de cotações também é um desafio para esse ponto.

Quando se observa como reserva de valor, se acaba, apenas, levando pro longo prazo as características da unidade de conta, onde a volatilidade acaba sendo um grave entrave nas projeções. Como forma de traçar cenários, buscou-se mecanismos de valuation do bitcoin para ancorar algumas possibilidades e correlações dentro do sistema que pudessem apontar para algum direcionamento de estabilidade, além de bibliografia direcionada especificamente para esse tema. No entanto, ainda assim, a conclusão foi a negativa dessa função.

Portanto, atualmente, criptomoedas não são uma forma viável de dinheiro. Sua criação veio na direção de ser um meio de pagamento online, diminuindo e barateando os intermediários, trazendo consigo uma inovadora tecnologia de registros, com forte criptografia e segurança, e o fim do gasto duplo. Apesar do grande progresso técnico, o movimento especulativo sofrido pelo bitcoin, o levou a ser o ativo mais volátil já registrado. No momento, não há elementos que apontem para uma mudança de cenário no médio ou longo prazo.

Sendo assim, como sugestão para futuros trabalhos sobre criptomoedas, propõe-se que seja feita uma análise dos fatores que influenciam o aumento da volatilidade, como as mídias sociais, os hedge funds e os movimentos de reguladores.

REFERÊNCIAS BIBLIOGRÁFICA

ANTONOPOULOS, Andreas M. *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*, 2017. Disponível em: <https://bitcoinbook.info/wp-content/translations/pt_BR/book.pdf>. Acesso em: 31/08/2019

BOUOIYOUR, J. e SELMI, R. *What Bitcoin Looks Like?* Annals of Economics and Finance, 16-2, p449-492, 2015. Disponível em: <https://econpapers.repec.org/RePEc:cuf:journl:y:2015:v:16:i:2:bouoiyour>. Acesso 31/08/2019

CARVALHO, F. J. C. de et al. *Economia monetária e financeira: teoria e política*. 2. ed. Rio de Janeiro: Elsevier, 2007.

CHAUM, David. *Blind Signatures for Untraceable Payments,* 1982. Disponível em: <https://nakamotoinstitute.org/static/docs/untraceable-electronic-mail.pdf>. Acesso em: 10/08/2019

DAI, Wei. *b-money*, 1998. Disponível em: <http://www.weidai.com/bmoney.txt>. Acesso em: 10/08/2019

EUROPEAN CENTRAL BANK (ECB). *Virtual Currency Schemes*. Frankfurt, 2012. Disponível em: <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf >. Acesso em: 31 ago. 2019.

FERGUSON, Niall. *A ascensão do dinheiro : a história financeira do mundo*.São Paulo: Editora Planeta do Brasil, 2009.

HAYEK, F.A. *O caminho da servidão*. São Paulo : Instituto Ludwig von Mises Brasil, 2010.

HAYEK, F.A. *Desestatização do Dinheiro*. São Paulo: Instituto Ludwig von Mises Brasil, 2011.

FINNEY, Hal. *Reusable Proofs of Work*, 2004. Disponível em: <https://nakamotoinstitute.org/finney/rpow/index.html>. Acesso em: 10/08/2019.

GREENBERG, Andy. *Nakamoto's Neighbor: My Hunt For Bitcoin's Creator Led To A Paralyzed Crypto Genius*, 2014. Disponível em <https://web.archive.org/web/20140326104029/http://www.forbes.com/sites/andygreenberg/2014/03/25/satoshi-nakamotos-neighbor-the-bitcoin-ghostwriter-who-wasnt/#42e4aeba4a37>. Acesso 21/07/2019

KEYNES, John Maynard. *As Consequências Econômicas da Paz*. Brasília: UnB, 2002.

MENGER, Carl. *Princípios de Economia Política.* São Paulo: Nova Cultural (Col. Os Economistas), 1985

MISES, Ludwig von. *A verdade sobre a inflação.* Instituto Ludwig von Mises Brasil, 27 mai. 2008. Disponível em: < http://mises.org.br/Article.aspx?id=101 >. Acesso em: 02 mai. 2017.

NAKAMOTO, Satoshi. *Bitcoin: a Peer-to-Peer Electronic Cash System,* 2008. Disponível em: <http://article.gmane.org/gmane.comp.encryption.general/12588/ >. Acesso em: 02 mai. 2017

NAKAMOTO, Satoshi. *Bitcoin open source implementation of P2P currency,* 2009 <http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source?id=2003008:Topic:9402 >. Acesso em: 21 jul. 2019.

NAKAMOTO, Satoshi. *Duality*, 2018 Disponível em: <https://drive.google.com/file/d/13mF6RreQ-e2ahOIUmVKdX_WjYMlBHUbI/view?usp=sharing >. Acesso em 10/08/2019

SZABO, Nick. *Bit gold,* 2005. Disponível em: <http://unenumerated.blogspot.com/2005/12/bit-gold.html>. Acesso 21/07/2019

TRACHSLER, Tracy. *Short history of Bitcoin rises and crashers*, 2019. Disponível em: <https://cryptoheroes.ch/short-history-of-bitcoin-rises-and-crashes/>. Acesso em: 11/08/2019

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

WOO, David et al. *Bitcoin: a first assessment*. FX and Rates | Global, 2013.

WRAY, L. Randall. *Trabalho e moeda hoje: a chave para o pleno emprego e a estabilidade dos preços.* Rio de Janeiro: UFRJ / Contraponto Editora,p. 37-58, 2003.