

Nome: Vinícius Junger dos Santos
Curso: Graduação em Relações Internacionais
Período: 8º
Data: 15/08/2017



A espada e a rede

Ascensão das criptomoedas no sistema Estatal contemporâneo

Estados, bancos e moedas

Existem diversas qualidades que definem um bom meio de troca, algumas físicas, outras voltadas para sua função de mercado. Das qualidades físicas, podemos esperar que uma moeda seja durável: você não quer seu dinheiro estragando com o tempo; quer que seja divisível, para facilitar transações menores; fácil de carregar, para não se gastar energia com transporte; e que seja razoavelmente escassa, visto que serve para o intermédio de troca de bens escassos. Metais nobres, particularmente o ouro, tinham todas essas características e logo se tornaram o padrão de trocas e acumulação de riquezas até o final do mercantilismo, quando o ouro começou a ser substituído por moedas nacionais, mesmo tendo sido utilizado como lastro para o dólar até o fim do acordo de Breton Woods, em 1971 (KILSZTAJN, 1989). Atualmente, as moedas comuns em circulação, emitidas e controladas por bancos centrais dos Estados, são conhecidas como moedas *fiat*, do latim 'faça-se', como referência ao fato que podem ser criadas pela simples vontade dos governantes ou burocratas responsáveis por aumentar a oferta da moeda, uma vez que o lastro não é mais físico, mas fiduciário.

Durante muito tempo, as moedas *fiat* foram as únicas em circulação, fazendo com que toda a população mundial ficasse a mercê das regras de mercado sem qualquer outra opção formal. Aos poucos, grupos não-estatais começaram a criar moedas alternativas, que visavam combater as falhas sistêmicas do mercado, ao fazer moedas *fiat* ou crédito bancário chegarem a lugares economicamente marginalizados. Os benefícios locais trazidos por tais moedas foram recentemente reconhecidos pelos Estados e incorporados em sua legislação, sendo nomeadas de *moedas sociais* (físicas ou digitais). No Brasil, havia dezenas delas espalhadas pelo país, sendo umas das mais conhecidas as Palmas, moeda física do Banco (Comunitário) Palmas¹, e a Palafita, moeda digital do Banco

¹ Pode-se saber mais sobre a iniciativa em: <http://www.institutobancopalmas.org/>.

Maré². É importante perceber que tanto no Brasil como em outros países, as moedas sociais estão sendo cada vez mais submetidas à regulação e são estritamente locais: a extrapolação da moeda para lugares onde o mercado já é abastecido por moedas *fiat* desestabiliza a moeda social e faz com que se perca o benefício que ela vem gerar, que é o acesso à moeda aos desprovidos (FREIRE, 2011). A Palafita é um exemplo de moeda social digital que só pôde vir a funcionar após a aprovação do Banco Central da resolução 4480³ de 2016 e exemplifica a maioria dos casos nos quais moedas sociais buscam paridade na moeda *fiat* local (BATISTA, 2016).

Digital ou física, *fiat* ou social, as moedas ganham novas funções quando tramitadas em larga escala e após suas fronteiras de controle. Enquanto até o período mercantilista as qualidades físicas das moedas eram muito importantes, com o avanço do capitalismo, da cédula, do capital e do crédito, novas características ganham importância: características funcionais. Uma moeda precisa ser uma boa intermediária de trocas – ser facilmente trocada por bens e serviços; ser uma boa unidade de medida – bens e serviços poderem ser facilmente mensurados sobre a moeda; ser uma boa reserva de valor – capaz de reter valor e de transferir o poder de compra do presente para o futuro (FRANCO, 2015).

O controle sobre a moeda nacional, sua emissão, seu valor e seu câmbio constituem – junto com o monopólio da violência, a estatística e a burocracia –, alguns dos pilares que sustentam o Estado contemporâneo (KAVANAGH; MISCIONE, 2015). A manutenção econômica do Estado contemporâneo respalda-se na manutenção de uma moeda *fiat*, uma vez que somente uma homogeneidade na moeda permite taxaço universal, administração de políticas monetárias, financeiras e controle na distribuição de recursos (KAVANAGH; MISCIONE, 2015). Como se pode perceber, em uma crise como vivemos hoje, todo o restante dos pilares do Estado entra em conflito quando a taxaço não é o suficiente para cobrir seus gastos, tendo sido a burocracia – no caso, servidores públicos – um dos principais pilares escolhidos para pagar tal dívida⁴. Outros setores também foram atingidos, como os aposentados e cidadãos por impostos, mas a análise frisa a burocracia por ser considerada um pilar do Estado.

² Pode-se saber mais sobre a iniciativa em: <http://bancomare.com.br/>.

³ Encontrada em:

<https://www.bcb.gov.br/pre/normativos/busca/normativo.asp?numero=4480&tipo=Resolu%C3%A7%C3%A3o&data=25/4/2016>

⁴ A crise atual tem afetado tanto em nível estatal (<https://extra.globo.com/emprego/servidor-publico/sem-salario-aposentados-pensionistas-do-estado-relatam-dificuldades-financeiras-21189306.html>) quanto em nível estadual (<http://g1.globo.com/rio-de-janeiro/noticia/mais-de-200-mil-servidores-do-rj-ainda-nao-receberam-o-salario-de-marco.ghtml>) para quem mora no Rio de Janeiro.

Difícilmente o controle sobre a moeda é afetado, mesmo em momentos de crise, uma vez que ele é instrumento essencial para a manutenção do Estado, para o controle estatal sobre seus cidadãos e para suas relações externas, para o controle do câmbio, das tarifas de importação e de exportação, da legislação financeira e do gerenciamento de dados econômicos em escala estatal (KAVANAGH; MISCIONE, 2015).

De fato, independentemente de crença sobre direito ou dever do Estado de intervir na economia, não há muitas dúvidas de que, constantemente, interesses financeiros, bancários e governamentais se misturam e geram políticas que são implementadas a despeito de seus efeitos na população, por vezes gerando crises em escala global (FILIPPI; LOVELUCK, 2016), seguidos de resgates em termos de 700 bilhões de dólares para os bancos cujas ações resultaram na crise de 2008⁵. O embaraço entre tais instituições torna-se cada vez mais forte, desde que foi abandonado o lastro físico e os bancos passaram a ser as únicas outras instituições capazes de emitir moeda, por meio da criação de crédito, embora haja regulação estatal sobre o limite de criação, a chamada reserva fracionária. A verdade é que a maior parte do controle econômico, falando em termos de quantidade absoluta, acontece pelas políticas financeiras e bancárias, visto que o sistema de crédito em escala internacional contava por 97% da oferta mundial de dinheiro em 2003, com tendência a crescimento (MCLEAY; RADIA; THOMAS, 2014).

Funcionamento das criptomoedas

Toda essa estrutura é abalada quando se começa a tratar de criptomoedas em geral, sendo a mais famosa o *Bitcoin*, embora atualmente existam mais de mil delas. O *Bitcoin* é a primeira das criptomoedas e com ela começou uma revolução, de forma que seu código serviu como base para a criação de todas as outras, mesmo que atualmente existam criptomoedas mais elaboradas. *Bitcoin* é uma rede descentralizada e de ponto-a-ponto (P2P), que permite a transferência e validação da posse de uma moeda virtual – o *bitcoin* – sem a necessidade de envolvimento de um intermediário, contornando o papel de instituições financeiras tradicionais (YEE, 2014). Embora as definições de *Bitcoin* variem de “um método de criar livros-razão descentralizados, validados ponto-a-ponto e com marca de horário” (SCOTT, 2014) a “um sistema de negociação de valor baseado

⁵ Muita indignação pode ser encontrada até em setores conservadores da população Estadunidense: <https://www.theguardian.com/commentisfree/2013/may/28/bank-bailout-cost-taxpayers>.

em criptografia” (BARBOSA, 2016), permanece a certeza de que as criptomoedas são muito diferentes de qualquer outra moeda.

Enquanto no sistema bancário tradicional existe o cliente e o banco, em uma relação de controle na qual todos os clientes são centralizados no seu banco e todos os bancos centralizados no banco central, nas criptomoedas existem somente usuários e mineradores, ambos participando da mesma rede descentralizada como nós (laços de uma malha). Enquanto os usuários utilizam *bitcoins* - em minúsculo para diferenciar do algoritmo *Bitcoin* – para realizar transações comerciais, mineradores destinam parte da capacidade de processamento de seus computadores para validar tais transações, assumindo o papel *fiduciário* dos bancos (GAVRONSKI; FOPPA, 2015). As transações em *bitcoin* têm pequenas taxas que servem para pagar o trabalho dos mineradores, que recebem, além de tais taxas, um adicional de moedas recém-geradas pelo algoritmo *Bitcoin*. Dessa forma, o algoritmo *Bitcoin* fica responsável pela emissão de novas moedas, assumindo o papel de banco central, e cria um processo de autogestão economicamente sustentável (FILIPPI; LOVELUCK, 2016). O *Bitcoin* se torna então a primeira resposta para o ‘Problema dos Generais Bizantinos’, configurando-se como uma rede de transações autônomas onde não há necessidade de confiança em um intermediário para garantir a integridade das transações. Para maior entendimento, faz-se necessário quebrar os componentes de seu código em elementos que vão dar a essas moedas digitais suas características:

Criptografia: A rede de transações das criptomoedas é composta por usuários com suas carteiras digitais em cada nó. Para que uma transação seja realizada, é preciso que os envolvidos se identifiquem um ao outro, como em qualquer transação na vida real. Seja fisicamente, ao apresentar o dinheiro no caixa de uma loja, seja virtualmente, ao conectar seu perfil com seus dados ao perfil do vendedor, uma identificação faz-se necessária. No entanto, utilizando-se da criptografia PGP (*Pretty-Goo-Privacy*)⁶, a identidade do dono da carteira é preservada durante a transação, de forma que se configure uma rede de transações *pseudônima*. O endereço criptografado é utilizado como um pseudônimo, um nome de usuário para os envolvidos na transação, de forma que qualquer vínculo encontrado entre o usuário e o endereço é o suficiente para os expor.

⁶ PGP é consideravelmente diferente das criptografias comuns, onde somente o conteúdo das mensagens é criptografada. Mais informações em: <http://openpgp.org/>.

P2P: Arquitetura Ponto-a-Ponto, *peer-to-peer* de onde vem P2P, é uma arquitetura de rede na qual cada ponto atua tanto como cliente como servidor. Nossa vida é majoritariamente baseada no modelo tradicional de arquitetura, o cliente-servidor, no qual um ponto oferece um serviço e outro somente o utiliza. Qualquer comércio físico obedece o modelo cliente-servidor, e a parte mais acessível da internet também funciona com este modelo: nosso computador – o cliente – pede informações a um servidor sobre um site, e o servidor faz o serviço de armazenar o site e enviar uma cópia do site sempre que ele for requisitado. Uma característica dessa rede é a centralização, visto que um serviço pode ser facilmente acessado por milhões de clientes ao mesmo tempo, quando se trata da internet. Tal modelo facilita a regulamentação, pois o servidor, que é o intermediário entre o cliente e o serviço, como qualquer intermediário, fica em uma posição vantajosa ao saber informações sobre todos seus clientes, possibilitando que o serviço seja interrompido por atores externos que sabem onde – em que máquina no mundo real – o serviço está sendo oferecido. Para isso, basta que o intermediário envie as informações à polícia federal, que desliga e apreende computadores, como ocorre em investigações sobre corrupção⁷.

Já em um modelo P2P, todas as informações para utilizar e prover um serviço estão distribuídas por todos os nós da rede; no caso de uma criptomoeda, nos celulares e computadores da rede. Como todos atuam da mesma forma - oferecendo o serviço quando pedidos, utilizando o serviço quando quiserem e compartilhando todas as informações entre si – não há intermediários capazes de centralizar a informação e não há forma de algum ator governamental retirar o serviço do ar, a não ser que confisque todos os nós da rede. Ou seja, aplicativos P2P tendem a ser resilientes frente a qualquer tipo de censura, estatal ou não, visto que quanto mais pessoas os utilizarem, mais computadores e celulares precisariam ser apreendidos, tornando inviável a apreensão quando aplicativos P2P se tornam comuns, como os aplicativos de compartilhamento de arquivos via *Torrent*⁸. Dessa forma, o algoritmo *Bitcoin* fica protegido de qualquer tentativa de intervenção direta, estatal ou não.

⁷ Como é de praxe na instituição: <http://g1.globo.com/sao-paulo/noticia/2016/06/agentes-apreendem-computador-na-sede-do-pt-em-sp-diz-policia-federal.html>.

⁸ Em 2012, somente os usuários de dois aplicativos de compartilhamento via *torrent*, tecnologia com arquitetura P2P, contavam com mais de 150 milhões de usuários espalhados pelo planeta. Qualquer apreensão nessa escala é inviável e enquanto sobrar um computador vivo os sistemas P2P podem ressurgir: <https://torrentfreak.com/bittorrent-surges-to-150-million-monthly-users-120109/>.

Proof-of-Work: Todas as transações feitas com *bitcoins* são agrupadas em blocos que são transformados em sequências muito confusas de letras e números chamadas de *hashes* pelo algoritmo *Bitcoin*. Um *hash* criptográfico é uma função matemática capaz de pegar dados de tamanhos diferentes e gerar códigos do mesmo tamanho, mas com composição de dígitos distinta, de forma que somente a mesma palavra gera um mesmo código, que também chamamos de *hash*. Um dígito qualquer de diferença gera *hashes* completamente distintos, o que significa que algoritmos que fazem *hashes*, como o *SHA-256*, são ótimas ferramentas para verificar a integridade de qualquer dado a ser transmitido⁹: a única forma de saber a mensagem é comparar *hashes* idênticos, ou seja, ter a mensagem original em mãos.

Proof-of-Work é o mecanismo de validação para o qual os mineradores emprestam a capacidade de seus computadores. Sua função final, como qualquer validação, é dar segurança à rede de transações (FILIPPI; LOVELUCK, 2016). O maior perigo para uma rede comercial é não fazer o gasto corresponder aos ganhos, de forma que se faz necessário garantir que um ator não receba um produto ou serviço sem completar o pagamento ou use do mesmo dinheiro para pagar por produtos ou serviços diferentes (FILIPPI; LOVELUCK, 2016). A única resposta conhecida pelo ser humano para este problema, até então, era a confiança em um intermediário que garantia que o acordo fosse cumprido, seja ele o banco, quando se trata de transações monetárias, seja ele o Estado, quando se trata de transação de posse, via sistema de patentes.

Um sistema *proof-of-work* baseado em *hashes* faz com que todas as transações de um período sejam agrupadas em um bloco e esse bloco seja transformado em um *hash*. Partes deste *hash* são distribuídas a todos os mineradores que tentam adivinhar, por tentativa e erro, o restante do *hash*, processo que consome cálculo e energia elétrica. Se algum minerador acaba acertando o *hash* original completo, o algoritmo gera novas moedas *bitcoin* e as adiciona na carteira deste minerador como recompensa (FILIPPI; LOVELUCK, 2016). Este processo provê segurança contra ataques, pois a única forma de um *hacker* conseguir comprar algo sem pagar ou fazer múltiplas transações com a mesma moeda seria conseguir validar o bloco no qual estão suas transações. Esse processo requer que ele acerte esse cálculo antes de todos os outros mineradores da rede. Não só ele precisaria de um grande poder computacional como precisaria de muita sorte,

⁹Caso o conceito ainda esteja confuso, antes de seguir a leitura, recomendo brincar com o conceito de *hashes* em sites como esse: <http://www.hashemall.com/>.

visto que a conta é na tentativa e erro, o que gera uma margem estatística muito pequena para conseguir tal ataque. Trata-se de um sistema de validação em rede, que não depende de confiança em ator algum e cuja segurança se fortalece com mais membros, capaz de substituir todos os mecanismos de certificação existentes, desde escrituras até selos verdes. Atualmente, *Proof-of-Work* não é o único método de validação existente, mas nos ateremos a ele para simplificar nossa abordagem.

Blockchain: Por enquanto, pense no *Blockchain* como uma cadeia de blocos conectados com *hashes* de blocos anteriores, o que torna cada vez mais custoso realizar alterações ou falsas validações. Qualquer erro no processo elimina todo o trabalho, visto que um dígito de diferença gera um *hash* completamente diferente, tornando improvável o custo de se *hackear* este tipo de sistema (FILIPPI; LOVELUCK, 2016). Quando um minerador acha a resposta para algum bloco, ele adiciona este bloco na corrente e transfere para todos os nós próximos a si. Os outros mineradores validam essa nova corrente com o algoritmo *Bitcoin* e, considerando ela válida, começam a transmitir a mesma para nós de mineração mais próximos, até que 50% dos mineradores considerem a nova corrente válida. Só após a confirmação de 50% da rede de mineradores, a lista antiga é abandonada e os mineradores começam a tentar quebrar os blocos da lista nova.

Associe esse processo a uma tabela dinâmica onde todas as transações realizadas são adicionadas em tempo real¹⁰, podendo ser acessadas por qualquer um que saiba a identificação de uma carteira envolvida na transação¹¹, faça milhares de transações por bloco e repita o processo cerca de 480 mil vezes¹² e você tem o livro-razão mais transparente e mais seguro da história da humanidade. *Blockchain* dá a confiança no processo que antes só podia ser atingida com um intermediário. Não só é capaz de substituir bancos e Estados como intermediários, como já dito, mas é capaz de substituir empresas que nada mais fazem do que oferecer serviços baseados na confiança de intermediários. Algoritmos funcionais desenvolvidos com *Blockchain* e P2P são capazes de fornecer serviços automatizados como Uber a taxas muito menores ou

¹⁰ Tabela dinâmica de transações a serem validadas: <https://blockchain.info/unconfirmed-transactions>.

¹¹ Exemplo de transação já realizada:

<https://blockchain.info/pt/tx/8088eeadbb0c6cbc6cc87ffacc05045f50195bd3837ec392a894465693578b57>.

Clicando no endereço da carteira, os dígitos criptografados, você pode ver todas as transações feitas pelo endereço:

<https://blockchain.info/pt/address/18NzmGzcY9HsWsOdr5PmmTTYoX1GuCqJu9>.

¹² Lista dos últimos blocos resolvidos: <https://blockchain.info/pt/blocks>.

inexistentes¹³, aplicativos de carona e divisão de custos de corrida¹⁴, serviços de certificação de posse¹⁵ e até internet permanente e descentralizada¹⁶. Efeitos do *Blockchain* sobre o Estado serão abordados em outro artigo, por questão de tamanho do artigo.

Código aberto: Embora não seja uma característica técnica, os efeitos de ser um projeto de código aberto torna as criptomoedas um projeto de organização social ainda mais disruptivo. Código aberto, *open source* em inglês, é um modelo de desenvolvimento de software que promove acesso a uso, cópia, distribuição, estudo e modificação universal de um código que normalmente seria protegido por direito autoral. Códigos desenvolvidos neste modelo podem ser vistoriados pela comunidade, modificados e relançados, gratuitamente ou com uso comercial, e já constituem parte significativa do nosso dia-a-dia, embora não percebamos. Se seu celular usa o sistema operacional *Android*, seu computador usa *Ubuntu*, *Debian* ou qualquer distribuição do *kernel Linux*, se seu navegador é *Mozilla Firefox*, já leu livros com *Calibre* ou acessa sites feitos com *Wordpress*, você já se beneficia do acesso a serviços gerados por esse movimento.

Com relação às criptomoedas, o fato de sua maioria ser de código aberto significa que parar o desenvolvimento de algum projeto não é uma tarefa trivial. O *Bitcoin*, por exemplo, conta com um núcleo de desenvolvedores voluntários desde dois anos após o seu lançamento e que se autodenomina *Bitcoin Core*¹⁷, ou o núcleo *Bitcoin*. Esse núcleo fica em constante contato com a comunidade de usuários e mineradores, ouvindo críticas, sugestões e erros de funcionamento e atualizando o algoritmo *Bitcoin* e seus aplicativos. Todas as mudanças de todas as versões são disponibilizadas para que qualquer um tenha acesso em páginas de compartilhamento de código, como o *GitHub*¹⁸.

Isso tem alguns significados para a regulação: a comunidade crescente de usuários dá retornos sobre o algoritmo, apontando quaisquer tipos de erro, normalmente mais rapidamente do que qualquer governo ou empresa possa contratar pesquisadores para achar falhas técnicas, simplesmente pela diferença em números de usuários envolvidos. Dessa forma, o algoritmo é atualizado sempre que se descobre uma falha e cada vez

¹³ O primeiro que tenho conhecimento é o *Arcade City*: <https://arcade.city/> que funciona na plataforma da criptomoeda *Ethereum* e roda com a criptomoeda *ARC*. Ambas são diretamente conversíveis em dólares e outras criptomoedas.

¹⁴ O mais conhecido é o *La Zooz*: <http://lazooz.org/>.

¹⁵ Fornecidos gratuitamente por *proofOfExistence*: <https://proofofexistence.com/>.

¹⁶ Projeto inovador do *IFPS*: <https://ipfs.io/>.

¹⁷ Os membros podem ser encontrados nesta página: <https://bitcoincore.org/en/team/>.

¹⁸ Todo o código atual da moeda pode ser encontrado aqui e em outros repositórios: <https://github.com/bitcoin/bitcoin>.

mais raras são as chances de intervenção técnica; diferentemente de projetos mantidos em âmbito privado, não adianta haver perseguição aos desenvolvedores em projetos de código aberto, uma vez que mesmo que eles parem de atualizar, qualquer um ou qualquer grupo com conhecimento suficiente pode assumir a tarefa, visto que o código continua disponível para o mundo inteiro; por fim, o código aberto abre a possibilidade para o desenvolvimento e diversificação do nicho que está contido, uma vez que permite alterações e não discrimina o uso nem os usuários do projeto. No caso das criptomoedas, isso significa que tínhamos apenas o *Bitcoin* em 2009, surge o *Litecoin*, *Namecoin* e *Swiftcoin* em 2011, que é o ano em que o *Bitcoin* torna-se de código aberto, e seis anos depois, existem mais de 1.000 criptomoedas alternativas em circulação, também chamadas de *altcoins*¹⁹. Todas partilhando dessa composição técnica, que já tornava o *Bitcoin* algo disruptivo, e algumas oferecendo plataformas e qualidades muito mais evoluídas e diversas, como *Ethereum*, *Zcash* e *Monero*.

Resumindo, com o *Bitcoin*, nasce uma categoria de moedas capaz tanto de ser usada de forma pseudônima, quanto de forma transparente e descentralizada, ou seja, extremamente resiliente, cuja segurança reside na matemática, e não na confiança de qualquer intermediário; extremamente segura e capaz de ser mantida, evoluída e diversificada por qualquer um com competência técnica para tal. É um sistema elegante para fazer transações sem a necessidade de confiança envolvida, excelente para situações onde não se sabe em quais atores pode-se confiar.

Análise econômica das criptomoedas

Embora tanto moedas *fiat* quanto moedas sociais possam ser digitais, como o BRL (padrão ISO para o Real utilizado em trocas on-line) e as Palafitas respectivamente, as criptomoedas continuam sendo completamente distintas das outras duas, mesmo também sendo digitais. De fato, adotei a abordagem ‘criptomoedas’ e não ‘moedas digitais’ para *Bitcoins*, *Litecoin* e todas as outras *altcoins* exatamente para ressaltar tais diferenças. Enquanto as moedas fiat e as sociais têm sua emissão e, conseqüentemente, seu valor controlados pelo Estado, as criptomoedas têm sua emissão controlada pelo algoritmo. Isso significa que, sabendo como o algoritmo funciona, não há espaço para flutuação de valor, inflação ou deflação não calculada por conta de emissão baseada em interesses privados. No caso do *Bitcoin*, é declarado que serão criados no máximo 21

¹⁹ Existem diversos sites de cotação de *altcoins*: <https://www.cryptocoincharts.info/coins/info/1001>.

milhões de *bitcoins*, de forma que a recompensa dada aos mineradores pelo algoritmo está programada para cair pela metade a cada 210 mil blocos de transações validados (BARBOSA, 2016). Dessa forma, em 2009, a recompensa por se minerar um bloco era de 50 *bitcoins*, que eram adicionados ao total circulante na conta do minerador responsável pela validação. Já em 2012, quando o bloco número 210 mil foi minerado, a recompensa caiu para 25 *bitcoins* (CARSLTEN; KALODNER; NARAYANAN; WEINBERG, 2016). Todos os valores capazes de influenciar a valoração da moeda por meio de emissão podem ser encontrados em diversos sites abertos²⁰, diferentemente da estrutura financeira atual que depende da confiança de que bancos abram seus valores corretamente para cálculos macroeconômicos. Nesse sistema, as taxas de inflação são de conhecimento prévio e irrestrito, tornando as criptomoedas consideravelmente mais estáveis para cálculos macroeconômicos. Quando todas as moedas forem inseridas no mercado, a recompensa dos mineradores será somente das taxas de transação (CARSLTEN; KALODNER; NARAYANAN; WEINBERG, 2016).

Frente às moedas *fiat* e às moedas sociais, as criptomoedas compartilham praticamente das mesmas características que as fazem ser consideradas bons instrumentos para serem moedas: são tão duráveis quanto a rede de computadores que as carregam e, como vimos, protocolos P2P são consideravelmente resilientes; são fáceis de carregar, por serem dados e poderem ser acessados em quaisquer computadores conectados à rede; são altamente divisíveis, de forma que no preço atual, 1 *bitcoin* valendo 12 mil reais, a menor unidade possível de transferência em *bitcoins*, que é 0.0000001 *bitcoin*, tem o valor de 0.00013 reais, sendo mil vezes mais divisível do que o real atualmente. Essa diferença gritante na divisibilidade ocorre porque o *bitcoin* é divisível até a oitava casa decimal, e não até a segunda, como as moedas *fiat*.

Frente às funções de mercado, as criptomoedas comportam-se de maneira diversa, de acordo com o código de cada uma: em sua maioria, as criptomoedas funcionam bem como meio de troca, visto que apresentam taxas de transferência consideravelmente baratas e são capazes de se distribuir por pontos da rede, independentemente de fronteiras, sejam essas nacionais, linguísticas, bandeiras ou bancos (FRANCO, 2015). Com alguns centavos é possível enviar *bitcoins* para qualquer carteira do mundo, enquanto a simples transferência entre bancos distintos por DOC ou TED bate

²⁰ Pode-se ver a recompensa atual, a dificuldade dos blocos para mineração, a inflação e muitos outros cálculos em sites como <http://www.bitcoinblockhalf.com/>.

facilmente os 10 reais para bancos brasileiros²¹. Aproximadamente 450 bilhões de dólares foram enviados por trabalhadores migrantes para suas famílias este ano²², de forma que, nas transações feitas por bancos tradicionais, as tarifas interbancárias internacionais podem consumir montante considerável dessas transações. Transações em criptomoedas diminuiriam os custos, a burocracia e qualquer consequência monetária decorrente de políticas contra migração. Diferenças no acesso às criptomoedas influenciam seu uso como moeda de troca, mas como as conversões cambiais podem ser feitas de pessoa a pessoa, fica fácil se realizar trocas online²³. Além disso, pode-se ressaltar a segurança na transação e no sistema baseado em *blockchain*, que até hoje não foi hackeado. Enquanto isso, a rede de transações bancárias *SWIFT*, responsável por realizar a integração bancária em todo o mundo, não só já foi hackeada diversas vezes²⁴, como já foi utilizada para isolar financeiramente países do mundo que estavam em desacordo com os operadores do sistema²⁵ (DUBOWITZ; FIXLER, 2015). O uso da ameaça de isolamento desse sistema tem sido utilizado como instrumento de política externa²⁶ e a estratégia de alguns países frente às criptomoedas reflete em certo grau questões de domínio técnico, mas que também são completamente políticas. A maior dificuldade para a confirmação de criptomoedas atualmente como moeda de troca é a ignorância de sua existência ou quanto à forma de uso por lojistas e clientes que ainda não as adotaram em massa.

Frente à armazenagem de valor, as criptomoedas parecem também, em sua maioria, ser mais promissoras do que qualquer moeda *fiat* ou social existente, por causa do processo de emissão de novas moedas. Em sua maioria, as criptomoedas seguem o mesmo modelo do *Bitcoin*: têm um valor total a ser emitido já previamente definido, taxas de inflação estáveis e seu preço é basicamente regulado pela oferta e demanda. Em seu

²¹ Dou como exemplo as tarifas do Banco do Brasil, mas basta pesquisar a do seu banco para ver que provavelmente até as tarifas de transferências para contas do mesmo banco ultrapassam alguns centavos: <http://www.bb.com.br/docs/pub/trf/tarifasPF.pdf>.

²² De acordo com estudo do Fundo Internacional para Desenvolvimento Agrícola da ONU: <http://www.un.org/apps/news/story.asp?NewsID=56973#.WZDSy1WGOM>.

²³ Fenômeno interessantíssimo é ver o Mercado Livre se transformando em casa de câmbio: <http://lista.mercadolivre.com.br/bitcoins#DJA:bitcoins>].

²⁴ Rápida procura revela diversas reportagens sobre hacks e enormes quantias desviadas: <https://www.cyberscoop.com/losing-millions-hackers-swift-banks-now-enforce-mandatory-security-controls/>.

²⁵ Só após quatro anos de isolamento e mudança de regime que o Irã voltou a estar completamente conectado à rede que operacionaliza as transações globais: <http://www.nytimes.com/2012/03/16/world/middleeast/crucial-communication-network-expelling-iranian-banks.html>.

²⁶ As elites dos países atingidos tendem a se revoltar contra qualquer governo que seja banido do *SWIFT*, tornando a ameaça especialmente ameaçadora para países cuja riqueza está muito concentrada em um setor de exportação, como a Rússia: <http://www.investopedia.com/articles/investing/022315/sanctions-swift-could-hit-russia-where-it-hurts-most.asp>.

tradicional ³⁰, até propostas de plataformas múltiplas e descentralizadas de balanceamento entre criptomoedas³¹.

Junta-se tudo isso aos atuais 63%³² da população mundial tendo acesso a um celular e já temos um cenário onde estudos estão sendo feitos sobre a morte das moedas *fiat*, embora pareça muito pouco provável, além de bancos e governos se revezarem em adotar novas estratégias para se adaptar a esta nova realidade financeira.

Impactos e Estratégias

Em primeira instância, o maior e mais visível impacto das criptomoedas foi resumido por estudiosos como a “perda do monopólio das autoridades monetárias de cada país de gerenciar a parte monetária de sua economia como bem entender” (GAVRONSKI; FOPPA, 2015) ou “a substituição de um conjunto de intermediários poderosos como bancos comerciais, bancos centrais e o Estado por uma rede difusa controlada por pessoa alguma” (SCOTT, 2014). Embora não haja muitas dúvidas sobre a profundidade de tais impactos, acredito que ainda seja possível ressaltar outro aspecto tão abrangentes e profundo quanto esses: um impacto no modo de pensar das pessoas. O *Bitcoin* questiona uma das prerrogativas fundamentais do Estado, a emissão e regulamentação da moeda, causando dúvidas sobre a **necessidade** e, conseqüentemente, sobre a **legitimidade** das instituições financeiras existentes (FILIPPI; LOVELUCK, 2016). Dividiremos então a análise entre os três atores mais afetados: bancos comerciais, bancos centrais e Estados.

Bancos comerciais

Bancos comerciais podem ser severamente impactados e sabem muito bem disso: o *Bitcoin* sozinho é suficiente para “retirar alguns bancos do jogo”³³. Embora acredite que as criptomoedas serão altamente disruptivas no sistema bancário comercial, é difícil dizer que, pelo menos a curto ou médio prazo, o *Bitcoin* sozinho seria capaz de ruir a estrutura bancária. Pelo menos, não sozinho.

³⁰ Serviços de liquidez oferecidos para qualquer mercado: <https://b2broker.net/cryptocurrency-solutions/>.

³¹ A melhor solução feita até agora, esperando para ser lançada, é a *Omega One*, empresa que se propõe a resolver o problema da liquidez, e conseqüentemente diminuir a volatilidade das criptomoedas, ao quebrar e redistribuir transações de uma criptomoeda em diversas outras: <https://omega.one/>

³² De acordo com o site: <https://www.statista.com/statistics/274774/forecast-of-mobile-phone-users-worldwide/>.

³³ Como anunciado por banqueiros que se reuniam no Texas para discutir impactos do *Bitcoin* e Blockchain: <https://news.bitcoin.com/banker-i-am-scared-for-the-banking-industry-bitcoin-could-knock-banks-out-of-the-game/>.

A grande variedade de criptomoedas disponíveis já é capaz de oferecer uma parte significativa dos serviços bancários a custos muito menores. O controle das criptomoedas ser feito por um algoritmo que não necessita de manutenção de uma estrutura física e social complexa como a de um banco faz com que haja grande discrepância de valor nas taxas. Os últimos séculos terem sido quase que exclusivamente dominados por moedas *fiat* e bancos comerciais, também não foi um grande impulso a uma variedade de preços e serviços entre bancos, de forma que só muito atualmente novos modelos de bancos começaram a vingar (DELUCA, 2016).

Pode-se ter certeza que em pouco tempo bancos acabarão tendo que enfrentar grande concorrência com criptomoedas, com relação a transferências, investimentos de curto prazo, comércio cotidiano e investimentos em longo prazo. Para competir com os baixíssimos preços de transações, bancos que dependem em grande parcela deste tipo de entrada precisarão se reorganizar e oferecer tarifas cada vez menores se quiserem manter clientes orientados pelo preço. A conversão monetária que já é feita por serviços bancários também sofre um golpe forte, uma vez que criptomoedas permitem que pessoas físicas façam seu papel muito mais facilmente, quase sem nenhuma regulação e com preços muito baixos, seja em páginas pessoais³⁴, plataformas centralizadas de lances de pessoas físicas³⁵ ou aplicativos P2P³⁶ de trocas de criptomoedas³⁷. Criptomoedas partilham muitas características com outras moedas e ouro, também se configurando como forma de investimento de segurança que vem a competir com investimentos bancários: nos últimos meses, o *Bitcoin* ficou três vezes mais caro que o ouro³⁸. Criptomoedas como a *42Coin*, voltada para armazenagem de valor, investimento de segurança a longo prazo, estão cotadas atualmente em 25.400 reais cada, mais do que seis vezes o valor do ouro³⁹.

De qualquer forma, os serviços oferecidos pelos bancos continuam sendo úteis e com algumas características capazes de continuar atraindo pessoas para o sistema bancário.

³⁴ Nas quais você pode realizar trocas diretamente com os donos do site ou pelo chat de mídias sociais como o *FaceBook*: <http://bitcoinp2p.com.br/quem-somos.html>.

³⁵ Nas quais qualquer um pode fazer seu lance e trocar moedas diretamente: https://poloniex.com/exchange#btc_eth.

³⁶ Formato de rede de computadores onde o computador de cada usuário conectado acaba por realizar funções de servidor e de cliente ao mesmo tempo. Enquanto houver apenas um computador ativo na rede, o programa pode ser copiado, redistribuído e manter-se aquém de regulação, visto que não há um servidor central a ser interceptado.

³⁷ Aplicativos que brincam com o fato de pessoas perderem noites de sono tentando fazer dinheiro trocando criptomoedas: <http://www.coinfeine.com/>.

³⁸ Como pode ser visto em: <http://www.xe.com/currencycharts/?from=XBT&to=XAU>.

³⁹ Valor do *42Coin*: <https://coinmarketcap.com/currencies/42-coin/>.

O papel de intermediário capaz de garantir segurança e retornar o dinheiro do comprador em caso de golpe, embora possa ser feito com criptomoedas, configura-se como um serviço em que bancos têm especialidade em desenvolver. Os algoritmos de criptomoedas não são orientados para reembolsos, de forma que se precisa organizar um intermediário à parte, em caso de segurança. Compras grandes e entre atores desconhecidos poderão continuar sendo intermediadas por bancos, mesmo que eles próprios façam as transações em criptomoedas.

Não se pode esquecer que, embora as criptomoedas tenham surgido como alternativa ao sistema bancário e financeiro, isso não impediu as pessoas de tomarem algumas delas como capital financeiro e especulativo (FILIPPI; LOVELUCK, 2016). Bancos continuam sendo instituições especialistas em prestar consultoria para investimentos, sejam estas em quaisquer tipos de moedas, mesmo que esse serviço esteja cada vez mais sendo descentralizado, em função de usos de algoritmos e Inteligências Artificiais, sob aluguel, para manutenção de ativos⁴⁰.

Os bancos comerciais já começaram a adotar estratégias para se adaptar às criptomoedas, como utilizar as tecnologias envolvidas nestas para manter e melhorar seus serviços, em especial a tecnologia *blockchain*⁴¹. De fato, estima-se que 15% dos grandes bancos já estarão utilizando a tecnologia até o final de 2017⁴², tentando aprimorar-se tecnologicamente para manter a vantagem competitiva e oferecer serviços mais seguros, com menor custo.

“Se não pode vencê-los, junte-se a eles”. A segunda estratégia mais comum é o investimento pesado em entender as criptomoedas e comprá-las em moedas *fiat*, enquanto são baratas. Bancos gigantes – como *J.P Morgan* e *Santander*, junto com a *Microsoft*, outros 30 bancos e algumas empresas menores – estão por trás de massivos investimentos na plataforma *Ethereum*⁴³, ao mesmo tempo em que o FMI insiste que

⁴⁰ Uso cada vez mais comum inclusive entre pessoas físicas: <https://www.pwc.com/us/en/financial-services/research-institute/artificial-intelligence.html>

⁴¹ Uma tecnologia de registro de dados assegurada por criptografia que tem se mostrado a forma mais segura, e até então inviolável, de realizar registro de transações. Diversas criptomoedas utilizam a tecnologia para gerar um livro-razão contendo todas as transações realizadas com a moeda, se tornando um instrumento de transparência. Bancos também correm nessa direção: <https://futurism.com/visa-microsoft-and-ibm-are-all-hiring-blockchain-developers/>.

⁴² Pesquisa da IBM reportada na Forbes: <http://fortune.com/2016/09/28/blockchain-banks-2017/>.

⁴³ O que explica em parte seu sucesso: <http://fortune.com/2017/02/28/ethereum-jpmorgan-microsoft-alliance/>.

bancos invistam rapidamente em criptomoedas⁴⁴. Conforme o lastro tende a mudar de moedas *fiat* para criptomoedas, bancos comerciais poderão escolher entre oferecer benefícios cada vez mais extraordinários em moedas *fiat* para ou adaptar-se para oferecer serviços utilizando-se da mesma tecnologia.

Uma última derivação estratégica parece ser a adotada por todos os atores: lançar a própria moeda digital. Caso as criptomoedas sejam adotadas em larga escala e os Bancos Centrais comecem a emitir as próprias criptomoedas, os bancos tradicionais terão o grande problema de ter de lidar com moedas impossíveis de se trabalhar com crédito. Criptomoedas não podem ser duplicadas em bancos via digitalização e a perspectiva de moedas nacionais se tornarem digitais torna iminente uma possível mudança na legislação sobre reservas fracionárias⁴⁵. Ter moedas digitais próprias seria uma possível alternativa ao crédito, uma alternativa controlada pelo próprio banco, no qual poderia oferecer descontos e taxas altamente competitivas. Cabe ressaltar que não temos como garantir que serão utilizadas criptomoedas em si, por causa do processo de emissão dessas moedas, mas o lançamento de diversas moedas digitais, cuja operacionalização seja idêntica às criptomoedas, pode ser uma boa aposta para garantir continuidade de seus clientes e captar usuários leigos pela ignorância⁴⁶.

Bancos centrais

Não é possível dissociar completamente os impactos das criptomoedas sobre os Bancos Centrais dos impactos sobre o Estado. Aqui há de se tentar restringir aos impactos sobre aspectos de gerenciamento macroeconômico do Estado via Banco Central, enquanto no próximo subtítulo nos atentaremos à regulamentação e às políticas voltadas às criptomoedas.

Os Bancos Centrais parecem ser os mais afetados pelas criptomoedas, pelo simples fato de que o avanço no seu uso impede a realização de suas funções mais básicas para o Estado: regular taxas de juros, implementar políticas monetárias, gerir o suprimento de moeda, regular bancos e o câmbio (FILIPPI; LOVELUCK, 2016). Nada disso pode ser

⁴⁴ Como explicitado na nota de uma reunião em junho de 2017: <http://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2017/06/16/Fintech-and-Financial-Services-Initial-Considerations-44985>.

⁴⁵ Foi necessário adiantar uma parte da discussão sobre bancos centrais:

<https://www.linkedin.com/pulse/why-banks-want-own-cryptocurrencies-lucas-cervigni-lucce->

⁴⁶ Criptomoedas em sua maioria têm uma quantidade ou inflação fixa estabelecida por algoritmos, são feitas em código-aberto e permitem que o usuário decida se vai querer acompanhar ou não as mudanças propostas pelos desenvolvedores, diferentemente de qualquer serviço centralizado. Bancos já começam a adotar esta última estratégia no Japão: <http://www.thejavacoin.com/javacoin-news/item/427-japan-s-largest-bank-to-issue-its-own-digital-coin.html>.

plenamente realizado com a disseminação do uso de criptomoedas pela população visto que sua emissão é realizada pelos seus algoritmos, que não são desenvolvidas para permitirem cópias possíveis de virar crédito por bancos e não facilitarem sua fiscalização, por serem descentralizadas, pseudônimas ou anônimas e de código aberto.

“De fato, se perguntados, muitos vão dizer que um dos benefícios chave do *Bitcoin* é que ele opera além do escopo de governos, política e bancos centrais” (FILIPPI; LOVELUCK, 2016).

Não só as funções dos Bancos Centrais ficam impedidas pelas criptomoedas, como os algoritmos dessas moedas já são suficientes para realizar tais funções, levantando a questão sobre a necessidade da instituição (FILIPPI; LOVELUCK, 2016). Como muito bem resumido por *Jon Matonis*, “você não pode acreditar que bancos centrais desenvolvem um papel importante em nossa sociedade e também acreditar que *Bitcoins* servem como solução monetária” (MATONIS, 2014). É seguro apontar que os Bancos Centrais, se não se adaptarem às criptomoedas, são as instituições que correm o maior risco de se tornarem cada vez menos atuantes nas sociedades.

É fato consumado que o embaraço existente entre Estado e as elites se reflete frequentemente nas políticas operacionalizadas pelo Banco Central, com ênfase na taxa de juros e no câmbio (NUNES, 2015). A primeira estratégia que tem sido tomada pelos governos, em parceria com bancos centrais, é fazer o possível para impedir que novas criptomoedas sejam criadas espontaneamente. Enquanto o mercado das criptomoedas ainda for incipiente, as empresas que surgem continuam precisando se submeter voluntariamente à regulação governamental, visto que precisam lidar com moedas *fiat* e que quase toda a logística atual é passível de fácil fiscalização estatal. A regulação de Ofertas Iniciais de Moedas, *Initial Coin Offers* ou *ICO's*, é uma das estratégias adotadas por bancos centrais até agora⁴⁷. Ao garantir que as novas empresas do país precisem de permissão do Banco Central para lançar suas criptomoedas, os Bancos Centrais fazem valer suas preferências sobre as moedas da empresa: isso significa poder alterar o funcionamento do código das criptomoedas, de modo a tornar fácil a identificação de usuários, e/ou a forma de emissão da criptomoeda; pedir paridade na moeda *fiat* local ou simplesmente inviabilizar a criação da criptomoeda, ao impedir o funcionamento da empresa. Tal estratégia parece se tornar cada vez menos eficaz com o tempo, visto que

⁴⁷ Singapura, Rússia e Estados Unidos já estão envolvidos em cruzadas jurídicas para a regulamentação de ICO's: <https://news.bitcoin.com/singapore-central-bank-clarifies-ico-regulations/>; <https://news.bitcoin.com/russia-legalize-icos/>; <https://news.bitcoin.com/the-end-of-the-ico-wild-west-blockchain-advocates-weigh-in-on-sec-report/>.

quanto maior for a disseminação das criptomoedas e quanto mais elas estiverem integradas a produtos e serviços, menores serão os incentivos para empresas se submeterem à regulação voluntariamente, pois precisarão cada vez menos de moedas *fiat* para trocas.

A outra maior estratégia percebida até agora é, novamente, baseada em juntar-se ao time vencedor e criar sua própria criptomoeda⁴⁸. Muito provavelmente não serão criptomoedas como abordadas anteriormente, com todas as tecnologias que as fazem pseudônimas ou anônimas e com emissão de moedas controladas por algoritmo, mas caracterizando-se mais pelo uso do *blockchain* e pelo controle da instituição sobre a moeda. Sendo esse o caso, bancos centrais, como, por exemplo, o da China⁴⁹ e os dos Estados Unidos⁵⁰, lançariam suas respectivas moedas digitais, usando o termo mais apropriado, para implementar políticas e fiscalização para o uso de tais moedas, atraindo usuários que apoiam um maior controle do estado, a burocracia, as elites e aqueles que ignoram as diferenças entre criptomoedas e moedas digitais⁵¹.

Moedas digitais emitidas por bancos centrais e com tecnologia *blockchain* poderiam ser um excelente recurso para garantir a transparência de contas públicas e recursos por todos os países. No entanto, um controle impecável concebido pela tecnologia *blockchain*, associado ao uso da força para proibir o uso de criptomoedas, seria a combinação perfeita para Estados totalitários. “Fazer que um banco central utilize *blockchain* requer um certo nível de confiança entre os cidadãos do país e sua autoridade monetária, o que significa que é um modelo mais adaptado para sociedades transparentes e desenvolvidas”⁵² diz *Lasse Olesen*, criador da *Coinify*.

Por fim, acredita-se que os Bancos Centrais podem atrair diversos adeptos para suas moedas digitais, por conseguir prover exatamente o que parece ser o que mais falta nas criptomoedas: estabilidade de preços. Essa estratégia será mais bem sucedida para os

⁴⁸ Canada, China, estados Unidos, Singapura, Alemanha entre outros países já examinam a possibilidade de criar suas próprias moedas digitais: <https://www.bloomberg.com/news/articles/2017-06-28/rise-of-digital-coins-has-central-banks-considering-e-versions>.

⁴⁹ Os primeiros testes da criptomoeda do banco central chinês já foram realizados: <https://www.bloomberg.com/news/articles/2017-02-23/pboc-is-going-digital-as-mobile-payments-boom-transforms-economy>.

⁵⁰ Interpretado como o último recurso dos bancos centrais, o lançamento da moeda digital do banco central estadunidense – *Federal Reserve* - é aguardado no mundo inteiro: <http://www.nasdaq.com/article/fedcoin-could-replace-the-dollar-as-we-know-it-cm774260>.

⁵¹ Como a emissão da moeda ser fixa por algoritmo, ser anônima ou pseudônima, descentralizada em arquitetura P2P e de código aberto.

⁵² Análise pode ser lida na íntegra em: <https://www.bloomberg.com/news/articles/2016-12-11/blockchain-lures-central-banks-as-danes-consider-minting-e-krone>.

Bancos Centrais quanto mais rapidamente o fizerem, visto que não só já estão sendo desenvolvidas tecnologias para diminuir a volatilidade das criptomoedas, como maior será o entendimento das pessoas sobre criptomoedas com o passar do tempo, diminuindo a margem de usuários que confundem as moedas digitais com as criptomoedas.

Estado

Com bancos comerciais e bancos centrais sendo impactados pelas criptomoedas, é claro que o Estado não poderia deixar de ser afetado. A diminuição da capacidade de realizar políticas financeiras e monetárias para a população como um todo pode ser considerada um dos pilares sobre os quais o Estado se estrutura (KAVANAGH; MISCIONE, 2015). Porém, como veremos, os efeitos dessas novas moedas sobre o Estado não se limitam à capacidade de alterar as políticas financeiras, mas também afetam seus outros pilares.

As criptomoedas crescem em seu uso, com caixas de *bitcoins* e até de *litecoins* espalhando-se pela Ucrânia⁵³, Malta⁵⁴, Kosovo⁵⁵, Canadá, Estados Unidos e Reino Unido⁵⁶, com o *Bitcoin* sendo reconhecido por 28% dos russos⁵⁷ e por 97% dos indianos envolvidos com a indústria⁵⁸. Na China, o papel-moeda está se tornando obsoleto⁵⁹; mais de 260 mil lojas começam a aceitar *bitcoins* no Japão⁶⁰; e as trocas em *bitcoin* vêm experimentando crescimento rápido na África⁶¹. Quando esses mercados começarem a se integrar com pagamento via *bitcoins*, pode ocorrer o primeiro abalo em outro pilar do Estado: dificuldades crescentes em realizar análises estatísticas para guiar as políticas internas e externas. O discurso de *Gareth Murphy*, diretor do banco central irlandês na conferência *BitFin* em 2014 é exemplar:

⁵³ 150 terminais para serem instalados ainda em 2017: <https://news.bitcoin.com/150-bitcoin-atms-ukraine/>

⁵⁴ O primeiro terminal causou alerta de autoridades financeiras: <https://news.bitcoin.com/maltas-first-bitcoin-atm-triggers-warning-from-financial-services-authority/> .

⁵⁵ Com os caixas sendo instalados a despeito dos protestos do Banco Central: <https://news.bitcoin.com/kosovo-first-bitcoin-atm-central-banks-warning/>

⁵⁶ Inovando com os primeiros terminais de Litecoin: <https://news.bitcoin.com/litecoin-atms-proliferate-globally/>

⁵⁷ De acordo com a pesquisa da National Agency for Financial Studies disponível em: <https://nafi.ru/analytics/kriptovalyuty-eshchye-ne-dengi-budushchego-no-uzhe-modnoe-yavlenie/> com análise em <https://news.bitcoin.com/survey-russians-bitcoin/>.

⁵⁸ De acordo com a pesquisa do *PHD Chamber of Commerce and Industry* com análise em <https://news.bitcoin.com/indian-multi-industry-survey-bitcoin/>.

⁵⁹ Com os pagantes utilizando moedas digitais, créditos de *WeChat* e Criptomoedas: <https://www.nytimes.com/2017/07/16/business/china-cash-smartphone-payments.html>

⁶⁰ Todas usuárias de um aplicativo que permite pagamentos e conversão chamado *CoinCheck*: <https://news.bitcoin.com/rollout-of-260000-bitcoin-accepting-stores-in-japan-begins/>

⁶¹ Em especial na África do Sul e Nigéria: <https://news.bitcoin.com/bitcoin-experiences-rapid-growth-africa/>.

“O ponto de partida para toda a gestão econômica é a mensuração de sua atividade. A maioria dos países possui pelo menos uma agência estatística oficial encarregada por essa responsabilidade. O uso mais generalizado de uma moeda virtual significaria que as agências estatísticas teriam que coletar dados sobre a atividade em moedas virtuais. Caso contrário, medidas de atividade econômica não seriam completas. Não devemos subestimar a gama de fins para os quais as medidas contábeis nacionais são usadas na administração das economias. A esse respeito, a completude e a integridade dessas estatísticas são vitais.” (MURPHY, 2014).

O Bitcoin, cujas criptomoedas em sua maioria são baseadas, não foi pensado de forma a facilitar a integração técnica com os bancos de dados do Estado. Mesmo que se conseguisse alcançar uma quebra suficientemente representativa de pseudônimos para identificar as pessoas envolvidas nas transações, ainda há a barreira técnica de ser capaz de trabalhar com os dados guardados no *Blockchain* (MURPHY, 2014). Os impactos de uma economia mista de criptomoedas com moedas *fiat* se daria não só no cálculo de taxas de juro e câmbio, mas também em medidas básicas sobre riqueza e distribuição de renda dentro do país. E o impacto seria ainda maior à medida que mais usuários utilizarem criptomoedas para efetuar compras internacionais.

Um dos maiores impactos sobre a estrutura estatal se daria na evasão de impostos possibilitada pela troca em criptomoedas, especialmente em sociedades com enorme desigualdade social, nas quais uma grande parte da população precisaria ser fiscalizada e teria consideráveis incentivos financeiros para não aderir à taxaço, as criptomoedas facilitam em demasia processos de evasão de impostos (MURPHY, 2014). Criptomoedas com algoritmos especializados em garantir anonimato aparecem aos montes, são atualizadas e ganham cada vez mais valor no mercado: moedas como *ZCash*, *Monero*, *Dash*, *PIVX* e *XSPEC* têm se mantido valorizadas as três primeiras configuram-se entre as 13 criptomoedas com maior preço em dólares no momento desta pesquisa⁶².

Sem um fluxo regular de impostos, o Estado pode encontrar dificuldades em manter pagamentos para o seu corpo burocrático e forças armadas, abalando assim os pilares da burocracia e monopólio da violência. Visto que qualquer servidor público, político, funcionário ou professor, corpo de segurança, militar ou policial, vive de rendimentos derivados de impostos, e as criptomoedas podem diminuir significativamente esse

⁶² Cotação das criptomoedas pode ser vista em diversos domínios como: <https://coinmarketcap.com/>.

fornecimento, o Estado poderia precisar escolher entre diminuir o corpo burocrático ou militar proporcionalmente ao corte na entrada de impostos, ou mantê-los com emissões crescentes de moedas *fiat* pelo Banco Central. Enquanto a primeira opção em si representa um baque direto na capacidade de ação do Estado, a segunda opção poderia ocasionar em maiores quantidades de moeda *fiat* circulando, sua crescente desvalorização e servidores públicos e corpos militares ganhando em moedas com cada vez menor poder de compra. Fica clara a possibilidade de os efeitos sobre tais pilares do Estado serem os mesmos nas duas opções, só que na segunda, tal efeito seria em longo prazo, contribuindo para maior abandono das moedas *fiat*, mas tornando maior a janela de tempo necessária para qualquer tentativa de intervenção pesada do Estado nas criptomoedas. Para a burocracia estatal propriamente dita, a situação pode ser mais complicada, visto que contratos inteligentes associados à tecnologia *blockchain* conseguem padronizar relações sociais de forma completamente transparente, impossíveis de serem alteradas e a custos mínimos, prometendo serem capazes de realizar diversas funções monopolizadas pela burocracia estatal (KAVANAGH; MISCIONE, 2015).

O penúltimo impacto é a diminuição na capacidade de operacionalizar a legislação. O *Bitcoin* se mostrou um desafio ao sistema legal muito rapidamente, visto que sua explosão aconteceu em 2011, dois anos após seu surgimento, quando nasceu o primeiro grande mercado desregulado da internet: a Rota da Seda, ou *Silk Road*, hospedada em um servidor escondido pela rede *TOR*, a qual somente pessoas razoavelmente safas da Internet conseguiam acessar (FILIPPI; LOVELUCK, 2016). A Rota da Seda transacionava diversos tipos de produtos comuns, além de uma impressionante variedade de drogas, tendo movimentado apenas 1,2 milhões de dólares em *bitcoins* (YEE, 2014), até ser desmantelada e seu operador preso, que foi identificado por não ter preservado seu pseudônimo. Apesar do valor moderado das transações, a *Silk Road* foi prova suficiente para as autoridades de que criptomoedas são capazes de manter mercados paralelos em escala global. O ponto é que, naquela época, a os mercados paralelos ainda eram somente estruturados em arquitetura cliente-servidor, o que possibilitava ações de busca e apreensão, como foi o caso da Rota da Seda. O que acontece agora que estão surgindo mercados descentralizados, anônimos e com

arquitetura P2P, ou seja, inviáveis de serem retirados do ar?⁶³ De fato, não foi nem necessário começar a operacionalizar sobre arquitetura P2P para os mercados desregulados pelo Estado começarem a surgir em peso⁶⁴, muito embora as autoridades não tenham efetuado eficiente trabalho em encontrar e prender operadores e clientes.

Outro impacto que não vai ser abordado em profundidade aqui, visto que se torna de simples compreensão após toda esta discussão, é a maior facilidade de lavagem de dinheiro. Com criptomoedas variando em questão de anonimato, torna-se relativamente fácil realizar operações de lavagem de dinheiro com compra e venda de moedas digitais, bastando que o usuário não relacione seu pseudônimo a si mesmo ou que utilize criptomoedas voltadas para o anonimato (YEE, 2014). Os esforços para se manter anônimo são proporcionais aos ganhos que se teria com qualquer atividade ilegal com criptomoedas, no entanto, os esforços das forças de segurança também crescem proporcionalmente. Sendo o caso de um crescente uso das criptomoedas, e também crescente uso para atividades ilegais, mesmo que não houvesse qualquer impacto sobre a estrutura estatal, seria necessário um contingente ou eficiência também crescente para realizar tantas investigações.

“Se a moeda é um instrumento do Leviatã que reduz a violência de todos contra todos, então uma pergunta interessante é o que acontece se esse argumento *Hobbesiano* for contornado por moedas como *Bitcoin* que não dependem do Estado de forma alguma?” (KAVANAGH; MISCIONE, 2015).

O último grande impacto das criptomoedas sobre o Estado é o provável questionamento sobre a necessidade do sistema estatal atual, a ser feito pelos cidadãos não satisfeitos com a atuação dos mesmos. As criptomoedas, junto com outras aplicações de suas tecnologias, proporcionam um cenário onde seria possível viver com cada vez mais liberdade econômica (criptomoedas), serviços de padronização (contratos inteligentes)⁶⁵, serviços com segurança acessível (*Blockchain*)⁶⁶ e maior participação política direta, por organização em arquitetura ponto-a-ponto (P2P), sem ter de lidar com os percalços

⁶³ Embora ainda podem seguir as leis ou ética estatal, como discutido, o avanço das criptomoedas na economia diminui cada vez mais os incentivos para isso: <https://particl.io/>.

⁶⁴ Com pouca pesquisa pode-se acessar domínios e descobrir quais foram retirados do ar, quais estão com suspeita de estarem sendo utilizados como isca por policiais e qual a taxa de aprovação dos sites: <https://www.deepdotweb.com/dark-net-market-comparison-chart/>.

⁶⁵ Algumas criptomoedas possuem carteiras programáveis e podem realizar transações automaticamente, de acordo com a programação do usuário. São capazes não só de gerir seus fundos e realizar aplicações, como um banco, mas também podem interagir de forma programada com outros serviços automatizados que utilizem a mesma moeda e tecnologia *blockchain*.

⁶⁶ Sistema de registros descentralizado, criptografado, totalmente transparente e até hoje não hackeado.

de conviver com corrupção sistêmica, impostos abusivos e mal aproveitados, além de não ver suas vontades políticas acontecerem por causa de sistemas de representatividade voltados para manutenção de elites no poder. Não é difícil prever uma redução significativa na legitimidade de alguns processos no sistema estatal, não havendo mais necessidade de tais processos serem monopolizados pelo mesmo.

Todos esses cenários partem do pressuposto de as criptomoedas continuarem a ser adotadas em larga escala por pessoas em todo o mundo e os Estados escolherem o embate, frente à adoção e à adaptação. As estratégias de regulamentação, sua operacionalização e, principalmente, a reação das pessoas a elas, serão fatores primordiais para definir se a relação tenderá para uma harmonização entre os atores envolvidos ou para uma série de disputas tecnológicas, econômicas e sociais.

Por sua vez, tais estratégias abordadas pelos Estados variam em demasia, visto o quanto o tema é recente. Embora suas preocupações flutuem em torno das mesmas questões, como lavagem de dinheiro, crime organizado, proteção ao consumidor e evasão de impostos (SCOTT, 2014), suas formas de abordar e operacionalizar as questões têm sido razoavelmente distintas. Como único caso conhecido de Estado que declara ciência da questão das criptomoedas, mas não acredita ser relevante por causa de seu tamanho, temos a República Tcheca⁶⁷.

Os demais Estados têm adotado um modelo similar de operacionalização, mesmo com objetivos variando entre a adoção e o impedimento das criptomoedas. A abordagem mais convencional é a prática comum de o Estado de colocar as regulações nos intermediários. No caso das criptomoedas, isso significa identificar as lojas que estão aceitando criptomoedas e as empresas que oferecem serviços no mercado de criptomoedas e aplicar legislação para forçar a identificação própria e dos clientes. Pedir documentos de identificação na hora da compra, no caso de lojas, ou aplicar legislação para fornecimento de dados dos clientes, no caso de programas *on-line*, parece ter sido a abordagem padrão. Formas utilizadas para realizar a taxação das operações não parecem estar com muita concordância, mas devem seguir os mesmos princípios.

A estratégia da taxação parece ser a principal, embora em termos de operacionalização ainda seja deficiente por depender quase que exclusivamente da colaboração dos

⁶⁷ A reportagem do pronunciamento pode ser encontrada em: <https://news.bitcoin.com/czech-national-bank-publishes-letter-addressing-bitcoin/>.

intermediários ou de vistorias sistêmicas para fiscalização (YEE, 2014). Isso acontece porque é muito fácil criar e utilizar novas carteiras, ou simplesmente novos endereços de carteira para cada transação, ficando a critério do lojista realizar transações ou não pelo endereço de carteira declarada ao Estado. É fato que fiscalizações *in loco* poderiam identificar quais lojistas estão fazendo tais práticas e multá-los, mas o provável crescente número de usuários só dificultaria as fiscalizações e aumentaria o desgaste entre forças policiais e população. Os lojistas que conseguirem manter sua clientela terão também cada vez mais incentivos para embarcar no mercado informal, caso multas sejam aplicadas sucessivamente.

No caso de serviços, especialmente os capazes de serem automatizados, o método de regulação tradicional por ameaça do uso da força se mostrará cada vez menos eficiente. Até mesmo grandes grupos podem simplesmente mudar de região e continuar oferecendo o serviço para todo o mundo, mas hospedados em locais com legislação menos restrita, como é o caso da plataforma de trocas *Poloniex*, que se mudou de Washington após o aumento da regulação⁶⁸. Além disso, mesmo que houvesse consenso na legislação em todo o mundo, as plataformas sempre poderiam se retirar e reemergir em ambientes sem o controle do Estado, como nas plataformas P2P e redes criptografadas, desta vez sem a menor intenção de colaborar (YEE, 2014). A abordagem atual precisa ser mais sutil, se os Estados quiserem manter algum tipo de controle, de forma que tais serviços se sintam incentivados a colaborar e não incentivados a se reconstruir fora de seu controle (YEE, 2014).

A segunda estratégia parece ser a mais radical e envolve trabalhar com a arquitetura da internet para conseguir intervir na comunicação de pacotes de dados partilhados pelas criptomoedas (YEE, 2014). A comunicação pela internet pode ser entendida por um modelo de quatro camadas: uma física, uma protocolar, uma de aplicativos e uma de conteúdo, de forma que se classifica a física como a camada mais baixa e a de conteúdo como a mais alta (CHOUCRI; CLARK, 2012). Intervenções na mesma camada normalmente são contornáveis com conhecimentos técnicos sobre a camada, enquanto intervenções utilizando uma camada inferior para capturar informações de uma camada mais alta tendem a ter efeitos indesejados e indiscriminados (YEE, 2014). Se você já frequentou algum ambiente que utilize filtro de pacotes para impedir certos tipos de

⁶⁸ Fator ainda mais propício de acontecer em sistema federativos: <https://news.bitcoin.com/washingtons-bitcoin-exchange-regulations-become-active/>.

aplicativos ou acessos a sites na internet, já deve ter percebido que outros aplicativos não direcionados pelo filtro por vezes param de funcionar também, além de os filtros raramente funcionarem direito⁶⁹.

É pouquíssimo provável, porém possível, que Estados possam recorrer ao bloqueio da comunicação das criptomoedas em camadas mais baixas. Este método é altamente custoso e contraproducente, não só por causa dos gastos técnicos envolvidos, mas porque, outros pacotes não relacionados podem acabar sendo bloqueados também, impossibilitando sua comunicação em aplicações não relacionadas a criptomoedas (YEE, 2014). Este método poderia ter severos efeitos limitantes na economia e na vida das pessoas, além de não permitir a distinção entre usuários de criptomoedas que abraçam as legislações estatais dos que não as abraçam. Algo deste nível pode ser claramente interpretado como uma decisão estratégica de manutenção do poder, a despeito da população, gerando consequências graves aos governos em modelos democráticos. É, portanto, muito difícil acreditar que este método seja utilizado, e, se o for, tão fáceis são as formas de contornar a fiscalização – como o uso de conexões criptografadas e de redes virtuais privadas – que provavelmente não cobririam nem os custos de sua aplicação. Vale mencionar o método como conhecimento acadêmico.

Alguns Estados parecem pretender investir em barrar o avanço das criptomoedas como a política oficial, embora seus métodos de operacionalização de suas políticas também sejam variados. A Índia experimenta uma crescente adoção de *bitcoins* em mercados, especialmente em Bangalore⁷⁰, e a sugestão dada por um painel formado pelo Ministério das Finanças foi a de começar campanhas de “conscientização” contra *Bitcoin*, seguida de regulação dos lojistas, se necessário⁷¹. Quando uma larga cadeia de mais de 5.000 restaurantes começou a aceitar pagamentos em criptomoedas, as autoridades financeiras polonesas fizeram declarações condenando seu uso e não aconselhando o investimento, mas não propuseram legislação⁷². Outros países apostam na regulação para conter as criptomoedas em sua economia: Israel acaba de ser

⁶⁹ Segundo pesquisa do *MediaWatch-UK* três a cada quatro filtros de internet não bloqueavam pornografia na maioria dos sites: <http://www.telegraph.co.uk/technology/news/10634035/Three-out-of-four-ISPs-porn-filters-fail-to-protect-children.html>.

⁷⁰ Mais de 50 mercadores começaram a aceitar oficialmente *bitcoins* em um período curto de tempo: <https://news.bitcoin.com/indian-bitcoin-hotspot-bangalore-50-new-merchants/>.

⁷¹ Como pode ser lido na reportagem: <https://news.bitcoin.com/indian-government-take-immediate-steps-to-stop-bitcoin-use/>.

⁷² A declaração pode ser encontrada em: http://www.nbp.pl/home.aspx?f=/aktualnosci/wiadomosci_2017/ww-pl.html e análise em: <https://news.bitcoin.com/polish-authorities-issue-sweeping-condemnation-of-bitcoin-and-other-digital-currencies/>.

advertida pela sua autoridade chefe em segurança para ser mais ‘paternalista’ na regulação sobre lançamento de Ofertas Iniciais de Moedas (ICO’s)⁷³.

O Japão é um caso especial, no qual as moedas virtuais já sofreram o primeiro processo de legislação e foram reconhecidas como um método legal de pagamento. Seguindo a primeira abordagem citada, o Japão criou extensiva legislação para transparência de informações nas casas de troca de moedas virtuais, além da taxaço sobre lojistas que comecem a aceitar criptomoedas. Não há taxa sobre consumo na questão de troca de criptomoedas por moedas *fiat*, mas as casas de troca seriam obrigadas a reter um valor de 90 mil Ienes para poderem operar⁷⁴. A legislação deixa aberto espaço para alterações num futuro recente, mas foi muito bem recebida pelos japoneses e pelos mercados do mundo todo. Processo de legalização muito similar ocorreu na Coreia do Sul⁷⁵ e promete ocorrer com algumas diferenças relevantes no caso da Rússia⁷⁶. A África do Sul também traz regulamentação como questão a ser discutida em breve⁷⁷.

Por fim, alguns países veem as criptomoedas como forma de disputa de poder no sistema internacional. A China já foi acusada de adotar técnicas de manipulação do mercado de *bitcoins* para benefício de uma elite⁷⁸, visto que mais que 70% da mineração da criptomoeda vinha do país⁷⁹. Já o Cazaquistão pretende investir nas criptomoedas para se tornar um polo regional desta tecnologia⁸⁰, enquanto a Coreia do Norte parece ter começado uma larga operação de mineração de *bitcoins*, provavelmente, como forma de obter recursos para o país. Há teorias sobre conexões

⁷³ Ao declarar que 67% das pessoas não conseguem cuidar de si mesmas quando investem em criptomoedas, o israelita reafirma o argumento paternalista de o Estado precisar defender seus cidadãos da moeda para chamar por maior regulação de ICO’s: <https://news.bitcoin.com/israeli-official-concerned-about-challenges-with-regulating-icos-and-bitcoin/>.

⁷⁴ A regulação dos *Bitcoins* pelo Japão foi muito bem recebida pelo mercado e fez o preço da criptomoeda disparar: <https://bravenewcoin.com/news/bitcoin-regulation-overhaul-in-japan/>.

⁷⁵ Uma reportagem pode ser encontrada em: <https://news.bitcoin.com/south-korea-legalizes-bitcoin-international-transfers-challenging-traditional-banks/>.

⁷⁶ Embora ainda esteja indecisa em como tratar as criptomoedas, a Rússia pode seguir caminhos parecidos com o Japão em termos d legislação: <https://news.bitcoin.com/russian-politician-central-bank-japan-legalize-bitcoin/>.

⁷⁷ Autoridades se consideram atrasadas neste aspecto frente aos outros países desenvolvidos: <https://news.bitcoin.com/south-africa-will-begin-testing-bitcoin-and-cryptocurrency-regulations/>.

⁷⁸ As criptomoedas podem ser mais ou menos facilmente manipuladas em seu valor por causa de sua razoavelmente pequena liquidez frente às moedas *fiat*: <https://www.bloomberg.com/news/articles/2017-01-16/high-speed-traders-are-taking-over-bitcoin-as-easy-money-beckons>.

⁷⁹ De acordo com pesquisas como em: <https://www.buybitcoinworldwide.com/mining/china/>.

⁸⁰ O país pretende atrair empresas de tecnologia financeira e fomentar projetos com *Blockchain*: <https://news.bitcoin.com/kazakhstan-seeks-to-become-regional-hub-for-cryptocurrency-industry/>.

desse país com o recente ataque mundial do vírus *WannaCry*, que cobrava resgate dos dados em *bitcoins*⁸¹.

É possível perceber alguns padrões econômicos frente à adoção de regulação e abordagens das criptomoedas pelos países. Estados de economia e tradição mais liberal em termos econômicos parecem tender à regulamentação e à adoção das criptomoedas, com o foco em fazê-las parte do gerenciamento estatal dentro do possível, como é o caso do Japão e Coreia do Sul. Países que enfrentam alguma oposição da hegemonia estadunidense ou do ocidente parecem ver nas criptomoedas formas de escapar de tais imposições no âmbito financeiro e podem adotar o uso estratégico das criptomoedas também para evitar futuras sanções econômicas impostas pelo *SWIFT* (DUBOWITZ; FIXLER, 2015), como a Rússia e a Coreia do Norte.

Brasil

A questão das criptomoedas no Brasil reflete o despreparo atual de grande parte dos países, e em especial dos legisladores brasileiros, de sequer começar a entender a questão, embora operadores do Banco Central tenham demonstrado maior entendimento sobre o tema.

Até o início de 2014, as criptomoedas eram definidas como moedas eletrônicas, segundo a lei 12.865 de 09/10/2013. Sua definição constava como: “recursos armazenados em dispositivo ou sistema eletrônico que permitem ao usuário final efetuar transação de pagamento.”⁸² Claramente esta definição não fazia jus às criptomoedas, visto que tal definição no máximo abrangeria as chaves privadas⁸³ para a criptografia da carteira, enquanto as moedas ficariam na rede e não nos dispositivos. Esse primeiro passo grotesco é consertado em 2014, com um comunicado oficial do Banco Central corrigindo a definição anterior, esclarecendo que não está envolvido na emissão nem na proteção ao consumidor, no caso de uso dessas moedas, e avisando que usuários de boa-fé podem ser envolvidos em investigações sobre lavagem de dinheiro⁸⁴. Mais importante ainda é o comentário que ilustra a postura do Banco central até hoje:

⁸¹ Ainda não parece haver muita informação sobre o que realmente está acontecendo, mas pode-se ler uma matéria especulativa em: <https://news.bitcoin.com/north-korea-begins-bitcoin-mining-operation/>.

⁸² A lei pode ser encontrada em: http://www.planalto.gov.br/ccivil_03/ato2011-2014/2013/lei/12865.htm.

⁸³ São códigos primordiais de identificação capazes de gerar endereços a serem usados como pseudônimos.

⁸⁴ É interessante perceber que enquanto o comunicado em português é uma simples e horrorosa página em HTML:

9. No Brasil, embora o uso das chamadas moedas virtuais ainda não se tenha mostrado capaz de oferecer riscos ao Sistema Financeiro Nacional, particularmente às transações de pagamentos de varejo (art. 6º, § 4º, da Lei nº 12.685/2013), o Banco Central do Brasil está acompanhando a evolução da utilização de tais instrumentos e as discussões nos foros internacionais sobre a matéria – em especial sobre sua natureza, propriedade e funcionamento –, para fins de adoção de eventuais medidas no âmbito de sua competência legal, se for o caso. (BRASIL, 2014).

Considerando o tema muito recente para se discutir regulação, e tendo em vista que o volume de transações era irrelevante no Brasil, a postura do Banco Central Brasileiro de esperar mais informações foi prudente, mesmo que isso não tenha impedido a Receita Federal de declarar que moedas virtuais, como *bitcoins*, seriam consideradas “outros bens” e precisariam ser declaradas no imposto de renda e taxadas em 15%, em casos de transações com valores acima de 35 mil reais⁸⁵.

Em 2015, o deputado Aureo Ribeiro (SD-RJ) lança um projeto de lei que só tem comissão instaurada em 30/05/2017 e que mostra total desconhecimento não só do tema que pretendia regular, como do posicionamento do Banco Central Brasileiro a respeito do assunto. O projeto de lei nº. 2.303 de 2015 do deputado Aureo Ribeiro mostra literalmente, na sua primeira frase, que a lei não tem como ser executada:

“PROJETO DE LEI N.º 2.303, DE 2015 (Do Sr. Aureo): Dispõe sobre a inclusão das moedas virtuais e programas de milhagem aéreas na definição de ‘arranjos de pagamento’ sob a supervisão do Banco Central.” (BRASIL, 2015).

Após longas discussões, o projeto de lei objetiva que o Banco Central: regularize tais moedas, mesmo elas já sendo regularizadas para efeitos de imposto de renda como “outros bens” (sendo impossível encaixar criptomoedas como arranjos de pagamentos); faça com que o comércio com *bitcoins* atenda às leis federais de proteção ao consumidor (que já são obrigatórias a comércios legais e impraticável de aplicação em comércios ilegais, com ou sem *bitcoins*); enquadre as moedas virtuais sob a lei de lavagem de dinheiro, como já enunciado no comunicado do Banco Central de 2014. Resumindo, não tem qualquer efeito prático, a não ser o de acalmar o colega deputado Alexandre Valle cujos interesses refletem os riscos estruturais para o Estado, como já

<https://www3.bcb.gov.br/normativo/detalharNormativo.do?method=detalharNormativo&N=114009277>, a versão do comunicado para o exterior é um PDF, repleto de informações de contato e seguindo o modelo oficial para legislação no Brasil: <http://www.bcb.gov.br/pom/spb/ing/IComunicado25306.pdf>.

⁸⁵ Como foi noticiado em diversos jornais: <http://www1.folha.uol.com.br/mercado/2014/04/1436809-brasileiro-tem-que-declarar-bitcoin-ir-pode-ser-cobrado.shtml>.

discutido anteriormente: “No caso de bitcoin, a valorização é absurda, como é que uma moeda dessa pode valer 10 mil reais e ninguém controla, ninguém fiscaliza?”⁸⁶.

O uso de criptomoedas continua modesto no Brasil, mas seu crescimento no mundo, inclusive aqui, pode ter efeitos mais rápidos do que o imaginado, visto que a regulamentação do outro lado do mundo já está afetando os mais distintos mercados espalhados pelo globo.

Conclusão

A tecnologia mostra-se, ao passar dos séculos, como a grande constante nos casos de alteração das estruturas sociais. Seu poder disruptivo já foi internalizado pelo Estado nas faculdades e instituições de pesquisa e desenvolvimento, mas nada impede que surjam novas tecnologias capazes de causar alterações até mesmo na estrutura dos Estados. Frente ao cenário tecnológico e socioeconômico atual, criptomoedas apresentam este valor disruptivo, a ponto de já terem criado novas elites transnacionais e prometendo uma reviravolta na balança do poder. Espero que as projeções aqui feitas sejam consideradas potenciais na tecnologia e *zeitgeist* atual, de forma que tecnologias futuras – como o computador quântico⁸⁷ – podem se mostrar um grande desafio, inclusive para as criptomoedas⁸⁸.

Uma eventual transição para um período de adoção de múltiplas moedas pode ser tanto um momento de liberação e reordenação local de um número cada vez maior de pessoas, quanto um momento de caos. Estados perdendo suporte em um dos pilares, no caso o controle da moeda e impostos, podem tanto se adaptar para novas relações com cidadãos, como os bancos comerciais estão fazendo – buscando criar relações baseadas na experiência e satisfação mútua – ou podem tentar se manter por hipertrofia de seus outros pilares. Acredito que ninguém gostaria de viver em um Brasil com maior uso do monopólio da força ou da burocracia.

É importante perceber o advento das criptomoedas como um momento chave onde seres humanos do mundo inteiro poderão ter acesso a uma escolha negada por séculos:

⁸⁶ Notícia e exclamação podem ser lidas na íntegra em: <http://www2.camara.leg.br/camaranoticias/noticias/ECONOMIA/535524-INSTALADA-COMISSAO-ESPECIAL-PARA-ANALISAR-NEGOCIACOES-COM-MOEDAS-VIRTUAIS.html>.

⁸⁷ Para efeitos de comparação: <http://www.techtudo.com.br/noticias/noticia/2015/12/computador-quantico-do-google-e-nasa-e-100-milhoes-de-vezes-mais-rapido.html>.

⁸⁸ Seu desenvolvimento deixou a comunidade de mineradores sobre alerta: <https://news.bitcoin.com/is-bitcoin-at-risk-as-google-and-ibm-aim-for-50-qubit-quantum-computers/>.

escolher que moeda utilizar e que tipo de ordem social apoiar com cada moeda. A escolha da moeda torna-se um critério tão importante quanto o voto para legitimar a distribuição de poder político. Gestões consideradas ineficientes ou incapazes de satisfazer suficientemente a população provavelmente não contarão com impostos para se manter e precisarão escolher entre continuar no poder por medidas que desgastem ainda mais o poder do Estado na sua gestão – como emitir mais moedas *fiat* para pagar – ou adaptar-se aos pedidos da população.

É possível utilizar criptomoedas para gerar desenvolvimento em locais onde há abundância de recursos e falta de acesso a moedas, podendo ser especialmente aplicada em países subdesenvolvidos e em desenvolvimento, para trazer acesso a bens de mercado para grandes parcelas da população. Criptomoedas possibilitam que ações humanitárias ou contra regimes autoritários possam ser viabilizadas pelas populações locais, e não por ingerência externa, além de fomentar o comércio capilar entre distintas comunidades, contornando qualquer enfrentamento entre seus respectivos Estados, como em Israel e na Palestina. Ao mesmo tempo, criptomoedas podem ser utilizadas para o crime organizado e, por enquanto, podem ser manipuladas com alguma facilidade por grandes atores.

Podemos caminhar para um cenário de uma relação cada vez mais baseada na escolha, satisfação e reciprocidade entre interesses das pessoas e ações dos Estados, de modo que impostos passem cada vez mais a ser reais contribuições para legitimar ou não uma estratégia política. Podemos caminhar para cenários onde o Estado pode representar a manutenção atual de poder, abusar da burocracia e do uso da força, no qual o desgaste entre cidadãos e forças policiais fique cada vez mais tenso⁸⁹, de forma que ninguém realmente ganhe. Muito provavelmente caminharemos para algo entre os dois, mas o importante é que, pela primeira vez, fazer nossa escolha como indivíduos e tentar determinar para que caminho seguiremos nunca foi tão acessível a tantos seres humanos.

⁸⁹ A prática de esconder suas contas dos policiais já é comum, mas conforme o atrito aumenta, as medidas podem se tornar mais drásticas, como uma simples pesquisa no Google pode mostrar novas opiniões: <https://news.bitcoin.com/do-not-help-u-s-cops-seize-your-assets/>; <http://wallstreetexaminer.com/2017/01/global-war-cash-fight-back/>; <https://btctheory.com/>.

Referências

BANCO CENTRAL. **O que é o dinheiro?** Cadernos Educativos. Brasil: Banco Central. 2002. Disponível em <<https://www.bcb.gov.br/Pre/educacao/cadernos/dinheiro.pdf>>. Acesso em <09/08/2017>.

BATISTA, Carter Gonçalves. **Moedas Sociais**. Estadão: 2016. Disponível em <<http://politica.estadao.com.br/blogs/fausto-macedo/moedas-sociais/>>. Acesso em <11/08/2017>.

BARBOSA, Paulo Celso Lavinas. **Bitcoin e moedas fiat: um estudo de volatilidade comparada**. São Paulo: Fundação Instituto de Pesquisas Econômicas, 2016. Disponível em <https://s3.amazonaws.com/academia.edu.documents/46515440/BITCOIN-RISCOS.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1502496866&Signature=iFmGiTs9En58bkeWRJ%2BW2Kav4P4%3D&response-content-disposition=inline%3B%20filename%3DBITCOIN_E_MOEDAS_FIAT_UM_ESTUDO_DE_VOLAT.pdf>. Acesso em <11/08/2017>.

BRASIL. **COMUNICADO Nº 25.306, DE 19 DE FEVEREIRO DE 2014**. Esclarece sobre os riscos decorrentes da aquisição das chamadas "moedas virtuais" ou "moedas criptografadas" e da realização de transações com elas. **Banco Central do Brasil**. Disponível em <<https://www3.bcb.gov.br/normativo/detalharNormativo.do?method=detalharNormativo&N=114009277>>. Acesso em <15/08/2017>.

BRASIL. **PROJETO DE LEI N.º 2.303, DE 2015**. Dispõe sobre a inclusão das moedas virtuais e programas de milhagem aéreas na definição de "arranjos de pagamento" sob a supervisão do Banco Central. **Câmara dos Deputados**. Disponível em <<http://www.camara.gov.br/sileg/integras/1361896.pdf>>. Acesso em <15/08/2017>.

CARLSTEN, Miles; KALODNER, Harry; NARAYANAN, Arvind; WEINBERG, S. Matthew. **On The Instability of Blockchain without the Block Reward**. Arvind Narayanan personal home page, 2016. Disponível em <http://randomwalker.info/publications/mining_CCS.pdf>. Acesso em <13/08/2017>.

CHOUCRI, Nazli; CLARK, David. **Integrating Cyberspace and International Relations: The Co-Evolution**. Massachusetts: Political Science Department, Massachusetts Institute of Technology, 2012. Disponível em <<http://ssrn.com/abstract=2178586>>. Acesso em <15/08/2017>.

DELUCA, Norman J. **Smart banks can win: Leveraging next-generation technology to win the battle for the customer relationship**. Journal of Digital Banking, 2016. Disponível em <<https://www.bottomline.com/application/files/6015/0117/9890/JournalofDigitalBankingSpring2017.pdf>>. Acesso em <14/08/2017>.

DUBOWITZ, Mark; FIXLER, Annie. **'Swift' Warfare: Power, Blowback and Hardening American defenses**. Washington: Foundation for Defense of Democracy, 2015. Disponível em <http://www.defenddemocracy.org/content/uploads/publications/Cyber_Enabled_Swift.pdf>. Acesso em <13/08/2017>.

FILIPPI, Primavera de; LOVELUCK, Benjamim. **The Invisible Politics of Bitcoin: Governance Crisis of a Decentralized Structure**. Internet Policy Review, 2016, v. 5, p. 5.

FRANCO, Pedro. **Understanding Bitcoin: cryptography, engineering and economics**. Cornwall: Willey, 2015. Disponível em <<http://choonsiong.com/public/books/Bitcoin/Understanding%20Bitcoin.pdf>>. Acesso em <11/08/2017>.

FREIRE, Marusa Vasconcelos. **Moedas sociais: contributo em prol de um marco regulatório para as moedas sociais circulantes no Brasil**. Brasília: Repositório UNB, 2011, p. 227 – 231. Disponível em <http://repositorio.unb.br/bitstream/10482/9485/1/2011_MarusaVasconcelosFreire.pdf>. Acesso em <11/08/2017>.

GAVRONKSI, Alexandre Michel; FOPPA, Suellen Barreto. **O Bitcoin como primeira moeda digital internacional**. Internacionalize-se, 2015. Disponível em

<<https://internacionalizese.blogspot.com.br/2015/05/o-bitcoin-como-primeira-moeda-digital.html>>. Acesso em <11/08/2017>.

KAVANAGH, Donncha; MISCIONE, Gianluca. **Bitcoin and Blockchain: a coup d'Etat in Digital heterotopia?** Dublin: University College Dublin Library, 2015. Disponível em http://researchrepository.ucd.ie/bitstream/handle/10197/6841/Heterotopia_CMS.pdf?sequence=1>. Acesso em <11/08/2017>.

KILSZTAJN, Samuel. **O Acordo de BrettonWoods e a evidência histórica. O sistema financeiro internacional no pós-guerra.** São Paulo: Revista de Economia Política Internacional. 1989. Disponível em < <http://www.rep.org.br/pdf/36-6.pdf>>. Acesso em <09/08/2017>.

MATONIS, Jon. **The Implications of Bitcoin: Money without government.** Coindesk, 2014. Disponível em <<https://www.coindesk.com/bitcoin--money-without-government/>>. Acesso em <14/08/2017>.

MCLEAY, Michael; RADIA, Amar; THOMAS, Ryland. **Money Creation in the Modern Economy.** Londres: Bank of England, 2014. Disponível em <<http://www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q102.pdf>>. Acesso em <11/08/2017>.

MURPHY, Gareth. '**Address by Director of Markets Supervision Gareth Murphy at the Bitfin 2014: Digital Money and the Future of Finance Conference**'. Dublin: *BitFin*, 2014. Disponível em < <http://bitcoinsinireland.com/irish-central-banks-gareth-murphy-transcript-from-the-bitfin-conference-in-the-rds-on-3rd-july-2014/>>. Acesso em <15/08/2017>.

NUNES, Wellington. **Elites estatais e desenvolvimento no Brasil recente: os tipos de estratégia e seus agentes.** The Observatory of Social and Political Elites of Brazil, 2015. Disponível em <<http://observatory-elites.org/wp-content/uploads/2012/06/wp-observatory-n.12-2015.pdf>>. Acesso em <14/08/2017>.

SCOTT, Brett. **Visions of a Techno-Leviathan: the politics of Bitcoin and Blockchain.** E-International Relations, 2014. Disponível em <<http://www.e->

ir.info/2014/06/01/visions-of-a-techno-leviathan-the-politics-of-the-bitcoin-blockchain/>. Acesso em <11/08/2017>.

YEE, Andi. **Internet Architecture and The Layer Principle: a conceptual framework for Regulating Bitcoin**. Internet Policy Review: Journal on Internet Regulation, 2014. Disponível em <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2483964>. Acesso em <11/08/2017>.