

UNIVERSIDADE FEDERAL FLUMINENSE - ESR
DEPARTAMENTO DE CIÊNCIAS ECONÔMICAS DE CAMPOS

NATHUR CARDOSO DE MIRANDA

BITCOIN: UMA ANÁLISE TEÓRICA SOBRE A CRIPTOMOEDA

CAMPOS DOS GOYTACAZES

2018

NATHUR CARDOSO DE MIRANDA

BITCOIN: UMA ANÁLISE TEÓRICA SOBRE A CRIPTOMOEDA

Trabalho de Conclusão submetido ao Curso de Graduação em Ciências Econômicas do Polo Universitário de Campos dos Goytacazes da Universidade Federal Fluminense como requisito parcial para a obtenção do título de Bacharel em Ciências Econômicas.

Orientador: Adriano Vilela Sampaio

CAMPOS DOS GOYTACAZES

2018

Ficha catalográfica automática - SDC/BUCG
Gerada com informações fornecidas pelo autor

M672b Miranda, Nathur Cardoso de
Bitcoin : uma análise teórica sobre a criptomoeda / Nathur
Cardoso de Miranda ; Adriano Vilela Sampaio, orientador ;
Sampaio Adriano Vilela, coorientador. Campos dos Goytacazes,
2018.
49 f.

Trabalho de Conclusão de Curso (Graduação em Ciências
Econômicas)-Universidade Federal Fluminense, Instituto de
Ciências da Sociedade e Desenvolvimento Regional, Campos dos
Goytacazes, 2018.

1. Bitcoin. 2. Moeda. 3. Valor. 4. Produção intelectual.
I. Sampaio, Adriano Vilela, orientador. II. Adriano Vilela,
Sampaio, coorientador. III. Universidade Federal Fluminense.
Instituto de Ciências da Sociedade e Desenvolvimento
Regional. IV. Título.

CDD -

NATHUR CARDOSO DE MIRANDA

Banca Examinadora:

Adriano Vilela Sampaio

Orientador

Maracajaro Mansor Silveira

Membro da Banca

Vanuza da Silva Pereira Ney

Membro da Banca

Sumário

Introdução	7
1. A moeda, suas funções e características e o conceito de dinheiro	11
1.1. As funções e características presentes nas moedas	11
1.2. Breve história do dinheiro	13
1.3. Moedas Paralelas.....	20
1.4. Moedas Virtuais	22
1.5. Criptomoedas e os Cypherpunks.....	23
1.6. A moeda enquanto fato social	25
2. A Bitcoin	31
2.1. Funcionamento	31
2.2. A Mineração e a emissão de Bitcoins	32
2.3. Os casos da Mt.Gox e da Silk Road	34
2.4. A caracterização da Bitcoin como moeda	36
2.5. As heranças da Bitcoin: a Blockchain e as altcoins	43
Conclusão.....	44

Índice de Figuras

Figura 1 - Difusão dos Sistemas RTGS.....	19
Figura 2 – Dificuldade de Mineração.....	33
Figura 3 – Hash Rate.....	33
Figura 4 – Rede de Aceitação de Bitcoins como meio de pagamento.....	37
Figura 5 – Volume diário estimado de transações (em BTC).....	38
Figura 6 – Volume diário estimado de transações (Equivalente em US\$).....	39
Figura 7 – Preço da Bitcoin em US\$ nos últimos dois anos.....	39
Figura 8 – Índice Nikkei entre 1980 e 1992.....	40
Figura 9 – Tempo médio de confirmação de uma transação em Bitcoin.....	41
Figura 10 – Transações aguardando confirmação na rede (Mempool size).....	42

Resumo

O fato de ser uma moeda com a sua validade determinada apenas pelos usuários é constantemente citado como diferencial da Bitcoin, entretanto, o conceito e a utilização de moedas com o seu valor determinado apenas pela confiança está bastante presente na história monetária mundial. O presente trabalho tem como objetivo apresentar uma discussão acerca dos motivos pelos quais as moedas possuem valor e como estes valores foram interpretados com o passar do tempo para entender se a Bitcoin pode ser caracterizada como uma moeda. Também buscamos entender se a Bitcoin é o final de uma evolução das relações monetárias ou se é apenas mais um episódio de uma evolução que está sendo construída. Para alcançarmos tais objetivos, recorreremos a diferentes teorias sobre o valor da moeda e a revisão histórica do papel da moeda na sociedade com a intenção de entender como o valor da moeda é reconhecido e garantido. O resultado disso foi a conclusão de que o valor da moeda é garantido muito mais pela confiança da sociedade do que pela garantia do governo e que, portanto, uma moeda totalmente desregulada e baseada na fé das pessoas seria plausível se esta passasse a ser aceita.

Palavras-chave: Bitcoin, moeda, valor.

Resumo

The fact that it is a currency with its validity determined only by the users is constantly cited as a differential of Bitcoin, however, the concept and use of coins with their value determined only by trust is very present in world monetary history. The present work aims to present a discussion about the reasons why coins have value and how these values have been interpreted over time to understand if Bitcoin can be characterized as a coin. We also seek to understand whether Bitcoin is the end of an evolution of monetary relations or if it is just another episode of an evolution being constructed. To achieve these objectives, we have used different theories about the value of money and the historical review of the role of money in society with the intention of understanding how the value of money is recognized and guaranteed. The result of this was the conclusion that the value of money is guaranteed much more by the confidence of society than by the guarantee of the government, and that therefore a totally deregulated currency based on people's faith would be plausible if it were to be accepted.

Keywords: Bitcoin, currency

Introdução

A Bitcoin, primeira criptomoeda do mundo, é parte de uma história que começou a ser escrita na possibilidade do acesso a internet, no início da década de 1990, com o surgimento do movimento de ações independentes de pensadores conhecidos como *cypherpunks* e, portanto, é importante entender que a Bitcoin não é o desfecho da história ou uma revolução que surgiu do nada, mas que é um capítulo de uma evolução que continua acontecendo. Esta evolução é possível devido a crescente evolução tecnológica digital que presenciamos desde o surgimento da *world wide web*. A Bitcoin traz consigo uma grande contribuição para a continuação desta evolução como, por exemplo, a metodologia da Blockchain e o aprimoramento dos protocolos de validação por chave dupla utilizados atualmente em diversos setores da economia mundial.

Desde o seu surgimento, em 2008, a Bitcoin (BTC) tem se tornado conhecida como uma alternativa ao sistema bancário para a efetivação de transações financeiras por ser uma moeda que utiliza apenas o sistema *peer-to-peer*, ou seja, sem intermediários. Além disso, a criptomoeda é considerada não confiável devido ao fato de todas as suas transações serem criptografadas, ou seja, por utilizar a tecnologia para preservar a privacidade dos envolvidos nas transações ocultando as suas identidades. Apesar disso, a Bitcoin movimentou o total de US\$188,6 trilhões em 2017 e 170,6 trilhões de dólares entre janeiro e outubro de 2018, segundo dados da Blockchain.com¹, uma administradora de carteiras de Bitcoins. Segundo o Google Trends², “Bitcoin” foi o termo mais popular nas buscas no site durante a penúltima semana de 2017 em todo o mundo e atualmente tem 10% de popularidade no site, também ao redor do mundo. Segundo dados do Coinmap³, o número de estabelecimentos que aceitam o Bitcoin como forma de pagamento aumentou em 3.159 em 2017 e em 2.318 entre janeiro e outubro de 2018, totalizando 13.777 estabelecimentos ao redor do mundo atualmente, incluindo estabelecimentos espalhados por todos os estados brasileiros.

A Bitcoin ainda trouxe consigo uma série de avanços tecnológicos como a Blockchain e provocou outras evoluções, como os processadores ASIC’s (sigla para Application

¹ Acesso em 11/12/2018.

² Disponível em <https://trends.google.com.br/trends/explore?q=bitcoin&geo=BR>. Acesso em 11/12/2018.

³ Disponível em <https://coinmap.org>. Acesso em 11/12/2018.

Specific Integrated Circuits) desenvolvidos para o uso específico em *mining pools* e que atualmente podem ter diversas aplicações no mercado.

Ou seja, os dados sobre a criptomoeda mostram valores que não podem ser ignorados. Tais dados comprovam a existência de uma economia mundial que existe através do Bitcoin e sua rede.

Entretanto, é necessário entender se a suposta revolução trazida pela Bitcoin e pelas criptomoedas pode ser um indício das novas formas de transações financeiras que experimentaremos em um futuro que parece estar cada vez mais próximo. Considerando que a Bitcoin é interpretada globalmente como uma moeda, sendo aceita como meio de pagamento em estabelecimentos comerciais, e ao mesmo tempo se comportando como um ativo, como mostra a flutuação do seu câmbio em relação ao dólar, é necessário entender se podemos considerá-la uma moeda ou se ela é apenas uma nova forma de ativo com uma liquidez muito alta.

E para isto, este trabalho propõe uma breve revisão sobre o que compôs o valor das moedas utilizadas em diferentes civilizações ao longo da história para entender como esta aceitação foi criada e aplicar estas informações em uma análise sobre a Bitcoin com o intuito de entender o seu potencial como nova forma de pagamento. Em resumo, este trabalho busca responder se com base nos principais exemplos de moedas ao redor do mundo, em teorias sobre o seus surgimentos e na análise dos dados sobre a movimentação global da rede Bitcoin, é possível caracterizar a Bitcoin como uma moeda e qual é o legado deixado pelos avanços trazidos com e pela criptomoeda em questão.

Acredita-se que ao final do trabalho será possível entender que, apesar de conseguir cumprir as funções de uma moeda, alguns fatores dificultam a utilização da Bitcoin como substituta ao dinheiro, mas que existirão novas criptomoedas capazes de corrigir estas dificuldades. Além disso, acredita-se que será possível verificar que o surgimento da Bitcoin impactou não apenas o mercado financeiro, com o desenvolvimento tecnológico global.

Este estudo está organizado em duas partes, sendo a primeira dedicada ao levantamento de informações sobre o valor da moeda desde o seu surgimento e ao debate sobre qual seria a origem dos valores de tais moedas. A segunda parte é dedicada a apresentação do Bitcoin, trazendo informações sobre o seu surgimento, funcionamento, um breve

histórico das questões mais recorrentes, a caracterização da Bitcoin enquanto moeda e o legado deixado.

1. A moeda, suas funções e características e o conceito de dinheiro

1.1. As funções e características presentes nas moedas

Ao longo da história as trocas de mercadorias sempre fizeram parte da construção de qualquer sociedade ao redor do mundo. As trocas possibilitavam o acesso a mercadorias sem que fosse necessário produzi-las aumentando significativamente o total de mercadorias que poderiam ser acessadas.

Os estudos numismáticos e econômicos demonstram uma infinidade de exemplos de sociedades, desde as mais primitivas às mais organizadas, que utilizavam formas de intermediar e facilitar as trocas de mercadorias. Parte destas formas se deu de forma centralizada e controlada por alguma organização política governante, enquanto outras se apresentaram de formas mais orgânicas, acordadas entre os integrantes das populações. Sejam quais forem as formas de organizar as trocas, convencionou-se a utilização da denominação *moeda* para algo que é utilizado como entreposto das transações provenientes destas trocas.

O nome moeda decorre do antigo Império Romano e sua cultura politeísta, como conta Weatherford (2005). A deusa Juno Moneta, divindade a qual é atribuída a proteção das mulheres e das famílias também é, segundo historiadores, considerada protetora do Estado Romano. Em seu templo eram cunhados os denários, a primeira emissão de dinheiro da qual se tem conhecimento, que eram marcadas com o rosto da deusa e seu nome completo, fazendo com que o seu sobrenome se popularizasse como nome do objeto (WEATHERFORD, 2005). O termo dinheiro será utilizado neste trabalho como a denominação de uma forma de moeda que tem a sua emissão realizada e controlada por um governo.

Antes de avaliarmos o processo histórico dos surgimentos das moedas, precisamos elucidar no que consiste o conceito de moeda. Uma moeda é um objeto capaz de cumprir funções específicas durante transações comerciais e que possui determinadas características físicas e econômicas contidas em si que garantem a este objeto a capacidade de cumprir estas funções. O fato de este objeto, doravante moeda, perder a capacidade de efetuar uma de suas funções durante um período crítico pode não ser suficiente para retirar dele o poder de ser moeda, ou seja, uma moeda pode perder a

capacidade de executar uma de suas funções por um período e continuar sendo utilizado como moeda, obviamente com restrições e com dificuldades. Este tema será esclarecido durante o texto.

A função de intermediária de trocas é a mais destacada dentre as funções da moeda, porém, se adicionarmos a esta ocasião da troca o fato de que a moeda permite realizar barganhas de mercadorias por dinheiro e de dinheiro por mercadoria, a moeda passa a ser mais do que um intermediário de troca e passa a ser um meio de pagamento. Ou seja, ao trocar uma mercadoria por moeda, o vendedor desta primeira troca pode utilizar esta moeda que recebeu para comprar outras mercadorias em outro momento (CARVALHO, 2007). O efeito temporal adicionado a esta situação provoca outra reflexão acerca das funções inerentes a moeda. Se é possível trocar mercadorias por moeda em um momento e trocar estas moedas por mercadoria novamente em qualquer momento no futuro, a moeda deve carregar consigo a garantia de que valerá algo no futuro. Se isto não se cumprir, a moeda voltará apenas a ser um facilitador de trocas de mercadorias que devem ocorrer em um curto período de tempo. Sendo assim, uma moeda contém em si, além da função de meio de pagamento, a função de reserva de valor. Nas palavras de Carvalho (2007, p. 3), “No momento em que um agente econômico recebe recursos na forma monetária, ele ganha o direito de reter poder de compra, em tese, indefinidamente sem temer perdas”. Ainda sobre a função de reserva de valor, Carvalho (ibid) destaca que “em uma economia em estado hiperinflacionário, a moeda perde esta função de reserva de valor. Reter moeda nessa economia seria uma atitude custosa ao agente detentor, pois a moeda perderia poder de compra ao longo do tempo”, ao que é possível acrescentar que nesta situação de estado hiperinflacionário, o que se perde é o poder de compra pois, uma vez que uma moeda possui a sua aceitação garantida, ela terá o seu valor. Apenas para deixar o texto claro para qualquer leitor, podemos elucidar o poder de compra como o quanto se pode comprar com uma determinada quantidade de moeda. A função de reserva de valor é possível apenas porque, uma vez que as populações envolvidas em transações monetárias aceitam que o objeto que elas utilizam possui a importância de moeda, tais populações passam a calcular o valor das suas mercadorias em valores monetários, ou seja, a moeda possui ainda uma outra função que garante exequibilidade das funções supracitadas. É importante ressaltar que não se pretende discutir as variações de preços das mercadorias nem as pautas sobre o que de fato dá valor a uma mercadoria neste momento, mas

apenas elucidar que ao determinar os valores de troca das mercadorias em termos monetários, as populações que aceitam a utilização de um determinado objeto ou conjunto de objetos como moeda provam a existência nestas moedas da função de unidade de conta. Harari (2015) exemplifica muito bem a eficiência desta característica ao propor uma situação onde

um sapateiro, em uma economia monetária, precisa saber apenas o preço cobrado por diversos tipos de sapatos – não há necessidade de memorizar as taxas de câmbio entre sapatos e maçãs ou cabras. O dinheiro também livra os produtores de maçãs da obrigação de procurar sapateiros ávidos pela fruta, porque todos sempre querem dinheiro. (HARARI, 2015, p. 187)

As moedas devem, portanto, possuir características físicas e econômicas que facilitem a manutenção dos seus valores intrínsecos e da capacidade de executar as suas funções. Um objeto utilizado como moeda deve ser transportável para garantir que as transações realizadas com ele possam se concretizar, caso contrário, este objeto é apenas uma mercadoria. A moeda deve ser difícil de falsificar e deve haver alguma forma de confirmar a sua autenticidade como o caso supracitado do primeiro dinheiro a ser emitido, o denário, emitido pelo Império Romano a partir de 269 a.C. e que contava com o rosto da deusa Juno, para garantir a sua autenticidade. Outro exemplo que pode ser utilizado para ilustrar as tentativas de falsificação é o dos astecas que tentavam falsificar sementes de cacau, utilizado como moeda, colocando lama dentro da casca de cacau e misturando ao montante de grãos durante os pagamentos das transações (WEATHERFORD, 2005). Uma moeda deve ainda ser durável para que possa cumprir a função de reserva de valor e a função de unidade de conta pode ser garantida pela característica física divisível do objeto adotado como moeda para que transações de valores fracionados sejam realizadas sem valores adicionais. Para garantir o poder de compra de uma moeda, é importante ainda que o custo de estocagem e o custo de transação sejam aproximadamente nulos (CARVALHO, 2007). O custo de transação da moeda próximo a zero não diz respeito a custos de transações bancárias, que são os exemplos mais comuns. Os custos de transações bancárias são tarifas cobradas pelos bancos para efetuar o serviço de transação.

1.2. Breve história do dinheiro

As moedas possuíram diversos formatos, de acordo com cada sociedade e cada época, antes de tomar as formas como são conhecidas atualmente. Segundo Weatherford

(2005), as sociedades astecas que viveram na América Central entre os séculos XIII e XVI utilizavam grãos de cacau como moeda, os guatemaltecos utilizavam milho, enquanto os povos babilônicos e assírios utilizavam cevada. Povos das Filipinas, Japão e Birmânia utilizavam porções de arroz como intermediário de trocas. Alguns povos do Mediterrâneo e da região do Saara utilizavam até mesmo porções e lajes de sal. Temos ainda outros exemplos de commodities sendo utilizados como mercadoria como,

conchas de cauri foram usadas como dinheiro por cerca de 4 mil anos em toda a África, sul da Ásia, leste da Ásia e Oceania. No início do século XX, ainda se podiam pagar impostos em conchas de cauri na Uganda britânica. (HARARI, 2015, p. 186)

Objetos adotados como moedas que podem ser consumidos ou utilizados para outros fins além das transações monetárias como os exemplos citados acima são chamados de moedas-mercadoria ou moedas-*commodity*. Este tipo de moeda se caracteriza por não ter garantida a função de reserva de valor, uma vez que commodities, em geral, podem ser perecíveis. Este foi um dos principais motivos para o fim da utilização deste tipo de moeda.

Os artigos de consumo como tabaco e chocolate serviram como meio adequado de troca, mas não podiam cumprir todas as funções do dinheiro. Por exemplo, eles são pouco capazes de acúmulo de valor. Qualquer pessoa que tenha tido que acumular sacos de grãos ou uma carga de tabaco como forma de acúmulo de riqueza logo veio a descobrir que os grãos apodreciam ou eram atacados por insetos e ratos, e o tabaco logo perdia seu sabor e começava a se despedaçar. Para acumular riqueza para uso futuro, as pessoas precisam de itens mais duráveis como tecido, peles, plumas, dentes de baleia, dentes de javali ou conchas. Essas commodities duram mais do que alimentos, entretanto também deterioram e perdem o valor. Itens alimentícios podem funcionar adequadamente para troca de produtos, mas não são bons para acúmulo de valor. (WEATHERFORD, 2005, p. 27 e 28).

Alguns itens como as conchas de cauri citadas por Harari podem ter maior durabilidade mas, por surgirem naturalmente, estão propensas a aparecer de formas, texturas, pesos e tamanhos diferentes, fazendo-se perder a função de unidade de conta. A aceitação destas moedas é, de forma geral, acordada em regiões pequenas, devido as dificuldade de transportes destas sem perder a qualidade. Moedas-mercadoria aparecem ao longo da história principalmente em sociedades sem muito desenvolvimento tecnológico ou em situações extremas como o exemplo ocorrido na Romênia, durante o duro regime ditatorial de Nicolae Ceausescu, onde cigarros eram utilizados como moeda paralela diante da desvalorização do dinheiro do país (WEATHERFORD, 2005).

Apesar de também serem considerados commodities, os metais aparecem separados aqui neste texto porque as moedas metálicas trouxeram consigo, além da durabilidade e outros avanços, a principal forma de moedas que conhecemos até hoje: o dinheiro.

O início da utilização de moedas metálicas remete a 2.500 a.C., com os shekels, moedas de ouro e prata utilizados na Mesopotâmia. Ouro e prata são utilizados desde estes tempos primórdios por serem materiais raros e capazes de guardar as suas características, como peso e aparência, sem muita dificuldade. Mas estas sociedades primórdias não dominavam uma tecnologia de cunhagem eficaz o suficiente para que estas moedas fossem utilizadas em grande escala (WEATHERFORD, 2005). Este processo de massificação da utilização das moedas metálicas começa a partir de 640 a.C. com as moedas criadas na Lídia, hoje parte da atual Turquia, pelo rei Aliates. Estas moedas eram emitidas por diferentes autoridades que garantiam a autenticidade e o padrão das moedas (HARARI, 2015). As moedas lídias eram feitas de uma liga de ouro e prata e separadas em lingotes bastante pequenos, reduzindo o seu valor e facilitando a efetivação de pequenas transações monetárias cotidianas (WEATHERFORD, 2005). Muito do que conhecemos hoje sobre políticas monetárias surgiu neste período como, por exemplo, a redução da quantidade de prata na constituição dos denários que ocorreu entre 64 d.C e 268 d.C. que resultou em uma desvalorização gradual da moeda percebida pela população que aumentou os preços proporcionalmente (*ibid*).

Este exemplo de alteração da constituição da moeda mostra claramente que a partir do momento em que os Estados se tornam responsáveis pela emissão e/ou garantia de autenticidade das moedas, o valor destas passa a não depender mais do seu peso ou da sua constituição, mas da sua validade e da da garantia dessa validade pelo Estado (METRI, 2007). O exemplo da alteração da constituição das moedas de prata do Império Romano deixa claro que o valor de moeda do objeto não está ligado a sua constituição ou a um material específico, mas a validade daquele objeto enquanto moeda, a garantia desta validade e a aceitação da população daquele objeto como moeda (KNAPP, 1924) e esta característica do sistema monetário possibilitou o surgimento de dois dos maiores fenômenos da economia global: o papel-moeda e o crédito.

As diferentes formas de empréstimos parecem estar presentes nas diferentes economias desde sempre, mas foi entre os séculos XII e XIV que eles ganharam a primeira forma institucionalizada. A Ordem Militar dos Cavaleiros do Templo de Salomão, conhecida como Ordem Templária surgiu em Jerusalém no século XII fundada por cavaleiros

atuantes nas Cruzadas, missões de conquista da Igreja Católica. Os castelos dos Templários foram a primeira forma institucional conhecida onde era possível depositar uma quantia em um local e sacar em outro, através de um recibo escrito.

Pelo fato de os Templários serem donos dos castelos mais fortes do mundo e por constituírem uma das forças de combate mais ameaçadoras da época, seus castelos serviam como locais ideais para depositar dinheiro e outros artigos de valor. (WEATHERFORD, 2005, p.71)

Este modelo serviu de base para o sistema de bancos familiares privados italianos que popularizaram a utilização do papel-moeda. ⁴O papel-moeda surge quando os comprovantes de depósitos e de empréstimos, em forma de papel, começam a se popularizar. Os bancos⁵ passam então a lidar mais com os pedaços de papel do que com as moedas de ouro e prata. (WEATHERFORD, *ibid*).

Segundo Carvalho (2007), o volume de notas emitidas principalmente pelos bancos começou a competir com a quantidade de moedas metálicas, enquanto meios de troca, limitando a oferta de moeda. A solução deste problema começou em 1797 quando o Banco da Inglaterra suspendeu os pagamentos em metal e passou a desconsiderar vínculo entre as notas de papel e as moedas metálicas. Tal decisão levou a uma série de debates acerca do tema que culminaram no formato do padrão-ouro em 1844. Os defensores desta ideia diziam que o volume excessivo de notas bancárias emitidas pelo Banco da Inglaterra gerava uma desvalorização da moeda e que para solucionar este problema, deveria ser imposta uma restrição da emissão de notas de acordo com o volume de ouro que se havia em reserva. A Lei Bancária inglesa de 1844 separou o Banco da Inglaterra em dois setores com atuações diferentes, sendo o primeiro o banco comercial e o segundo um Departamento de Emissão com o volume emitido lastreado em ouro, conforme as teorias defendidas pelo padrão-ouro.

Em 1863, Nova York substituiu Londres como principal centro financeiro mundial e, seguindo o mesmo caminho do Banco da Inglaterra, o governo dos Estados Unidos promulgou o National Bank Act que estabelecia uma moeda realmente emitida e controlada pelo governo através da tributação da emissão de novas notas pelos bancos. Os Estado Unidos passaram por um período de emissão abundante de moedas, causando

⁵ O termo “banco” deriva do local onde eram realizados os contratos de empréstimo, chamadas “bancas”, e se espalhou por todo o mundo através da expansão destas instituições, gerando as variações linguísticas do termo como bank e banque.

diversas desvalorizações até o ano de 1900 quando o padrão-ouro foi adotado pelo Congresso estadunidense (WEATHERFORD, 2005).

A limitação da emissão de moedas com base na reserva de ouro foi um dos principais fatores para a garantia do equilíbrio da economia mundial durante o século XIX e alcançou o seu colapso em 1931 quando a Grã-Bretanha deixou de vincular a quantidade de moedas em circulação com a quantidade de ouro em reserva (GUTTMANN, 1996). Em 1933, o então presidente dos Estados Unidos, Franklin Delano Roosevelt, apresentou o plano econômico chamado de New Deal que introduziu um modelo monetário mais flexível com base na moeda-creditícia, ou seja, parte dos depósitos em papel-moeda nos bancos estadunidenses eram reservadas para ficarem disponíveis aos saques e o restante poderia ser colocado em circulação através de operações de crédito (ibid). Esta estrutura apresentava uma forma mais flexível de emissão de moeda e que poderia reagir aos choques de demanda e oferta com maior velocidade. Além disso, este momento na história marca a transição da era da influência das commodities no mercado monetário mundial para a o período de regulação total das economias pelos governos, principalmente através dos seus Bancos Centrais.

Em 1944 foi assinado por 44 nações o Acordo de Bretton Woods que alterou o funcionamento da emissão de moedas ao redor do mundo. A maioria das moedas do mundo ficaram submetidas a taxas cambiais em relação ao dólar determinadas durante as reuniões do acordo (WEATHERFORD, 2005). Ficou estipulado que o governo estadunidense ficaria responsável por manter o preço de 35 dólares por onça de ouro, mas, no entanto, este preço foi praticado apenas até a década de 60, aproximadamente 20 anos depois do acordo. O valor financeiro das moedas então estava atrelado ao dólar que, por sua vez, era controlado para ter seu preço equiparado a uma quantidade fixa de ouro. Ao trabalhar desta forma, as economias se desprenderam do modelo de emissão de moeda baseado na quantidade de ouro em reserva e passava a estipular o valor da financeiro das suas moedas com base no câmbio internacional. Por mais que o valor do câmbio em relação ao dólar fosse controlado com o intuito de se equiparar a uma determinada unidade de ouro, estamos falando sobre o preço da unidade de ouro e não mais sobre a sua quantidade.

O período compreendido entre o final da década de 1960 e o início da década de 1970 marcou o fim da relação do ouro com a quantidade de moedas em circulação ao redor do mundo. O governo americano se mostrava cada vez menos disposto a abrir mão da

autonomia da sua administração em prol do equilíbrio econômico internacional (CARVALHO, 2007). Em agosto de 1971, o então presidente estadunidense Richard Nixon suspendeu a garantia da conversão de dólar em ouro (GUTTMANN, 1996), fazendo com que

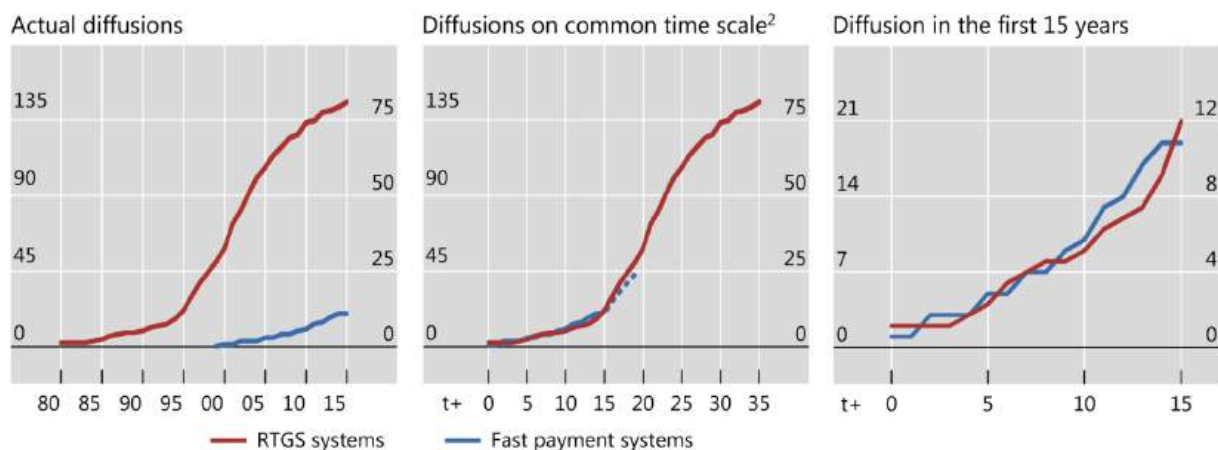
entre os mandatos de Franklin Roosevelt em 1933 e as ações de Richard Nixon em 1971, os Estados Unidos foram de um dólar baseado em metal precioso a um baseado exclusivamente na regulamentação do governo. O dólar americano de hoje é meramente dinheiro por reconhecimento, sustentado pela ordem do governo e pela fé do povo nessa ordem e nada mais. (WEATHERFORD, *ibid*, p.187).

Entre 1971 e 1973 a definição do valor da moeda passou de um modelo onde o dólar deixou de ser ancorado no ouro e passou para o modelo das relações monetárias internacionais com moedas creditícias e flutuação cambial preponderantemente influenciada por políticas monetárias (CARVALHO, 2007).

A partir deste momento o dinheiro passou a ter o seu valor totalmente derivado da confiança das populações e o seu preço definido pelo valor cambial em relação a dinheiros de outras regiões ou nações. O dinheiro, como foi dito, é a forma de moeda cuja emissão é de controle do governo. É através desta emissão que o governo consegue influenciar a economia do seu país. A discussão acerca da crença das populações no valor do dinheiro e das demais moedas serão abordados no último tópico deste capítulo. Por ora, devemos nos ater apenas ao formato da moeda que alcançou na década de 70 a base do formato de moeda mais utilizado atualmente em todo o mundo.

A década de 1980 foi a época do surgimento de um importante capítulo da história do dinheiro: a digitalização dos meios de pagamento. Os sistemas de liquidação bruta em tempo real (RTGS) são sistemas de comunicação entre as instituições financeiras que permitiram o avanço tecnológico das transações financeiras (CARSTENS, 2018) e surgiram a partir de 1985, agilizando os processos de transações financeiras. Em 1990, o número de Bancos Centrais que utilizavam estes sistemas passou de 3 para 8, em 2000 eram 49 e em 2005 todos os Bancos Centrais de economias avançadas utilizavam os sistemas de liquidação em tempo real (BECH, 2017), como mostra o gráfico abaixo.

Figura 1 - Difusão dos Sistemas RTGS



Fonte: Extraído de BECH (2017, p. 7)

Este avanço possibilitou o desenvolvimento de sistemas ainda mais robustos de liquidação, aumentando ainda mais o alcance e a velocidade de circulação da moeda. A partir de 2000 surgiram os sistemas de pagamentos rápidos, que agilizam ainda mais os processos e a velocidade da circulação da moeda. Estes avanços foram possíveis somente com o desenvolvimento da tecnologia digital a partir da década de 1980. Como Meyer (2001) descreveu, a movimentação de meios de pagamento de forma online, via internet, exigem avanços tecnológicos e consequentes investimentos pois isto envolve o acesso instantâneo aos bancos de dados das instituições financeiras com históricos de movimentações e saldos em tempo real. Os próximos passos dessa evolução atualmente convergem para a utilização do sistema de Blockchain, também chamado de Tecnologia de Registro Distribuída (DLT) (BECH, *ibid*) que será detalhado no segundo capítulo deste texto.

Outro principal fator que possibilitou tais avanços foi o fato do valor da moeda estar lastreado totalmente na fé das populações. A partir do momento em que as transações passam a ser digitais e até o papel moeda sai de circulação, não deixando sequer a evidência da validade das moedas que estão sendo transacionadas, a relação se dá puramente com base na confiança do valor dos saldos. Harari (2015) diz que objetos que são utilizados como moeda “só têm valor em nossa imaginação coletiva” para ilustrar que o que dá valor a estes objetos eleitos como moeda não está em suas formações químicas ou físicas, mas este valor é um “construto psicológico”, ou seja, “As pessoas estão dispostas a fazer essas coisas quando confiam no produto da imaginação coletiva. A confiança é a matéria-prima com que todos os tipos de dinheiro

são cunhados”. Antes de continuarmos a discussão, é importante ressaltar a diferença entre o termo “dinheiro”, utilizado por Harari e “moeda”, descrita anteriormente, e deixar claro que a colocação do autor é aplicável a qualquer forma de moeda. A expressão “imaginação coletiva” pode soar um pouco hostil ou desrespeitosa em um primeiro momento, mas é aí utilizado para demonstrar que as pessoas que realizam transações monetárias quaisquer, o fazem apenas por aceitar que o objeto utilizado como moeda possui, de fato, a importância social de moeda.

1.3. Moedas Paralelas

A primeira metade do século XIX foi um período de desenvolvimento de novas interpretações do impacto social causado pelo dinheiro principalmente após a Revolução Industrial e uma destas correntes de pensamento surgente neste período foi a economia solidária, caracterizada por empresas e iniciativas autogeridas com o intuito de promover a inclusão de todos na economia (SINGER, 2002). Um dos exemplos mais conhecidos deste período de surgimento das instituições cooperativas é o da Rochdale Society of Equitable Pioneers, considerada a primeira instituição cooperativa moderna. Fundada em 1844, a cooperativa de Rochdale foi uma cooperativa de compras coletivas criada por trabalhadores com o intuito de realizar compras coletivas por preços menores, garantindo o acesso de todos aos produtos (FAIRBAIRN, 1996).

As idéias da economia solidária e de novas formas de organizações financeiras como as cooperativas trouxeram consigo uma nova forma de moeda: a moeda social. A moeda social tem como intuito suprir necessidades específicas de determinadas comunidades que se encontram à margem da economia e não possuem acesso a bens e serviços. Cabe aqui a explanação de que moedas sociais não buscam competir espaço com o dinheiro oficial de cada local, mas de complementar o seu alcance (CAMINHA e FIGUEIREDO, 2011). Apesar de reconhecidas pela autoridade monetária local, as moedas sociais se diferenciam do dinheiro oficial por dois aspectos, sendo o primeiro a emissão independente do governo e realizada por organizações das comunidades onde as moedas sociais circulam e o segundo a não obrigatoriedade da sua aceitação imposta por lei, como no caso do dinheiro.

O primeiro exemplo bem sucedido de moeda social foi criado na Alemanha em 1929 por Hans Timm e Helmut Rödiger como alternativa ao Reichsmark, moeda alemã que

enfrentava uma forte desvalorização no período (SCHROEDER, 2005). O Wära era aceito como forma de pagamento em mais de mil estabelecimentos comerciais dois anos após a sua criação e foi utilizado como parte do pagamento para funcionários durante este período (ONKEN, 1997 apud SCHROEDER, 2006, p.35). O Wära teve que parar de ser emitido em 1931 quando o governo alemão proibiu a circulação do que chamou de “moedas de emergência” (SCHROEDER, *ibid*).

A moeda social é considerada sempre uma moeda paralela pois sua aceitação não é mandatória, mas baseada na confiança bilateral entre usuários envolvidos nas transações (SOARES, 2006). O nome “moeda social” advém do fato de que, de forma geral, estas possuem o intuito de recolocar na economia as populações desbancarizadas ou sem acesso a poder de compra. Seu funcionamento se baseia na emissão de uma massa monetária que é gerenciada pelos próprios usuários com a intenção de aquecer o comércio de uma determinada comunidade. A moeda social consegue cumprir perfeitamente as três funções básicas de unidade de conta, meio de pagamento e reserva de valor. Por ter a sua gestão coordenada pelos próprios usuários, possui uma maior capacidade de absorção de choques inflacionários. O lastro destas moedas não necessariamente está atrelado ao dinheiro emitido pelo governo, apesar de poder haver uma relação de paridade entre estas duas formas de moeda. (SOARES, *ibid*)

O incentivo para a adesão ao uso das moedas sociais provém do pensamento comunitário. Um dos principais exemplos deste tipo de organização foi o sistema LETS, implantado em 1982 no Canadá e que atualmente se encontra em execução em comunidades nos EUA, Austrália, Nova Zelândia, Inglaterra e França. O sistema consiste em uma moeda com o valor atrelado ao dinheiro oficial criada com o intuito de fortalecer o comércio de pequenas comunidades (SOARES, *ibid*).

No Brasil, a moeda social mais conhecida foi emitida pelo Banco Comunitário Palmas, em Fortaleza, Ceará. O Banco Palmas foi criado em 1999 pela Associação dos Moradores do Conjunto Palmeiras que existia desde 1981. As primeiras Palmas (P\$), moeda social emitida pelo banco de mesmo nome, tinham o valor equivalente a R\$ 0,50 e foram distribuídas entre a população através de operações de microcrédito com o objetivo de incentivar o comércio local. Inicialmente, o volume destas operações era limitado ao equivalente a P\$ 100,00 (cem palmas) para pessoas físicas e R\$ 5.000,00 (cinco mil reais) para pessoas jurídicas e o acesso exigia pré-requisitos como participar das reuniões da instituição e estar adimplente na comunidade (CAMINHA e

FIGUEIREDO, 2011). O incentivo ao comércio local era realizado através do desconto das compras realizadas utilizando Palmas (P\$), que variava entre 5% e 10% do preço. Em 2009, eram 240 estabelecimentos comerciais aceitando as Palmas como pagamento e as transações poderiam ser realizadas de forma eletrônica através do Palmacard (FOBE, 2016). Segundo uma pesquisa realizada pela Universidade Federal do Ceará encomendada pelo Ministério do Trabalho e Emprego em 2008, quando o Banco Palmas completou o seu décimo ano em funcionamento, 98% dos entrevistados consideram que o Banco Palmas contribui para o desenvolvimento do conjunto Palmeira, 90% declararam que o Banco Palmas contribuiu para a melhoria de sua qualidade de vida, 26% aumentaram a renda familiar devido à ação do Banco Palmas, 20,2% conseguiram trabalho por meio do Banco Palmas e 61% atribuí nota de 9 a 10 para o Banco Palmas (SEGUNDO, 2008)

Outro exemplo de Banco Comunitário que emite a sua própria moeda é o Banco Bem, criado em Vitória, Espírito Santo, em 2005. A atuação do Banco Bem é similar a do Banco Palmas, distribuindo a moeda através de microcrédito limitado a B\$ 100,00 (cem bens) por pessoa, sem juros e pagáveis em até duas parcelas mensais. Segundo a administração da instituição, entre outubro de 2005 e junho de 2006 foram concedidas 29 operações de empréstimos, totalizando os valores de B\$ 2.241,50 (dois mil duzentos e quarenta e um bens e meio) para consumo e R\$ 45.647,90 (quarenta e cinco mil seiscentos e quarenta e sete reais e noventa centavos) para comerciantes e realizações de obras (MENEZES e CROCCO, 2009).

1.4. Moedas Virtuais

A possibilidade de acesso a internet propiciado pela criação da *world wide web* e seus protocolos foi responsável por um novo capítulo na história das moedas. Além de possibilitar o aumento da velocidade da transação de informações que resultou na digitalização das instituições bancárias, a internet viabilizou a criação de uma outra forma de moeda: a moeda virtual. Segundo a publicação *Virtual Currency Schemes*, veiculada pelo Banco Central Europeu (ECB) em 2012, o acesso a internet provocou a organização de comunidades virtuais que passaram a ter a suas próprias moedas para utilizar como meio de pagamento em ambientes digitais específicos. Segundo a publicação, as moedas virtuais podem ser organizadas de três formas: fechada, aberta

com fluxo unidirecional e aberta com fluxo bidirecional. As moedas com o fluxo fechado são moedas que não podem ser compradas ou vendidas com nenhum dinheiro. Estas moedas são conseguidas dentro das plataformas onde são geradas e podem ser utilizadas somente dentro destas plataformas. Um exemplo deste tipo de moeda é o WoW Gold, uma moeda que circula dentro do jogo online Word of Warcraft, criado pela Blizzard Entertainment (EUROPEAN CENTRAL BANK, 2012).

As moedas virtuais com fluxo aberto unidirecional são moedas que podem ser convertidas a partir do dinheiro mas que não podem ser convertidas de volta. Ou seja, é possível comprar estas moedas utilizando dinheiro mas não é possível vender elas, tornando obrigatória a utilização apenas na plataforma onde as moedas foram criadas. Um exemplo destas moedas foi o Facebook Credits, moeda criada pelo Facebook em 2009 para realizar compras dentro da rede social ((EUROPEAN CENTRAL BANK, ibid).

As moedas virtuais com fluxo aberto direcional são moedas que podem ser convertidas a partir do dinheiro e que podem ser convertidas em dinheiro de volta, ou seja, é possível comprar e vender estas moedas utilizando dinheiro, como é o caso da moeda Linden Dollar, utilizada no jogo Second Life, criado em 2003 (EUROPEAN CENTRAL BANK, ibid). Somente durante o mês de junho de 2008 foram transacionados o equivalente aproximado a 9 milhões de dólares em Linden Dollars (ERNSTBERGER, 2009).

As moedas virtuais são uma parte dos reflexos gerados pela evolução da tecnologia de bancos de dados ocorrida desde a década de 1980 e que resultou na criação das criptomoedas.

1.5. Criptomoedas e os Cypherpunks

Desde antes mesmo do surgimento da *world wide web*, ocorrido na metade da década de 1990, alguns autores estavam discutindo a utilização das nascentes tecnologias de criptografia para assegurar a privacidade dos usuários de instituições bancárias. Estes autores ficaram conhecidos como os *cypherpunks*, junção das palavras *cypher*, inglês para cifra, e *punk*, movimento de contracultura. O termo apareceu pela primeira vez no “A Cypherpunk's Manifesto”, de Eric Hughes, escrito em 1993 e que apresenta as frases

we the Cypherpunks are dedicated to building anonymous systems. We are defending our privacy with cryptography, with anonymous mail forwarding systems, with digital signatures, and with electronic money. (HUGHES, 1993)⁶

Durante a década de 1990, muitos destes contestadores buscaram apresentar novas formas de utilizar a criptografia para garantir a privacidade dos usuários através do desenvolvimentos de sistemas de moedas que poderiam ser aplicados como alternativa às instituições financeiras. Dentre estes sistemas, existem dois que devem se citados com destaque. O primeiro sistema a ser destacado foi proposto por David Chaum em um documento publicado em 1989 que apresenta o conceito de um sistema de pagamento não rastreável, chamado de *Blind Signature Technology* (CHAUM, 1989). Em 1990, Chaum criou a digi.cash, uma empresa que realizava a movimentação de uma moeda digital com o mesmo nome e que utilizava a tecnologia supracitada. A empresa declarou falência em 1998, quando foi comprada pela eCash, Inc., atualmente pertence a empresa Blocura e ainda trabalha com soluções financeiras através da moeda eletrônica criada por Chaum.

A segunda iniciativa a ser destacada é a mais importante para o surgimento das criptomoedas como conhecemos atualmente. O Hashcash foi proposto por Adam Back em 2002 e apresenta um modelo de moeda eletrônica criptografada que utiliza o conceito de duas chaves para realizar as transações (BACK, 2002). Tal conceito será de suma importância para o desenvolvimento das criptomoedas modernas e para as tecnologias criadas por elas. Além disso, Back apresenta uma metodologia de verificação das amortizações das transações que foi aprimorado com o desenvolvimento das novas criptomoedas.

Em 2008, Satoshi Nakamoto publicou o artigo que mudaria o futuro das criptomoedas e da tecnologia digital. O texto intitulado “Bitcoin: A Peer-to-Peer Electronic Cash System” apresenta uma moeda com um sistema de segurança de transações praticamente incorruptível, com emissão controlada de moedas e um sistema de criptografia que consegue deixar anônimos todos os seus usuários (NAKAMOTO, 2008). Os métodos de utilização de chave dupla e de verificação das amortizações das transações propostos por Nakamoto são versões ainda mais robustas dos processos propostos por Back nos protocolos do Hashcash. Como foi apresentado na introdução do texto, a Bitcoin é a criptomoeda mais utilizada e conhecida na história. Como

⁶ Disponível em <https://www.activism.net/cypherpunk/manifesto.html>. Acesso em 11/10/2018.

exemplo, podemos citar os dados da Blockchain.com que mostram que no dia 02/12/2018 existiam 17.405.450 Bitcoins em circulação, haviam sido realizadas 361.720.055 transações utilizando a moeda e 1 Bitcoin era equivalente a 3.968,00 dólares estadunidenses⁷.

As criptomoedas foram possíveis devido a soma de dois fatores, sendo o primeiro o amplo desenvolvimento tecnológico, principalmente na área da criptografia, e o segundo o fato das moedas ao redor do mundo terem alcançado, desde a década de 1970, o ápice da sua construção social ao ser lastreada puramente na confiança dos seus usuários, tornando desnecessários os vínculos com reservas físicas de commodities ou com instituições quaisquer. Não pretende-se aqui alongar a discussão acerca das criptomoedas, uma vez que o próximo capítulo será dedicado inteiramente a elas, mas sim explicitar a forma como se deu o seu surgimento destas moedas, assim como foi feito com os outros tipos de moeda.

1.6. A análise da moeda enquanto fato social

Não seria possível discutir o valor da moeda como instituição social sem antes ter apresentado como a sua presença se deu nas diferentes civilizações existentes no mundo. Sendo assim, após a necessária explanação sobre a construção histórica do surgimento dos diferentes tipos de moedas, passaremos a discutir a última característica implícita nas moedas: o seu valor social.

A discussão se iniciará com o confronto das correntes de pensamento acerca do surgimento da moeda e se encerrará com as discussões acerca da construção da confiança na moeda e o impacto causado na sociedade por esta construção.

Sobre a origem do dinheiro, Carl Menger defende que a moeda surge espontaneamente da necessidade de agilidade nas trocas. Naturalmente, parte da população perceberá que é vantajoso trocar uma mercadoria com maior liquidez pela mercadoria que se quer vender. Por mais esta mercadoria de maior liquidez não lhe seja útil, ela será mais vendável e poderá lhe garantir a realização de uma troca no futuro por algo que lhe seja útil (MENGER, 2017). Esta percepção não se dá em toda a população instantaneamente, mas tal prática se repete a partir do momento em que a população passa a perceber os métodos aplicados pelos indivíduos mais bem sucedidos nas trocas. Portanto, a criação

⁷ Acesso em 11/12/2018.

da moeda não se dá, inicialmente, através de um acordo entre agentes, nem é resultado de legislações. Com o desenvolvimento do comércio a moeda-mercadoria passa a ser utilizada como unidade de conta, ou seja, os preços serão expressos em termos desta mercadoria adotada como moeda não por causa de nenhuma imposição governamental, mas pela facilidade de transação que esta mercadoria oferece por ser amplamente aceita (MENGER, *ibid*). Segundo Menger ainda, a função de reserva de valor se dá pela soma do caráter não perecível dos objetos utilizados como moeda e pela confiança das pessoas na utilização deste objeto no futuro, permitindo a utilização em momentos diferentes. A utilização da moeda como reserva de valor passa então a ser incentivada a partir da adoção de moedas metálicas, que possuem maior durabilidade e menor custo de estocagem. A origem do dinheiro e o início da participação do Estado como garantidor da autenticidade das moedas seria, portanto, um fator que agilizou o processo das transações monetárias ao remover a necessidade de conferência da validade das moedas de cada transação (MENGER, *ibid*).

Hayek complementa esta linha de raciocínio ao trazer a idéia de que as instituições sociais surgem a partir da repetição de comportamentos das comunidades. O autor traz a definição de que as comunidades, de forma geral, são formados por indivíduos que possuem diferentes conhecimentos e que parte deste conhecimento não pode ser sintetizado por nenhuma instituição deliberada, mas apenas pelas instituições criadas pela evolução natural destes indivíduos e que, portanto, somente esta evolução natural seria capaz de ajustar a convivência nestas comunidades (SOARES, 2006).

Soares (2006) também apresenta o contraponto da teoria do surgimento espontâneo com os apontamentos descritos por Geoffrey Hodgson em 2001 onde tentativas de modelização em computadores foram realizadas e em nenhuma delas surge uma unidade monetária. A partir disto, as conclusões tomadas são que teoricamente é impossível o surgimento de instituições provenientes do estado de natureza e que existe a necessidade da existência de intervenções legais para a manutenção de qualquer instituição, terminando a arguição com o fato de que não há consenso científico sobre a forma como surgem as instituições (HODGSON, 2001 apud SOARES, 2006). Soares ainda diz sobre as teorias contra a forma espontânea do surgimento das instituições criadas, que com base na teoria dos jogos, estes surgimentos dependem de variáveis como as condições nas quais as instituições nascem e qual é a estratégia utilizada para a sua manutenção. A autora termina o texto ressaltando que embora o Estado seja

essencial nas discussões sobre mercado e moeda, e apesar do tamanho da importâncias deste nesta discussão, o Estado não é a única instituição que influencia a elaboração e manutenção da instituição monetária (SOARES, *ibid*).

Knapp é autor da Teoria Estatal do Dinheiro que aponta que a moeda só passa a ter o seu valor aceito socialmente após o anúncio do valor da moeda e que Estado tem o papel determinante na definição do objeto que será utilizado como moeda, uma vez que, para o autor, um objeto só é considerado meio de pagamento quando o Estado passa a receber o pagamento dos seus tributos em unidades deste objeto (KNAPP, 1924). O complemento do contraponto aos teóricos da criação espontânea da moeda advém do ponto proposto por Keynes que diz que o Estado é o responsável por determinar qual é o valor nominal e qual objeto possui valor suficiente para ser considerado moeda (KEYNES, *apud* SOARES, 2006).

Sobre a construção da confiança da população na moeda, Therét (2008) apresenta uma explanação e um complemento ao conceito do tripé formado por Dívida, Soberania e Confiança utilizado para explicar o valor da moeda por Aglietta e Orléan. Segundo Therét, a partir do momento em que a moeda passa a se basear nas relações de crédito e não mais em moedas metálicas, o seu caráter fiduciário se torna evidente. O autor então evidencia a composição da confiança proposta por Aglietta e Orléan, através da divisão em três formas de confiança: metódica, hierárquica e ética.

A confiança metódica se apresenta quando indivíduos pertencentes a uma comunidade confiam no valor da moeda pelo fato de os outros indivíduos também confiarem, ou seja, é uma confiança baseada no empirismo do cotidiano. A confiança hierárquica surge da ciência da existência de uma instituição representante da comunidade garantir a validade da moeda. E a confiança ética, por sua vez, se baseia na crença da legitimidade do sistema de valores criado pela comunidade (THÉRET, 2008).

Deste modo, a confiança ética é para a confiança hierárquica o que a legitimidade é para a legalidade e o que a autoridade simbólica é para o poder político. Enfim, por ser elo de confiança, a moeda demanda a combinação destas três formas” (THÉRET, 2008, p. 7).

Desta forma o autor demonstra que, de acordo com Aglietta e Orléan, o papel do Estado na construção da confiança do valor da moeda se dá através da garantia da parcela hierárquica desta confiança. É importante ressaltar que um dos alicerces desta teoria é a consideração da moeda como uma instituição por si só, ou seja, o pensamento sobre a

moeda livre das caracterizações de suas funções, a interpretação da moeda apenas como fato social presente na construção da civilização (THÉRET, *ibid*). Desprender-se das funções ao analisar a moeda garante que o tema da discussão seja de fato a moeda enquanto parte da construção social. Não devemos ater-nos a definir a moeda pelas suas funções diante desta discussão, uma vez que as suas funções podem variar de acordo com cada contexto, como exemplo disto podemos citar os casos modernos onde o dinheiro se desvaloriza, perdendo a sua função de reserva de valor mas ainda mantendo a capacidade de realizar as funções de unidade de conta e meio de pagamento, por mais que estas sejam prejudicadas.

Harari (2015) define a moeda como uma instituição intersubjetiva, que depende da relação entre os indivíduos e está entre o que é considerado realidade objetiva e o que é realidade subjetiva para estes indivíduos.

O dinheiro, por exemplo, não tem valor objetivo. Não se pode comer, beber ou vestir uma nota de um dólar. Porém, como bilhões de pessoas acreditam que ele tem valor, pode-se usá-lo para comprar alimento, bebidas e roupas. Se o padeiro perder subitamente sua fé na nota de dólar e se recusar a me dar um pão em troca desse pedaço de papel verde, isso não tem muita importância. Basta atravessar alguns quarteirões e ir até o supermercado mais próximo. No entanto, se os caixas no supermercado também se recusarem a aceitar esse pedaço de papel, assim como os feirantes e os vendedores no centro comercial, então o dólar terá perdido seu valor. Os pedaços de papel verde continuarão a existir, é claro, mas sem nenhum valor. (HARARI, 2015, p. 128)

A moeda é então a instituição social existente com base na aceitação coletiva na confiança da existência do seu valor e no sentimento de pertencimento a comunidade e as suas práticas (STECHEER, 1995). Mas, ao mesmo tempo em que a moeda traz a um indivíduo a sensação de pertencimento, torna este mesmo indivíduo apto a se dissociar de sua comunidade, pois antes da possibilidade da utilização da moeda para compra e venda tal indivíduo era dependente de sua comunidade para sobreviver e com o acesso a moeda ele "carrega consigo o direito ao apoio e aos serviços dos outros, de forma condensada, como potencial", através da compra (SIMMEL, 1989 apud STECHER, 1995, p. 184).

A partir do momento em que a moeda passa a ser entendida como esta instituição que permite a emancipação da dependência da comunidade através do poder de compra, muda-se a percepção de sentimento de pertencimento ao mudar-se também o foco da sociedade. A moeda passa então a ser, não somente meio de troca, mas fim primordial

das atividades econômicas. Os indivíduos passam a buscar o acúmulo de moedas para garantir o direito de acesso a bens e serviços. Harari (2015) utiliza o significado da importância deste acúmulo de moedas como metáfora para ilustrar a importância da evolução da espécie humana ao dizer que

Assim como o sucesso econômico de uma empresa é medido apenas pelo número de dólares em sua conta bancária, não pela felicidade de seus empregados, o sucesso evolutivo de uma espécie é medido pelo número de cópias de seu DNA. Se não restam mais cópias de DNA, a espécie está extinta, assim como a empresa sem dinheiro está falida. [grifo meu] (HARARI, 2015, p. 90)

Trecho que pode ser complementado pela fala de Simmel que diz que

o importante, entretanto, é que o dinheiro é percebido em toda parte como fim e, com isso, muitas coisas que têm o seu fim em si mesmos são rebaixados a simples meios. Ao mesmo tempo que o dinheiro, por definição, é o meio, os conteúdos da existência se colocam num profundo contexto teleológico sem começo e sem fim. (SIMMEL, 1989, apud STECHER, 1995, p. 185).

A busca incessante pelo acúmulo de moedas propicia o desenvolvimento do surgimento de um novo fenômeno nas sociedades monetárias: a desigualdade social. Os movimentos de flutuações de preços e consequente alteração dos poderes de compra causados pelas alterações dos volumes de moeda em circulação tendem a impactar de formas diferentes os diferentes indivíduos. "A desproporcionalidade no aumento dos preços leva a que determinados grupos de pessoas e profissões sejam especialmente beneficiados e outros prejudicados" (SIMMEL, 1989, apud STECHER, 1995, p. 186).

Para explicar como este fenômeno impacta a confiança da população no valor da moeda, Ganssmann (2001) e Wennerlind (2001) propõem interpretações das transações monetárias como uma forma de linguística, teoria que é revisitada por Therét (2008), como é mostrado abaixo. Segundo esta interpretação, sinais linguísticos e símbolos monetários podem ser similares quando entendemos que para que as interações através destes mecanismos funcionem, é preciso um contexto cultural no qual estas instituições estejam inseridas, ou seja, tanto os sinais linguísticos quanto os símbolos monetários precisam ser reconhecidos, utilizados de forma repetitiva e conseguir transmitir a sua mensagem (THÉRET, 2008). Sendo assim,

enquanto conjunto de símbolos passíveis de serem criados, distribuídos, destruídos, recriados periodicamente no seio de uma comunidade de pagamento, a moeda, como demonstram fartamente as crises monetárias, pode aparecer para parte desta comunidade que está excluída do controle deste processo, não como um instrumento de cooperação e de coordenação, mas como um recurso de poder cuja distribuição desigual é passível de ser contestada e cujo uso será fonte de conflitos. A confiança na moeda não está, portanto, apenas na sua capacidade de gerar a coordenação, mas, também, e antes de tudo, na regulação dos conflitos relativos à emissão e à distribuição dos meios de pagamento; uma moeda de confiança é uma moeda que só pode ser uma boa convenção se for um bom compromisso social. (THÉRET, 2008, p. 14).

Ou seja, de forma similar às variações linguísticas, se a forma monetária atual de uma determinada comunidade não contempla todos os seus membros, os membros marginalizados passarão a não mais utilizar esta forma, criando as suas próprias, de forma muito similar as variações linguísticas e aos diferentes vocabulários existentes em regiões próximas. Este paralelo se mostra bastante esclarecedor quando o comparamos a moedas sociais, virtuais e criptomoedas, que são claramente exemplos de indivíduos que, por não sentirem que as formas atuais de dinheiro contemplariam as suas necessidades monetárias, criaram formas paralelas de moedas para preencher a lacuna de necessidades deixada.

Temos então o fato da moeda como instituição social existente com base na confiança da população em seu valor, em seu poder de compra e na sensação de pertencimento que ela propicia. A atuação do Estado nesta pauta se dá com o papel de garantidor da autenticidade da moeda, que passa então a ser chamada dinheiro, e com a coerção legal da aceitação do dinheiro como forma de pagamento. Entretanto, uma vez que a validade da moeda tem seu alicerce formado pela confiança da população, esta mesma moeda fica sujeita a crises quando parte da população não se sente contemplada na sua utilização. Cenários de crise monetárias deixam esta vulnerabilidade bem clara, como o caso da moeda paralela Wära criada quando houve a desvalorização do Reichsmark alemão citada no item 1.3. Outras ocasiões que deixam clara a dependência da confiança da população para que a moeda seja válida são as criações por comunidades desbancarizadas das moedas sociais e a utilização de criptomoedas como forma de pagamento, estas últimas possibilitadas pelo desenvolvimento tecnológico.

2. A Bitcoin

2.1. Funcionamento

A Bitcoin é uma criptomoeda descentralizada com fluxo bidirecional, ou seja, é uma moeda virtual cujas movimentações são protegidas por criptografia, os registros destas movimentações não são centralizados em nenhuma instituição e ela pode ser trocadas por outras moedas assim como outras moedas podem ser trocadas por Bitcoins (SEGENDORF, 2014).

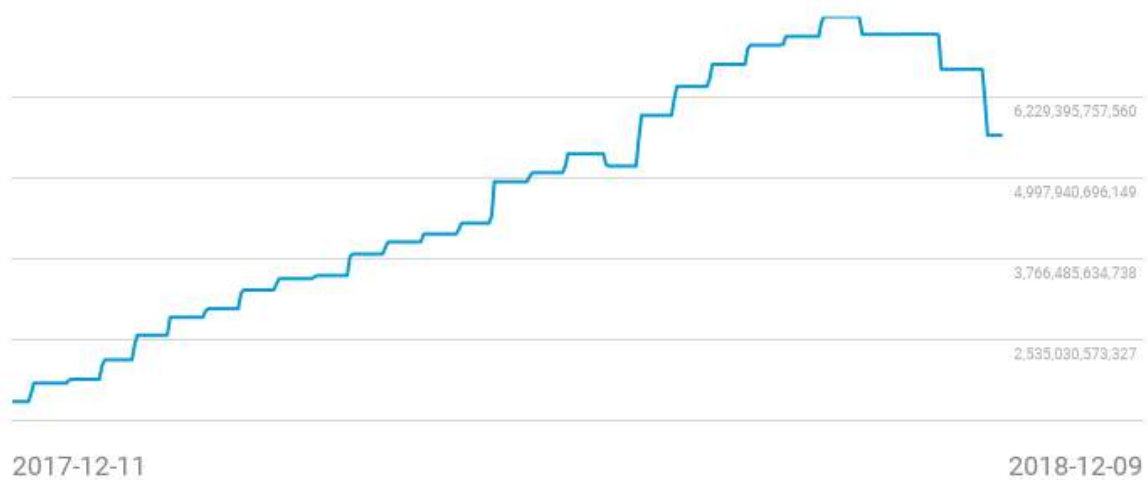
As transações de Bitcoins ocorrem de forma totalmente virtual através de programas de computador conhecidos como carteiras (wallet, em inglês). Cada carteira possui duas chaves, sendo uma pública e a outra privada, de forma muito similar ao Hashcash proposto por Adam Back, onde a chave pública é utilizada para identificar cada carteira durante as transações, devendo ser informada ao emissor de cada transação e a chave privada é a chave utilizada para acessar a carteira e apenas o usuário responsável pela carteira deve conhecê-la, por segurança. As duas chaves de cada carteira são utilizadas para encriptar as transações ocorridas entre elas, através de uma tecnologia conhecida como Hash (NAKAMOTO, 2008). Após ser criptografada a transação passa para o processo de verificação. As verificações são realizadas por usuários ao redor do mundo que disponibilizam o processamento dos seus computadores para realizar a apuração da autenticidade da criptografia das transações. Após verificada, cada transação se junta a um grupo de transações também verificadas naquele período de tempo. Este grupo de transações é conhecido como bloco. Cada bloco é encerrado a cada 10 minutos e então é anexado a Blockchain, um documento que registra todas as operações já realizadas desde o surgimento da Bitcoin (ibid.). Segundo dados da Blockchain.com, uma administradora de carteiras de Bitcoins com sede em Luxemburgo, a média de transações por bloco varia constantemente. Segundo a companhia, a média de transações na última data disponível, o dia 04/12/2018, foi de 1.973 e o ápice destas transações em 2018 ocorreu no dia 03/01/2018 com média de 2.530 operações a cada 10 minutos. Todos os computadores conectados a rede Bitcoin, conhecidos como “nós” (ou nodes, em inglês), possuem uma cópia da Blockchain. Atualmente, uma transação é considerada autêntica e anexada a Blockchain após seis nós confirmarem a conferência da mesma. Se esta verificação for confirmada, ela é adicionada ao bloco que é adicionado ao Blockchain e propagada para toda a rede. (SEGENDORF, ibid.)

2.2. A Mineração e a emissão de Bitcoins

Nakamoto programou a Blockchain da Bitcoin para efetuar o pagamento de uma comissão pelas transações verificadas como forma de incentivo aos usuários da rede para que eles utilizem os seus computadores para realizar as verificações. Segundo Nakamoto, “O incentivo pode ajudar a encorajar os nós a permanecerem honestos” (NAKAMOTO, 2008, p. 4. Tradução minha). Além disso, o sistema também é programado para liberar uma quantidade decrescente de moedas para os usuários donos dos nós a cada 10 minutos, quando um bloco de Bitcoins é processado e adicionado a Blockchain. Quanto mais cálculos estes nós realizarem, maior é a chance deles conseguirem uma destas moedas e, por isso, estes nós que realizam estas verificações ficaram conhecidos como mineiros. A quantidade de moedas liberadas a cada bloco começou com 50 Bitcoins em 2009 e chegará a 0 em 2140, quando o último Bitcoin será minerado e a quantidade de Bitcoins emitidas chegará ao seu final, com 21 milhões de Bitcoin, segundo o cálculo proposto por Nakamoto (ibid.).

Estes incentivos propiciaram um aumento exponencial do processamento computacional da rede de acordo com o crescimento do número de transações realizadas. Tal aumento do poder de processamento da rede se deu através do aumento do número de mineiros e do desenvolvimento de novas tecnologias e organizações como a invenção de processadores específicos para a mineração de Bitcoins e o surgimento de *mining pools*, ou seja, locais com grandes quantidades de máquinas validando as transações. É possível observar este dado na razão de dificuldade de mineração de um Bitcoin, ou seja, qual é a razão de chance de cada processador ser contemplado com a nova Bitcoin programada por Nakamoto. Esta razão é chamada de dificuldade de mineração, e mostrava o valor de uma chance em 5.646.403.851.534 em 09/12/2018 como mostra o gráfico abaixo.

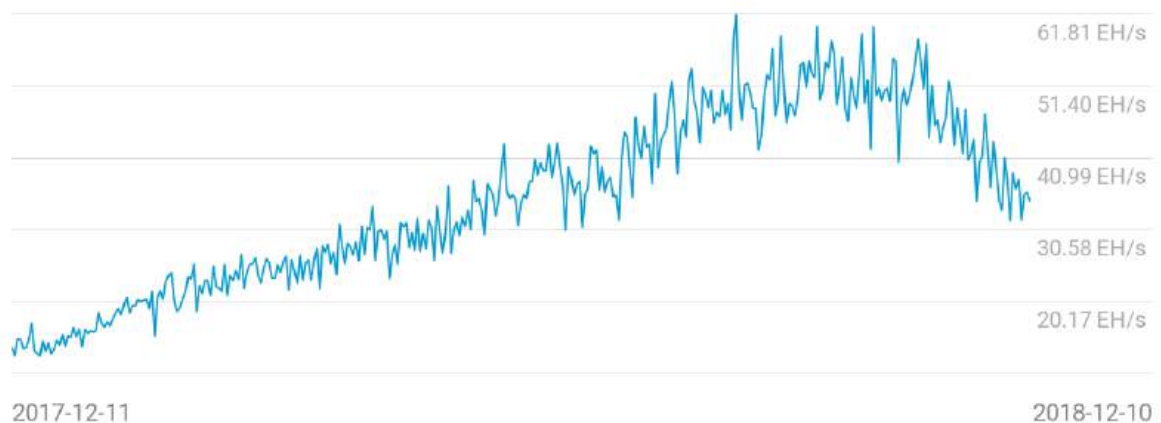
Figura 2 – Dificuldade de Mineração



Fonte: Blockchain.com. Acesso em 10/12/2018

Segundo dados da Blockchain.com, o Hash Rate, que é a estimativa da capacidade de *terabytes* por segundo de dados criptografados que a rede Bitcoin processa, aumentou exponencialmente a partir de janeiro de 2017, como mostra o gráfico abaixo.

Figura 3 – Hash Rate



Fonte: Blockchain.com. Acesso em 10/12/2018

O sistema de validação das transações pelos próprios usuários através da Blockchain funciona com base nestas criptografias possibilitando a construção de um sistema mundialmente integrado e com um nível elevado de segurança. Ao contrário do que acontece no sistema financeiro tradicional, os dados da Blockchain ficam espalhados em todas as máquinas conectadas ao sistema e são verificadas ininterruptamente, sendo

assim, qualquer ação fraudulenta teria que ser realizada com um poder de processamento maior do que a metade da soma de todas as máquinas conectadas ao sistema do Bitcoin ao redor do mundo. Uma vez que cada bloco é gerado a cada 10 minutos, tal ação fraudulenta teria ainda que realizar a alteração dos dados do sistema antes deste prazo se encerrar ou teria que começar toda a alteração novamente. Este sistema de autovalidação da Bitcoin também é robusto suficientemente para evitar o problema do gasto duplo, uma vez que as verificações são realizadas ininterruptamente.

2.3. Os casos da Mt.Gox e da Silk Road

Ainda sobre a segurança do sistema do Bitcoin, é importante explicitar a verdade sobre dois dos principais episódios da história da criptomoeda: os casos da Mt.Gox e as movimentações na SilkRoad.

A Magic: The Gathering, Online Exchange, ou Mt.Gox, foi criada por Jed McCaleb em 2006 como uma plataforma de trocas de cartas de jogos de tabuleiro. Em 2010, com o início da popularização da Bitcoin, McCaleb passou a utilizar a sua plataforma para compra e venda da criptomoeda. A Mt.Gox foi então vendida em março de 2011 para Mark Karpelès.

Na madrugada do dia 20 de junho do mesmo ano, o computador de um dos auditores da equipe de Karpelès foi atacado virtualmente, deixando disponível para os atacantes os dados da carteira de Bitcoins da Mt.Gox. Os atacantes dispararam um mecanismo de venda que reduziu o preço do Bitcoin para US\$ 0,01 durante 30 minutos e neste período compraram 2.000 Bitcoins da Mt.Gox e de seus clientes. O episódio não impactou o preço de mercado da Bitcoin, uma vez que as 2.000 Bitcoins representavam apenas 0,03% do total de 6.605.900 emitidas até aquele dia, segundo dados da Blockchain.com, mas deixou a clara a importância da proteção das chaves privadas das carteiras, como Karpelès enunciou em seu pronunciamento oficial sobre o ocorrido.⁸

Em 2014, um erro no sistema da Mt.Gox permitiu um novo ataque digital que liberou o acesso a toda a base de dados e de chaves privadas dos seus clientes. Os atacantes roubaram 750 mil Bitcoins dos clientes e mais 100 mil da companhia⁹, um prejuízo de

⁸ (Karpelès, 2011). Disponível em https://web.archive.org/web/20110919162635/https://mtgox.com/press_release_20110630.html. Acesso em 08/12/2018.

⁹ BBC. MtGox gives bankruptcy details. Disponível em <https://www.bbc.com/news/technology-26420932>. Acesso em 08/12/2018.

US\$ 460 milhões¹⁰. Neste caso, Karpelès não publicou uma nota oficial, mas apenas dois memorandos respondendo dúvidas sobre como os clientes deveriam fazer para entrar em contato com a Mt.Gox.

Os episódios de roubos a Mt.Gox mostram a importância da proteção das chaves privadas e dos bancos de dados dos clientes das bolsas que operam Bitcoins e provam que os erros foram cometidos pelas equipes destas bolsas e corretoras e não pelo sistema das Bitcoins. Os episódios também provam a eficácia da garantia da privacidade das transações financeiras, uma vez que os responsáveis pelo ataque nunca foram identificados. A criptografia das transações torna impossível o rastreamento das operações apenas pelas chaves públicas. Mas a leitura da Blockchain possibilita observar todo o caminho trilhado por cada fração de cada Bitcoin desde a sua emissão, facilitando qualquer possível investigação, como ocorreu no episódio da SilkRoad.

A Silk Road foi uma plataforma de vendas online sem segmentação que funcionava através da rede The Onion Router (Tor) que torna as conexões de internet irrastráveis através da troca constante de IP. A plataforma foi criada por Ross Ulbricht em 2011 e se tornou famosa pela venda de drogas ilícitas e posteriormente por utilizar o Bitcoin como forma de pagamento por crimes hediondos (ALDRIDGE e DECARY-HETU, 2014). O Silk Road foi encerrado em 2013 e seu criador condenado à prisão perpétua pelos crimes de lavagem de dinheiro, venda de drogas ilícitas e por encomendar o assassinato de 6 pessoas.¹¹

Apresentados os dados sobre estes episódios que são comumente mal explicados, é possível perceber que, assim como acontece com a movimentação ilegal de moedas oficializadas pelos Estados, a Bitcoin também foi utilizada ilegalmente, mas que tal fato não torna a Bitcoin uma forma de corrupção. (ANTUNES, FERREIRA e BOFF, 2015)

¹⁰ Wired. THE INSIDE STORY OF MT. GOX, BITCOIN'S \$460 MILLION DISASTER. Disponível em <https://www.wired.com/2014/03/bitcoin-exchange/>. Acesso em 08/12/2018.

¹¹ Wired. SILK ROAD CREATOR ROSS ULBRICHT SENTENCED TO LIFE IN PRISON. Disponível em <https://www.wired.com/2015/05/silk-road-creator-ross-ulbricht-sentenced-life-prison/>. Acesso em 08/12/2018.

No entanto, em que pesem as facilidades no cometimento de ilícitos que tenham como moeda de troca as Bitcoins, essa, por si só, não vem a ser um objeto ilícito, porquanto o próprio papel moeda utilizado oficialmente pelos Estados, como o Dólar, Euro e o Real, são usados no meio ilegal. Desta forma, é sensato colocar a utilização legítima acima da ilegítima, pois a tentativa de restrição da Bitcoin não prejudicará a rede, por tratar-se de uma tecnologia peer-to-peer, apenas afastaria os usuários cumpridores das leis. (ANTUNES, FERREIRA e BOFF, 2015, p. 8 e 9)

Constatação que Ferreira (2015) completa ao dizer que

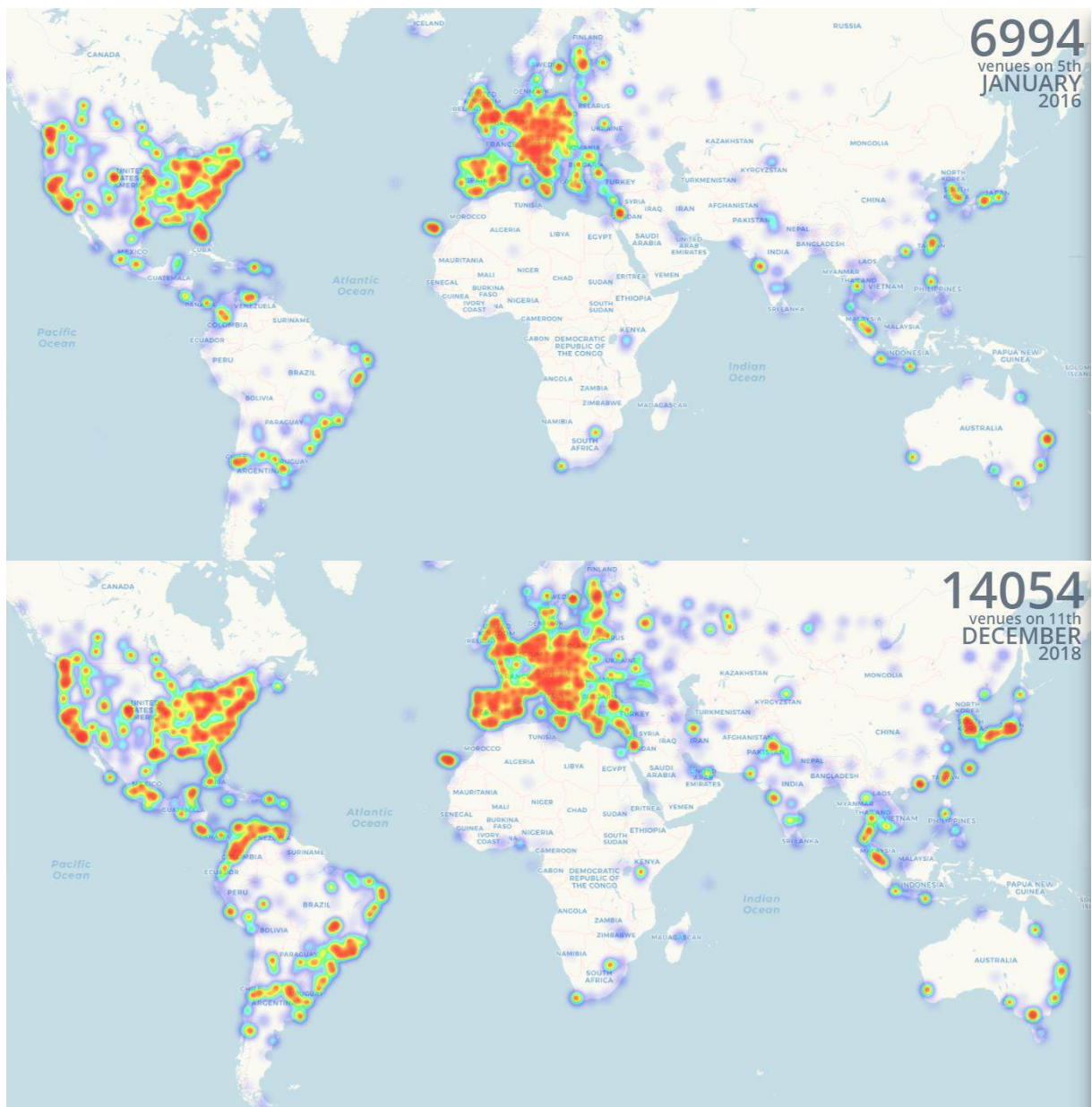
proibir o uso de Bitcoin é colocar-se em uma desvantagem competitiva internacional no desenvolvimento e no uso do que pode ser o sistema de pagamentos da próxima geração, já que é provável que muitos países não proibam seu uso. Contudo, a aplicação das legislações vigentes poderia impedir o desenvolvimento da Bitcoin. (FERREIRA, 2014 p. 23)

2.4. A caracterização da Bitcoin como moeda

Uma vez apresentado o funcionamento da Bitcoin, é necessário analisar os números acerca desta com o intuito de identificar se a Bitcoin possui em si as características econômicas e se ela é capaz de cumprir as funções de uma moeda. Para isto, nos ateremos aos conceitos apresentados nos itens 1.1 e 1.4 deste texto. Inicialmente, tentaremos encontrar um comportamento que possa demonstrar a confiança dos usuários no valor do Bitcoin e posteriormente buscaremos exemplificar como seria possível identificar se as execuções das funções de reserva de valor, unidade de conta e meio de pagamento são cumpridas pela criptomoeda em questão.

Segundo dados do coinmap, em 03/02/2013 apenas 3 estabelecimentos aceitavam o Bitcoin como pagamento em todo o mundo. No final daquele ano, o número havia subido para 1.790 e posteriormente para 5.293 em 2014, 6.980 em 2015, 8.046 em 2016, 11.204 em 2017 e 14.005 em 04/12/2018, como mostra o mapa abaixo.

Figura 4 – Rede de Aceitação de Bitcoins como meio de pagamento



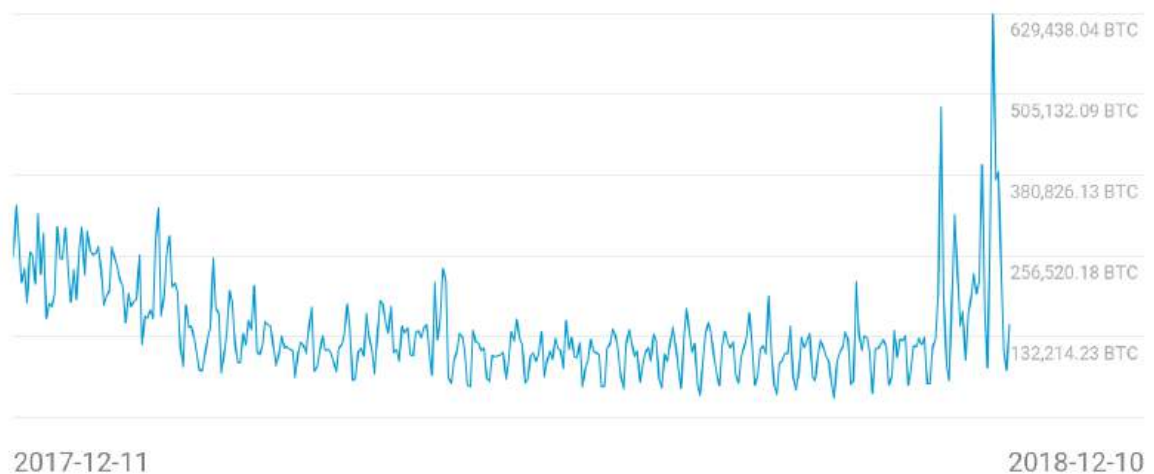
Fonte: Coinmap.org. Acesso em 10/12/2018.

Ao observar o mapa, é possível notar que as regiões que aceitam a criptomoeda como forma de pagamento não se alteraram. Este processo, muito provavelmente, se dá pelo fato do compartilhamento das informações sobre a Bitcoin nestas regiões. Ou seja, o número de estabelecimentos que aceitam Bitcoins como pagamento cresceu mais de 100% nos últimos dois anos mas se manteve distribuído nas mesmas regiões, fato que pode ser interpretado como um reforço a teoria de Menger exposta no item 1.6, sobre a construção da confiança no valor da moeda, onde inicialmente apenas alguns indivíduos

são capazes de perceber o potencial da utilização daquela moeda e posteriormente a população passa a seguir o método que parece ter dado certo.

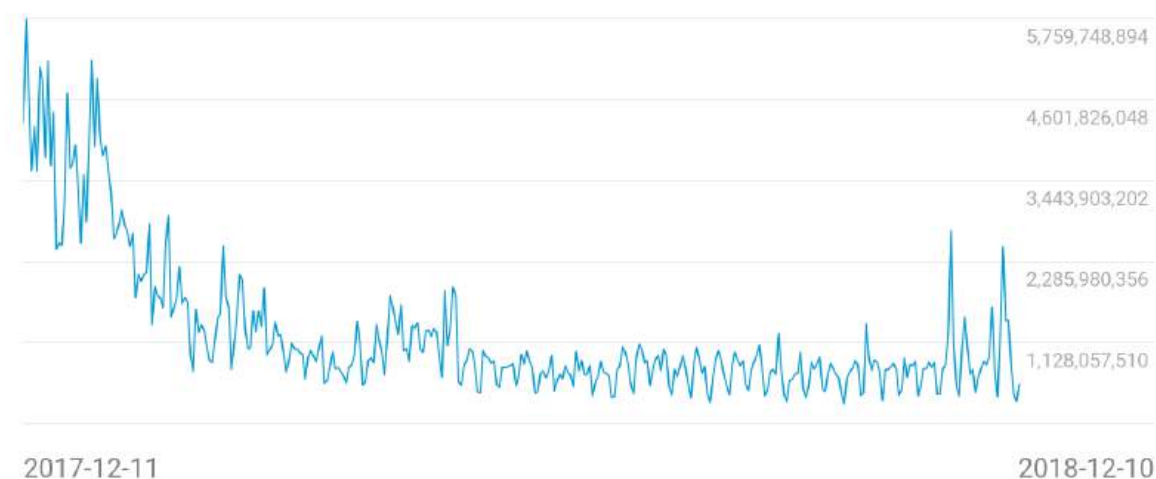
Segundo a Blockchain.com em 05/12/2018 eram 17.408.800 Bitcoins em circulação entre 31.276.102 usuários e um total de 362.246.745 transações realizadas desde agosto de 2009, com uma média diária dos últimos 12 meses de 229.371 transações e de um equivalente a 1.298.021.637,24 de dólares movimentados. Tais dados demonstram que apesar do número total de estabelecimentos que aceitam o Bitcoin como forma de pagamento ao redor do mundo ser pequeno, o número de transações cresce num ritmo cada vez mais acelerado. A confiança no valor do Bitcoin parece ter sido validada, porém é preciso avaliar se a Bitcoin pode ser moeda, ou seja, se ela pode exercer, mesmo que parcialmente, as funções primordiais da moeda.

Figura 5 – Volume diário estimado de transações (em BTC)



Fonte: Blockchain.com. Acesso em 10/12/2018

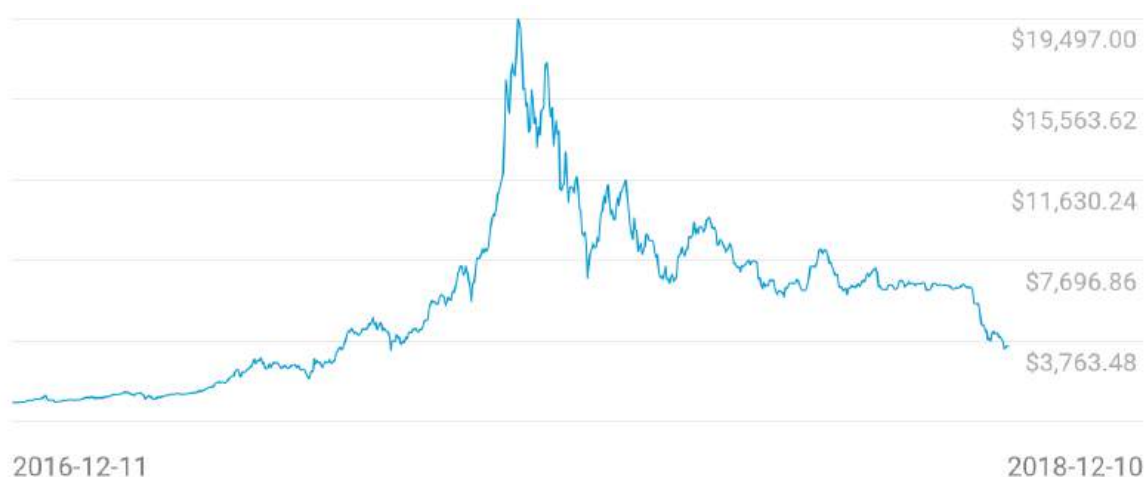
Figura 6 – Volume diário estimado de transações (Equivalente em US\$)



Fonte: Blockchain.com. Acesso em 10/12/2018

É possível notar com facilidade a diferença dos formatos dos gráficos 4 e 5, mesmo com ambos trazendo o volume diário estimado de transações no mesmo período. Tal diferença se dá pela variação abrupta e constante do preço dos Bitcoins em dólares estadunidenses. O gráfico abaixo mostra a variação do câmbio da Bitcoin em dólares estadunidenses nos últimos dois anos. O período mostra a crescente valorização ocorrida entre novembro de 2017 e janeiro de 2018, período onde a moeda chegou a valer USD 19.499,00.

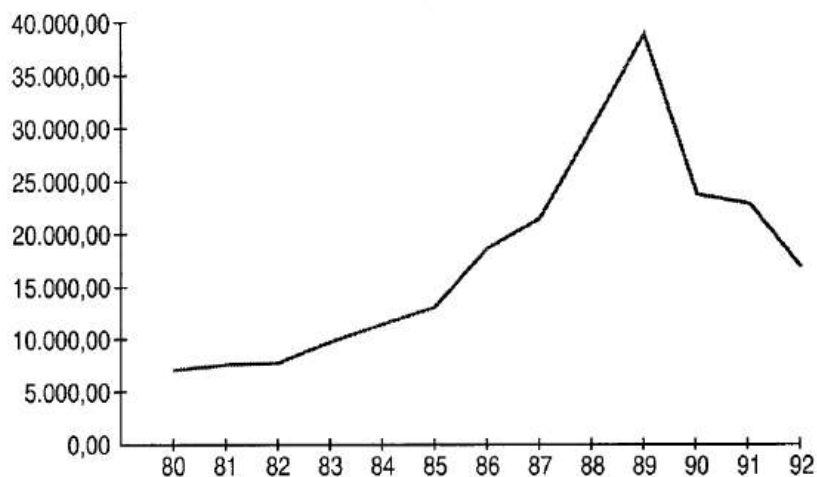
Figura 7 – Preço da Bitcoin em US\$ nos últimos dois anos



Fonte: Blockchain.com. Acesso em 10/12/2018

Este comportamento de alta exorbitante do valor e queda abrupta em um período curto mostra claramente a formação de uma bolha especulativa. O mesmo fenômeno pode ser observado, com uma velocidade menor devido a diferença de desenvolvimento tecnológico, na bolsa de Nikkei durante a segunda metade da década de 1980 (LEVI, 1997), como mostra o gráfico abaixo.

Figura 8 – Índice Nikkei entre 1980 e 1992



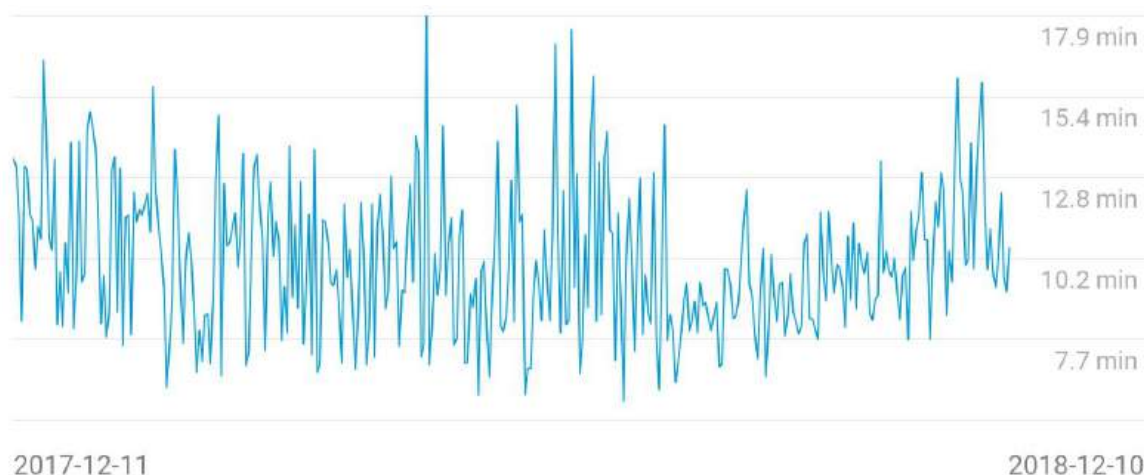
Fonte: Bank of Japan. Economic Statistics Annual (1992)

Tal fenômeno pode ter sido agravado pelo fato de a Bitcoin ter a sua emissão em um volume constante e nenhuma autoridade para interferir no seu valor. Atualmente assistimos o período pós-bolha, onde o Bitcoin volta ao valor cambial em relação ao dólar estadunidense próximo do patamar observado antes do fenômeno. Ou seja, o que vemos é a Bitcoin apresentar uma manutenção do seu valor próximo do equivalente a USD 3.000 observado anteriormente, mas o efeito ainda não chegou ao seu fim e, sendo assim, não é possível afirmar se o Bitcoin é capaz de exercer a função de reserva de valor. Se o preço da Bitcoin em dólares estadunidenses normalizar a sua flutuação em um valor próximo ao observado antes da bolha, temos então a presença da resistência a choques especulativos contida na moeda. Se a desvalorização se mantiver constante e o preço da Bitcoin em relação aos dólares chegar a patamares muito menores do que os observados antes da bolha, observaremos provavelmente a quebra da confiança no valor da criptomoeda e a sua provável derrocada.

Mas assim como foi ilustrado no item 1.4, historicamente existem diversos casos onde o dinheiro se desvaloriza, deixando de executar a função de reserva de valor mas ainda executando as funções de meio de pagamento e unidade de conta. Como foi também foi

exposto no item 1.4 deste trabalho, Menger (2017) defende que a função de unidade de conta está fortemente atrelada a função de unidade de conta não por alguma imposição governamental mas sim porque, ao utilizar a moeda como unidade de conta, as relações comerciais se tornam muito mais simples e rápidas. As análises da capacidade da Bitcoin de realizar estas duas funções portanto serão realizadas conjuntamente. Carvalho (2007), ao listar as propriedades físicas gerais das moedas destaca que estas devem ser confeccionadas em um material divisível e transportável. A Bitcoin, por ser totalmente virtual, permite a divisão infinita das suas unidades e depende apenas de acesso a internet para ser transacionada. O fato de depender apenas de acesso a internet pode ser um potencial a ser explorado em regiões afastadas dos centros urbanos e por populações desbancarizadas. Entretanto, a infinita divisibilidade pode impossibilitar o uso de transações comerciais de baixo valor. Por mais que se utilize uma nova nomenclatura para as frações das Bitcoins, seu uso em transações cotidianas pode ser dificultado. Outro fator que dificulta as transações cotidianas de valores baixos através das Bitcoins é o tempo de efetivação das transações. Segundo o Blockchain.com, o tempo médio das confirmações das transações varia atualmente entre valores próximos de 10 minutos, como mostra o gráfico abaixo.

Figura 9 – Tempo médio de confirmação de uma transação em Bitcoin

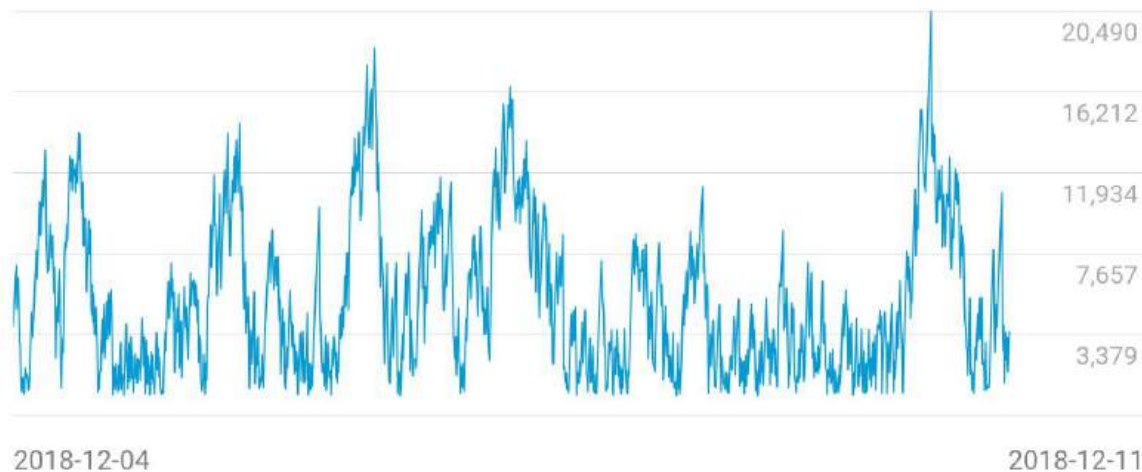


Fonte: Blockchain.com. Acesso em 10/12/2018

Outra forma de verificar esta informação é analisar a variação do tamanho do *Mempool*, ou seja, o volume de operações que estão esperando para serem verificadas. O gráfico abaixo mostra a movimentação do *Mempool* na última semana, na qual é possível ver o

pico de operações aguardando confirmação que, durante esta semana, ocorreu no dia 10/12/2018, quando o este volume chegou a 20.028.

Figura 10 – Transações aguardando confirmação na rede (Mempool size)



Fonte: Blockchain.com. Acesso em 11/12/2018

Ou seja, mesmo que o número de estabelecimentos que aceitam a Bitcoin como forma de pagamento possa parecer expressivo em algum âmbito, a sua utilização como meio de pagamento se mostra inviável, ao menos para pagamentos de pequenos valores. O tempo de espera atual de aproximadamente 10 minutos é suficiente para que ocorra até mesmo uma variação no valor da Bitcoin, que é um mercado que negocia durante todo o tempo. O fato de o valor da Bitcoin flutuar atualmente próximo do patamar de 3.500 dólares estadunidenses coloca como condição o fracionamento em pequenas parcelas de Bitcoins para possibilitar estas transações comerciais pequenas e cotidianas.

Ou seja, a Bitcoin pode ser uma moeda apenas se for considerada um tipo específico de moeda utilizado para transações de grandes valores. Se interpretarmos desta forma, a Bitcoin cumpre todas as funções presentes nas moedas e possui características para continuar cumprindo estas funções. O único fator que pode impossibilitar esta interpretação é a variação constante e abrupta do seu valor cambial, fato que pode trazer insegurança aos usuários da criptomoeda para grandes transações. Ao considerar esta flutuação rápida e, por vezes, violenta, a Bitcoin pode então ser interpretada como um investimento baseado na fé dos usuários e que possui um alto grau de liquidez demonstrado pela sua função de meio de pagamento.

Mas se a Bitcoin não é a substituta ao dinheiro e nem a revolução que vai nos livrar das instituições bancárias que extirpam o nosso dinheiro desde tempos feudais, qual é o impacto gerado por esta criptomoeda no sistema financeiro internacional?

2.5. As heranças da Bitcoin: a Blockchain e as altcoins

Assim como as diferentes formas de moeda passaram por um processo de construção da aceitação, determinação de valor e possibilidades de utilização, as criptomoedas estão evoluindo em uma velocidade nunca antes vista.

O conceito de Blockchain criado por Nakamoto abriu um novo horizonte para a utilização da ciência de dados. A criação da Blockchain é chamada de “The Fifth Disruptive Computing Paradigm” (SWAN, 2015) e a tecnologia já está em sua terceira geração de desenvolvimento e atualmente é utilizada em sistemas de segurança, economia de energia e tecnologias sustentáveis, sistemas acadêmicos de classificação, gerenciamento de riscos de investimentos (ZHENG, XIE, *et al.*, 2018). Além disso, a Blockchain possibilitou a criação de “contratos inteligentes”, que são contratos computadorizados que executam os seus termos de acordo com o que for programado (YERMACK, 2017). A plataforma de execução destes contratos mais conhecida atualmente é a Ethereum, criada por Gavin Wood em 2014. Uma vez que as blockchains são utilizadas também em serviços financeiros ao redor do mundo, a Bitcoin deixa indiretamente um impacto tecnológico no sistema financeiro internacional, mas este não é o seu único impacto na relação dos seres humanos com as moedas.

A criação da Bitcoin incentivou a criação de diversas novas criptomoedas, cada uma com a sua peculiaridade. Não cabe aqui discriminar cada uma destas moedas, mas podemos citar os nomes da Dash, Bitshare, Dash, DogeCoin, LiteCoin, PeerCoin e Ripple, por exemplo. A maioria destas moedas, chamadas de altcoins, utilizam o mesmo sistema ou uma versão muito similar a da Bitcoin (CIAIAN, RAJCANIOVA e KANCS, 2016). Como exemplo, a Zcash possui um protocolo muito similar ao da Bitcoin, se diferenciando apenas na forma como as transações são validadas (QUESNELLE, 2017). A moeda que destacaremos neste trecho não se diferencia por apresentar uma nova tecnologia de processamento ou um novo protocolo de execução da moeda, mas sim por ser uma criptomoeda emitida por um governo e que tem o seu preço baseado em

commodities, retrocedendo a construção histórica do padrão do valor fiduciário. A Petro foi uma criptomoeda com emissão finita lançada pelo governo venezuelano em outubro de 2018 com o intuito de ser uma ferramenta de controle cambial do governo (SUNACRIP, 2018). Segundo o documento de lançamento da criptomoeda, é possível utilizá-la para fazer transferências entre usuários mas o documento salienta a intenção da utilização para compra de commodities venezuelanos. O mesmo documento traz a forma de cálculo do preço da criptomoeda, baseada nos preços praticados nas vendas de petróleo, ouro, ferro e diamante venezuelanos para o exterior (SUNACRIP, *ibid.*). O documento ainda explicita que a forma de incentivo para a utilização da moeda será através de descontos nas emissões de Petro e adverte que haverá a cobrança de uma taxa para a conversão de Petro em moedas estrangeiras.

A Bitcoin traz consigo uma série de evoluções tecnológicas e processuais que possibilitaram a visualização de um novo horizonte de utilização da tecnologia nas relações sociais, sendo assim, é parte da construção não só da forma da moeda como conheceremos no futuro, mas da forma como pensamos a utilização da tecnologia.

Considerações finais

Foi possível observar que desde o primórdio das relações monetárias até o seu contexto atual em sua forma virtual, a intenção final de acumulo de moedas sempre se deu com o intuito de transformá-la em acesso em algum momento. Podemos perceber que intrinsecamente ao fato de ser buscada como fim, como objetivo, a moeda sempre foi meio, processo.

Ao pensar a moeda como uma instituição, um fato social, percebemos que esta está interligada a toda vivência social, seja em qual formato for. Ao tentar discutir o valor da moeda, constantemente tocamos em outras pautas como a efetividade das políticas econômicas, o tamanho do poder coercitivo do Estado e o comportamento político violento do homem.

A aplicação das tecnologias geradas pela Bitcoin em diversas áreas que vão desde o sistema financeiro até as indústrias pesadas mostram que nenhum debate, nenhuma inovação deve se ater ao seu campo de estudo.

Também foi possível perceber que, uma vez que a moeda possibilita o acesso a bens e serviços necessários, esta possibilita também a emancipação dos indivíduos de suas comunidades. Este comportamento poderia se tornar ainda mais evidente em cenários onde o acesso a moeda e ao poder de compra se tornam escassos, mas os episódios de moedas paralelas, principalmente as moedas sociais, trazem uma nova visão sobre este fato. As comunidades, ao se sentirem não pertencentes ao sistema monetário vigente, buscando formas próprias de manter a moeda presente nas suas relações podem provar que o papel do Estado neste cenário é apenas o de garantidor da autenticidade da moeda em sociedades onde este controle é necessário. As moedas sociais trazem, portanto, mais do que o acesso a bens, mas a conjuntura de formação de comunidade de volta e pertencimento desta aos seus membros, não mais o contrário.

O avanço propiciado pelo desenvolvimento de tecnologias digitais possibilitou, antes de mais nada, um aumento imediato na velocidade da comunicação ao redor do mundo. Como consequência, foram agilizadas as formas de transações monetárias. A partir da década de 1990, a velocidade de inovações da economia global impressiona e se torna difícil de ser acompanhado por usuários do sistema monetário convencional. Correntes de pensamento como a dos *cypherpunks* ganham, nesta agilidade de comunicação, a

possibilidade de se unirem, mesmo que geograficamente distantes. Uma forma paralela de moeda com base na tecnologia digital era algo inevitável, se analisarmos o cenário.

É difícil, no momento da composição deste trabalho, medir o impacto gerado pela Bitcoin, suas tecnologias, metodologias e influências. Ainda não é possível medir, por exemplo, o resultado da desvalorização da Bitcoin em relação a dólares gerada pela bolha especulativa de 2016 e 2017. Também não é possível medir o impacto do Petro, que atualmente tem menos de dois meses de existência e também não é possível ainda medir o impacto causado pela Blockchain em diversos setores da economia e da academia. No entanto, é possível observar que a criação da Bitcoin possibilitou a abertura de um novo campo de exploração da tecnologia e o legado desta abertura começa a ser percebido no desenvolvimento de novas criptomoedas mais ágeis e robustas ou nas diversas aplicações da Blockchain. Como foi suposto inicialmente, a Bitcoin não foi uma criação súbita de uma nova forma de pagamento, mas é parte de uma evolução tecnológica constante existente há mais de 20 anos.

Sobre a caracterização da Bitcoin como moeda de acordo com as determinadas funções pertinentes, foi possível observar que a Bitcoin pode ser considerada uma moeda que atualmente, no sexto ano da sua crescente utilização em larga escala, se mostra bastante volátil em relação ao câmbio e que pode apenas ser utilizada para transações contratuais não imediatas, uma vez que o seu tempo médio de transação ultrapassou a cada dos 15 minutos em alguns episódios durante o último ano e o seu valor de mercado, expresso em dólares estadunidenses, também inviabiliza a facilidade das transações de pequenos valor, como foi discutido nos itens 1.6 e 2.4. Se a desvalorização ocasionada pela bolha do biênio 2016/2017 chegar a um ponto crítico que faça com que os usuários percam a confiança na sua utilização, a Bitcoin poderá chegar ao seu fim ou se tornar apenas um ativo baseado na fé dos usuários.

Referências Bibliográficas

- ALDRIDGE, J.; DECARY-HETU, D. **Not an "eBay for Drugs": The cryptomarket "Silk Road" as a paradigm shifting criminal innovation.** [S.l.]. 2014.
- ANTUNES, F. D. S.; FERREIRA, N. A.; BOFF, S. O. **Bitcoin - Inovações, impactos no campo jurídico e regulação para evitar crimes na internet.** 3º Congresso Internacional de Direito e Contemporaneidade. Santa Maria / RS: [s.n.]. 2015.
- BACK, A. **Hashcash - Amortizable Publicly Auditable Cost-Functions.** [S.l.]. 2002.
- BECH, M. Central Bank Cryptocurrencies, 2017.
- BECH, M. **The quest for speed in payments.** [S.l.]: Bank for International Settlements, 2017.
- CAMINHA, U.; FIGUEIREDO, M. Atividade Financeira e Moeda: Análise da Experiência dos Conjunto Palmeiras em Fortaleza - CE. **Revista Direito GV**, São Paulo, 2011.
- CARSTENS, A. **Money and payment systems in the digital age.** [S.l.]: Bank for International Settlements. 2018.
- CARVALHO, F. J. C. D. **Economia monetária financeira: teoria e política.** Segunda. ed. [S.l.]: Elsevier, 2007.
- CHAUM, D. **Blind Signatures for Untraceable Payments.** [S.l.]. 1989.
- CIAIAN, P.; RAJCANIOVA, M.; KANCS, A. The economics of BitCoin price formation. **Applied Economics**, 2016.
- ERNSTBERGER, P. **Linden Dollar and Virtual Monetary Policy.** Forschungsstelle für Bankrecht und Bankpolitik. [S.l.]: University of Bayreuth. 2009.
- EUROPEAN CENTRAL BANK. **Virtual Currency Schemes.** [S.l.]. 2012.
- FAIRBAIRN, B. **The Meaning of Rochdale: The Rochdale Pioneers and the Co-operative Principles.** University of Saskatchewan. [S.l.]. 1996.
- FERREIRA, N. A. **Incertezas jurídicas e econômicas da Bicoín como moeda.** [S.l.]. 2014.
- FOBE, N. J. **Criptomoedas - Um novo paradigma.** [S.l.]: [s.n.], 2016.
- GUTTMANN, R. **A transformação do capital financeiro.** Campinas: Revista Economia e Sociedade, 1996.
- HARARI, Y. N. **Sapiens - Uma Breve História da Humanidade.** Primeira. ed. [S.l.]: [s.n.], 2015.
- HUGHES, E. **A Cypherpunk's Manifesto.** [S.l.]. 1993.
- KNAPP, G. F. **The State Theory of Money.** Primeira. ed. [S.l.]: Macmillan & Company, 1924.
- LEVI, M. L. Liberalização financeira, bolha especulativa e crise bancária no Japão. **Revista de Economia Política**, 1997.
- MENEZES, M. S.; CROCCO, A. M. Sistemas de moeda local: Uma investigação sobre seus potenciais a partir do caso do Banco Bem em Vitória/ES. **Economia e Sociedade**, Campinas, Agosto 2009. 371-398.

- MENGER, C. **Princípios de Economia Política**. 2ª. ed. [S.l.]: Lebooks, 2017.
- METRI, M. M. **Poder, Moeda e Riqueza na Europa Medieval**. [S.l.]: UFRJ / Instituto de Economia, 2007.
- NAKAMOTO, S. **Bitcoin: A Peer-to-Peer Electronic Cash System**. [S.l.]. 2008.
- QUESNELLE, J. **On the linkability of Zcash transactions**. [S.l.]. 2017.
- SCHROEDER, R. F. H. Community Exchange and Trading Systems in Germany. **International Journal of Community Currency Research**, 2005.
- SEGENDORF, B. What is Bitcoin? **Sveriges Riksbank Economic Review**, 2014.
- SEGUNDO, J. J. D. M. N. **Boletim de Responsabilidade Social e Ambiental do Sistema Financeiro**. Banco Central do Brasil. [S.l.]. 2008.
- SINGER, P. **Introdução à Economia Solidária**. 1ª. ed. [S.l.]: Fundação Perseu Abramo, 2002.
- SOARES, C. L. B. **Moeda Social - Uma análise interdisciplinar de suas potencialidades no Brasil contemporâneo**. [S.l.]: [s.n.], 2006.
- STECHER, H. **Georg Simmel: Dinheiro, a solidez do efêmero**. [S.l.]. 1995.
- SUNACRIP. **Petro - Hacia la revolución digital económica**. [S.l.]. 2018.
- SWAN, M. **Blockchain: Blueprint for a new economy**. [S.l.]: O'Reilly Media, 2015.
- THÉRET, B. Os três estados da moeda: Abordagem interdisciplinar do fato monetário. **Economia e Sociedade**, Campinas, Abril 2008. 1-28.
- WEATHERFORD, J. **A História do Dinheiro**. Primeira. ed. [S.l.]: Campus Elsevier, 2005.
- YERMACK, D. Corporate Governance and Blockchains. **Oxford Review of Finance**, 2017.
- ZHENG, Z. et al. **Blockchain challenges and opportunities: a survey**. [S.l.]: [s.n.], 2018.