Bitcoin

Uma tentativa de construção da confiança por meio da tecnologia

MARCELO DE CASTRO CUNHA FILHO

Resumo: O presente artigo tem por objetivo investigar as condições sociais fornecedoras de confiança ao *bitcoin*. Ao contrário das teorias monetárias contemporâneas, que atribuem papel central às instituições formais de direito como garantidoras da confiança em moedas do tipo fiduciárias, este trabalho enxerga como condicionante da confiança no *bitcoin* a sua imersão em uma rede institucional informal latente no ecossistema virtual e no mundo físico.

Palavras-chave: *Bitcoin*. Confiança. Instituições.

Bitcoin: an attempt to build trust through technology

Abstract: This article aims to investigate the social conditions under which trust in bitcoin may thrive. Contrary to contemporary monetary theories that assign central role to formal legal institutions as guarantors of trust in fiat currencies, this paper investigates how bitcoin's immersion into an informal institutional network latent to the virtual and to the physical world is capable of providing the same property to the cryptocurrency.

Keywords: Bitcoin. Trust. Institutions.

Introdução

Recebido em 3/10/18
Aprovado em 20/11/18

Teorias monetárias contemporâneas ressaltam o papel das instituições no processo de consolidação da confiança na moeda. Knapp (2003), por exemplo, é o primeiro pensador contemporâneo a vincular

o conceito de moeda à figura do Estado. Mais recentemente, Goodhart (1998) reforça esse posicionamento ao demonstrar que moedas fortes estão relacionadas a Estados igualmente fortes do ponto de vista fiscal e também do ponto de vista da afirmação de sua soberania nacional. Não é mera coincidência, diz Goodhart (1998), que praticamente todas as moedas contemporâneas são criaturas dos Estados soberanos, e não de uma zona monetária espontânea (*optimal currency area*) sem qualquer suporte do poder coercitivo estatal.

Keynes (1950) demonstra a mesma relação entre instituições e moeda ao distinguir a moeda estatal da moeda bancária privada e ao afirmar que tanto uma quanto a outra dependem fundamentalmente da credibilidade do Estado ao qual estão vinculadas. No caso específico da moeda bancária privada, o autor coloca que a confiança depende, além disso, da solvabilidade das instituições financeiras que a criam e a colocam em circulação. No Brasil, Cortez (2004) endossa essa mesma visão e sugere um nexo de causalidade entre as constantes crises do padrão monetário brasileiro ocorridas nas décadas de 1980 e 1990 e os vácuos institucionais da época que facilitavam a adoção de políticas monetárias corrosivas à moeda vigente.

Apesar da relação descrita na literatura entre instituições e confiança, é preciso reconhecer que um dos instrumentos tecnológicos atuais, o *bitcoin*, que se apresenta popularmente, pelo menos até o momento, como uma moeda, difunde-se aceleradamente[1] pelo globo a despeito da inexistência de institucionalização formal que lhe atribua regime de direito específico, claro e coerente. Ao contrário disso, vê-se que a nova tecnologia se insere num vácuo regulatório e institucional notável. Em lugar nenhum do mundo, há consenso a respeito do seu *status* jurídico, dos seus efeitos legais sobre as relações sociais cotidianas, da regulação dos negócios que envolvem a criptomoeda, dos instrumentos adequados a conformar seu uso em territórios nacionais e entre Estados. Em outras palavras, não há arranjo institucional específico que até agora tenha dado conta de acomodar a inovação tecnológica

[1] A utilização das criptomoedas na economia cresceu vertiginosamente no ano de 2017 e no início de 2018. Dados extraídos da plataforma *blockchain.info* denotam um significativo ganho de confiança nos ativos por parte do mercado e dos usuários de um modo geral. De acordo com um dos gráficos contidos no *site*, é possível visualizar que, em menos de 10 anos de existência, apenas o *bitcoin* atingiu um volume de transações em dólares superior a 5 bilhões nas principais *exchanges* do mundo. Não bastasse isso, o *bitcoin* impulsionou diversos *players* do mercado a adotarem-no como meio de troca por seus serviços e produtos. Entre as grandes empresas que tomaram a iniciativa, inserem-se *Microsoft, Reddit, Overstock.com* etc. Além disso, a própria proliferação de *exchanges* nacionais, com a consequente formalização de postos de trabalho, sugere o surgimento de um novo ramo do comércio que aparenta ter-se estabilizado a despeito da ausência de moldura institucional jurídica que lhe atribua direitos e deveres específicos.

nas economias contemporâneas sem promessa de insegurança e instabilidade.

Entusiastas das criptomoedas, vulgarmente conhecidos como *bitcoiners*, sugerem que a confiança nos ativos virtuais, e no *bitcoin* mais especificamente, deriva fundamentalmente do arranjo tecnológico que lhes possibilita escapar da conformação institucional da moeda convencionalmente adotada por Estados, bancos centrais e instituições financeiras de um modo geral. Alegam tecnoentusiastas da área que é exatamente devido ao desempenho falível das instituições oficiais e reguladas que moedas nacionais observam historicamente repetidas crises de confiança. Segundo a ideologia que sustenta essa visão, os mesmos mecanismos que denotam ganho de confiança nas moedas nacionais são também os responsáveis por permitirem que elas sejam manipuladas ao sabor das paixões políticas momentâneas e sofram, com isso, depreciação e perda de credibilidade.

Em que pese a força do argumento, este trabalho o contradiz por uma razão particular. É possível observar que tanto a configuração da rede do *bitcoin* quanto o modo por meio do qual a criptomoeda é incorporada às atividades sociais do dia a dia sugerem que a confiabilidade e, consequentemente, a escalabilidade do criptoativo estão diretamente relacionadas à densificação de uma rede institucional, se bem que informal, latente nos negócios envolvendo a criptomoeda. Karlstrøm (2014) chama essa rede de materialidades institucionais e aponta que, embora as criptomoedas estejam inseridas num vácuo regulatório aparente, elas não se encontram totalmente desamparadas por instituições. O conceito de instituições ao qual Karlstrøm (2014) se refere não alude apenas a instituições jurídicas formais propriamente. Por instituições, Karlstrøm (2014) se refere a redes formais e informais, acordos ditos e não ditos que conformam igualmente comportamentos e ações em âmbito social e econômico.

Partindo da concepção institucionalista de Karlstrøm (2014), assim como da classificação proposta pelo autor, este artigo apresenta como problema de pesquisa a seguinte indagação: como, mais especificamente, as formas institucionais descritas pelo autor são capazes de reforçar ou diminuir a confiança nos ativos? Por meio de extensa coleta de dados na internet, na literatura especializada e em notícias jornalísticas acerca da estrutura da rede do *bitcoin*, de sua governança e do modo como a criptomoeda se incorpora ao cotidiano popular, pretende-se resolver o problema proposto. Ao final da coleta de dados e da análise dos resultados, conclui-se que, apesar da aparente contradição entre *bitcoin* e instituições, a criptomoeda é ainda fortemente dependente das formas institucionais informais cotidianas para despertar a confiança do público em geral.

Por razões didáticas, divide-se o presente trabalho em mais três seções, além desta introdução. Na seção 1, será descrita a ideologia construída ao redor da criptomoeda e conhecido o principal argumento de sustentação da confiança no ativo por meio de sua arquitetura tecnológica. Na seção 2, será feito um breve excurso sobre o papel das instituições como deflagradores de confiança. Na 3, será apresentada a coleta de dados sobre a tecnologia do *bitcoin*, sistematizada de acordo com a classificação adotada por Karlstrøm (2014). Por fim, atesta-se que, se não pelos mecanismos convencionais de regulação jurídica, pelo menos por meio dos mecanismos informais e simbólicos de conformação de comportamentos, a confiança na criptomoeda encontra sustentação ou, simetricamente, motivo de declínio.

1 *Trust-free bitcoin* – a ideologia construída em torno da criptomoeda

No ano de 2008, pouco tempo após o irrompimento da crise financeira dos Estados Unidos, foi anunciada, em um fórum de discussão da internet, a concepção de uma moeda virtual, denominada *bitcoin*, cuja mais destacada propriedade consiste no fato de ela circular de maneira inteiramente *peer-to-peer*[2]. Ao contrário de uma moeda eletrônica[3], que somente pode ser transferida por meio da intermediação de uma autoridade central que a emite, o *bitcoin* é transferido diretamente de usuário a usuário sem ter de passar pelos procedimentos internos e pela fiscalização de qualquer instituição. No lugar de um terceiro intermediário que operacionaliza as trocas de valor, a criptomoeda é transmitida por meio de um protocolo criptográfico que obedece a regras matemáticas pré-programadas.

Seu modo de funcionamento não intermediado ensejou o entendimento de que, em virtude da eliminação do terceiro da cadeia de transferência de valor e da inserção, em seu lugar, de um procedimento tecnológico semiautomatizado, surgia uma moeda que excluía do seu modelo de governança todo e qualquer tipo de interferência política externa à sua lógica de funcionamento. A transferência do controle e da gestão da moeda do âmbito de uma instituição organizada social e juridicamente para o âmbito de um processo matematicamente controlado representou, em última análise, uma estratégia de se insular a moeda do campo da política e do direito mais especificamente. Por conta desse entendimento, associado ao reconhecimento de um processo gradativo de perda de credibilidade pelo qual passam a política e as instituições de direito no mundo de um modo geral[4], divulgou-se amplamente

---

[2] De acordo com Twomey (2013, p. 88), o termo *peer-to-peer* se refere tecnicamente ao processo segundo o qual "the internet-based currencies are exchanged on software in which data is transferred from one peer to another and where each workstation has equivalent capabilities and responsibilities".

[3] O conceito de moeda eletrônica no Brasil é fornecido pela Lei Nacional de Pagamentos (Lei nº 12.865/2013) (BRASIL, [2013]) e nada tem a ver com o conceito de moeda virtual. A moeda eletrônica, de acordo com a Lei, consiste em "recursos armazenados em dispositivo ou sistema eletrônico que permitem ao usuário final efetuar transação de pagamento". Por força da redação do artigo, moeda eletrônica é denominada exclusivamente em unidade de conta nacional. No caso do Brasil, o Real. Moedas virtuais, por outro lado, são todo o tipo de recursos digitais não denominados em unidade de conta nacional, assim como o *bitcoin*. Por falta de legislação específica, moedas virtuais não são consideradas método de pagamento no Brasil.

[4] Pesquisas conduzidas pelo Pew Research Center em 2017 demonstram que o nível de confiança que a população mundial deposita nos governos de seus respectivos países decresceu consideravelmente nos últimos anos. O gráfico disponível no *site* da referida instituição (PUBLIC…, 2017) revela a queda de confiança no governo americano por parte dos cidadãos do país de mais de 50% desde a década de 1950. Outro gráfico disponível também na página da Pew Research Center demonstra que países com menor

na mídia a criação de uma moeda cujas propriedades inspirariam a confiança que moedas administradas por uma autoridade central não conseguem inspirar. Tratava-se de uma moeda tão confiável que, paradoxalmente, eliminaria a necessidade de ser ela mesma objeto de confiança[5].

No cerne desse pensamento, escondia-se a ideia de que a moeda convencional tem seu modo de funcionamento e governança determinados por instituições falíveis, como bancos centrais e governos, os quais podem, ao comando da política, inflacioná-la, deflacioná-la, confiscá-la, retirá-la de circulação etc., ao passo que o sistema *bitcoin* teria delegado a gestão da criptomoeda[6] a máquinas incapazes de alterar as regras do protocolo segundo as quais ela é emitida e transacionada (ATZORI, 2015, p. 2). Ao contrário do que representa a administração da moeda conduzida por seres humanos, a gestão monetária conduzida por meio da infalibilidade matemática teria o condão de subtrair a circulação da moeda e o seu funcionamento do "mal" que historicamente os colocou em descrédito e os fez padecer da desconfiança generalizada, a saber, a política (DODD, 2017, p. 3).

A viabilidade do projeto anunciado deveu-se ao desenvolvimento de uma tecnologia subjacente ao *bitcoin* que, uma vez aplicada à circulação de um *token* virtual, daria materialidade à ideia da moeda desnacionalizada, despolitizada, despartidarizada (DE FILIPPI; LOVELUCK, 2016, p. 3). Trata-se da já referida *blockchain*, que, à semelhança de um livro-razão digital, equivale essencialmente a um banco de dados, cuja função precípua consiste em registrar a origem e a movimentação de cada unidade ou fração de *bitcoin* (SWAN, 2015, p. 2). Diferentemente, porém, de um arquivo de registro usual, a *blockchain* não é manipulada por uma autoridade central em que se confia (*trusted third party*). Sua atualização é exercida por meio do trabalho técnico computacional de servidores distribuídos, também chamados de mineradores, que têm poderes de ingerência limitados sobre a tecnologia em virtude do modo de funcionamento matematicamente controlado de acordo com o qual ela funciona (SWAN, 2015).

---

crescimento do PIB nos últimos anos, como Brasil, Argentina, Espanha, França e México, apresentam menores taxas de confiança no governo e na política (WIKE; SIMMONS; STOKES; FETTEROLF, 2017).

[5] Mais acertado seria referi-la por meio do termo em inglês *trust-free*, por falta de tradução mais precisa.

[6] Uma definição mais precisa de criptomoeda pode ser encontrada no seguinte fragmento: "bitcoin and bitcoin-like currencies should be defined in legislation as 'internet-based currencies that are not issued by a legal entity and are not confined to a specific virtual world'. Specific virtual world 'relates to situations where video games use a system whereby you can use in-game credits to buy extra content exclusively within the game'"(TWOMEY, 2013, p. 88).

Por meio do registro desintermediado e semiautomatizado de cada unidade ou fração de *bitcoin* foi possível à rede criar um mecanismo de verificação e de controle das criptomoedas de modo a reduzir tendencialmente a zero a possibilidade de qualquer agente, seja ele um servidor ou não, criar, duplicar[7], excluir, confiscar, redirecionar os valores com supostas características monetárias (SWAN, 2015). Por essa razão, a *blockchain* serve à rede *bitcoin* mais como uma ferramenta de contagem das criptomoedas e de transcrição do histórico de transações. Para além disso, a tecnologia age como um mecanismo de segurança do sistema e, indiretamente, de manutenção da confiabilidade nos ativos. O modelo de funcionamento da *blockchain*, baseado em criptografia de rede distribuída, representou a novidade do sistema de registro digital e o que o distinguiu de iniciativas similares antecessoras.

Apesar de toda a sofisticação técnica e garantia de segurança do sistema, Vigna e Casey (2015, p. 155) apontam que uma única hipótese ameaçaria a integridade e a configuração original de uma rede distribuída como a do *bitcoin*. Conhecida na literatura como ataque dos 51%, a possibilidade de risco se concretizaria quando pelo menos 51% da capacidade de processamento computacional global do sistema[8] fosse atingida por um único servidor central ou, então, por diversos servidores associados, e fosse direcionada contra a rede com a finalidade de nela provocar alguma alteração. Nesse caso, em que a capacidade de processamento computacional reunida suplantasse o patamar de 51%, a possibilidade de modificação estrutural da rede de acordo com uma nova configuração do sistema (VIGNA; CASEY, 2015, p. 151) estaria probabilisticamente dada. Como, no entanto, a possibilidade de se somar tamanho esforço computacional é improvável em virtude do alto poder agregado que o sistema reúne em face da atuação de mais de 10.000 servidores[9] de mineração espalhados pelo mundo, admite-se, então, a mínima chance de adulteração da rede.

Tendo reunido, portanto, as características mencionadas, em especial o recurso à criptografia de rede e a arquitetura de rede distribuída, o *bitcoin* deu origem não apenas a um mecanismo de segurança do sistema resistente a fraude e a ataques *hackers*, mas, para além disso, sua arquitetura distribuída foi responsável pela criação de um sistema que prescinde da coordenação de uma autoridade central cuja função consiste na atividade de validação e de autenticação das transações. Por conta da atuação de mineradores independentes, esse trabalho é desempenhado de forma distribuída, sem vínculo com nenhum Estado, empresa ou associação. Por essa razão particularmente, o sistema *bitcoin* alimentou, de acordo com

[7] De acordo com Swan (2015, p. 2), um dos maiores problemas resolvidos pela *blockchain* foi o dilema do duplo-gasto. Até o advento da *blockchain*, não era possível transferir valor por meio virtual sem que uma autoridade central em quem se confia (*trusted third party*) tivesse de registrar cada transação como forma de controle da escassez dos ativos. Esse fenômeno decorria da natureza dispersível dos bens na internet. O dinheiro, assim como qualquer ativo virtual, podia ser infinitamente multiplicado. A única forma de controlar sua escassez passava necessariamente pelo controle de um intermediário responsável por verificar cada transação. O poder de gestão sobre o registro dado ao centralizador não impedia, no entanto, ingerências arbitrárias de sua parte na dinâmica de circulação dos ativos. Com a *blockchain*, todavia, o controle "desinteressado" tornou-se possível na medida em que a tecnologia substitui o papel da autoridade central por protocolos criptográficos que não comportam desvio.

[8] Por capacidade de processamento global do sistema, entende-se grosseiramente a força computacional bruta que todos os servidores juntos entregam à rede para a realização do trabalho de manutenção do sistema.

[9] No momento da elaboração deste texto, 10.565 servidores de mineração conectavam-se à rede *bitcoin*. Esse número varia constantemente, tendo em vista que a entrada e a saída de novos servidores são livres e independem de permissão ou burocracia. Informação a cada 24 horas sobre a quantidade de mineradores conectados à rede está disponível em: https://bitnodes.earn.com. Acesso em: 5 dez. 2018.

Dodd (2017), duas ideias há muito difundidas na literatura sobre moeda. De um lado, a ideia da instituição do dinheiro desvinculada da atuação e da ingerência das instituições financeiras e, de outro, da intermediação do Estado e da política *lato sensu*.

A desintermediação promovida pela tecnologia levantou a hipótese de uma nova forma de produção do dinheiro não mais calcada no modelo de multiplicação monetária resultante do sistema de reservas fracionárias (DODD, 2017). A constituição de uma rede cuja lógica de funcionamento obedece a regras pré-determinadas teria dado ensejo ao surgimento de um serviço financeiro alternativo ao sistema bancário tradicional e substitutivo da política monetária conduzida indiretamente por bancos comerciais e instituições multiplicadoras de crédito bancário. Ao fixar uma quantidade limite de 21 milhões de unidades não sujeitas à multiplicação, o protocolo da rede teria supostamente possibilitado a emergência de um sistema monetário virtual semelhante ao da moeda lastreada em ouro, cuja quantidade não se encontra sob o poder de manipulação do administrador.

Além disso, a desintermediação teria provocado um efeito ainda mais relevante, segundo Dodd (2017). De acordo com o autor, muito da ideologia que sustenta a escalada do *bitcoin* nos primeiros anos de sua trajetória está intimamente relacionada a esse segundo aspecto especificamente. Parte do apelo que ganhou a criptomoeda se deve ao fato de muitos adeptos terem enxergado na tecnologia um recurso alternativo à utilização da moeda nacional. Diferentemente das unidades monetárias-padrão, que são criadas, sustentadas e administradas pelo Estado por meio de todo um conjunto de regras e de instituições, da política de juros, da política cambial, de reservas compulsórias etc., a estrutura de governança do *bitcoin* é constituída de forma independente e paralela aos mecanismos convencionais de controle da moeda. Isso por si só a preveniria, alegam os tecnoentusiastas em geral (DODD, 2017), de ser manipulada pela conveniência política de governos e autoridades públicas.

Reduzida a condições de operação controladas matematicamente pela engenharia do sistema de servidores distribuídos, que não apenas previne a fraude e a manipulação da rede, mas, além disso, serve como condição técnica de viabilidade de um projeto de transferência de valor *peer-to-peer* em meio virtual, a criptomoeda apresentou-se ao mundo mais do que meramente como um ativo transacionável na internet. Sua estrutura tecnológica deu azo ao entendimento de que um sistema monetário sustentável e emancipado das influências de poder das instituições financeiras e dos Estados nacionais houvera sido criado. Graças ao insulamento da influência política, incluindo a regulação estatal, o

bitcoin seria posteriormente considerado uma moeda cuja governança seria tão transparente e previsível que inspiraria a confiança que autoridades centrais e governos não seriam capazes de prover aos ativos que administram (MCGINNIS; ROCHE, 2017). A eliminação da política do campo monetário e a entrada das máquinas e da matemática em seu lugar teriam criado as condições de possibilidade de uma moeda inteiramente *trust-free*.

2 O papel das instituições como deflagradoras da confiança

Instituições têm sido concebidas pela literatura como verdadeiras propagadoras de confiança social (PUTNAM, 2000; HARDIN, 1996; WILLIAMSON, 1993; ZUCKER, 1986). Seja qual for a vertente adotada pela pesquisa, reconhece-se o papel das instituições como geradoras de expectativas positivas ou, simetricamente, negativas sobre a conduta de uma pessoa, de um grupo de pessoas ou sobre outras instituições. De acordo com o ramo da economia contemporânea conhecido como Nova Economia Institucional, as instituições funcionam como verdadeiros incentivos à consolidação da confiança, na medida em que elas geram expectativas sociais que agregam em previsibilidade ao agente que calcula custos e benefícios de se engajar em relações econômicas cotidianas (WILLIAMSON, 1993; HARDIN, 1996; GOOD, 1988). Por outro lado, a vertente sociológica que investiga o mesmo fenômeno ressalta que a construção da confiança por meio das instituições se dá porque essas estruturas criam significados sociais mais ou menos homogêneos que vão se incorporando ao dia a dia das pessoas e, com isso, direcionam comportamentos de maneira mais ou menos esperada (ZUCKER, 1986; MÖLLERING, 2006). Por razões metodológicas, este trabalho parte das premissas dessa última vertente para investigar o processo de construção da confiança no *bitcoin*.

Um dos estudos pioneiros sobre a relação entre confiança e instituições é de autoria de Zucker (1986), para quem os níveis de confiança societária em determinados setores da economia podem ser verdadeiramente manipulados a depender da configuração das instituições erigidas para regular as atividades afetadas. Partindo das ideias de Garfinkel sobre confiança, Zucker (1986, p. 6) define o termo como a expectativa dos atores sociais de levarem em consideração as coisas como elas normalmente são (*things as usual*) ou, então, de dar por garantido (*take for granted*) determinado estado de coisas da ordem social. De acordo com Zucker (1986, p. 8), a consolidação dessa disposição comportamental é

composta por duas variáveis sociais. A primeira delas, as expectativas de pano de fundo (*background expectations*); a segunda, as expectativas constitutivas (*constitutive expectations*).

Expectativas de pano de fundo dizem respeito aos entendimentos e aos significados não questionados e compartilhados na sociedade, que fornecem um horizonte comportamental comum a todos os participantes da mesma rede comunitária. Sem o compartilhamento desses significados, explica Zucker (1986), a vida em sociedade seria praticamente impossível já que eles representam uma forma de estruturação social com base na qual os indivíduos constroem sentidos, elegem objetivos, traçam estratégias para suas vidas. Configura expectativa de pano de fundo, por exemplo, a aceitabilidade do dinheiro como meio de troca na economia. Expectativas constitutivas, por outro lado, dizem respeito às regras do contexto e às situações particulares do dia a dia. São, por conta disso, mais sensíveis à variação. Exemplos de expectativas constitutivas são as regras de utilização do dinheiro, do cheque, de ações. Também funcionam como exemplo as regras relacionadas ao comércio, ao consumidor etc.

De acordo com Zucker (1986), quanto mais uma expectativa social, seja ela de que natureza for, se institucionaliza, tanto mais ela se dissemina e penetra no tecido social e, por consequência, tanto mais a confiança aumenta no nível da comunidade. Embora expectativas de pano de fundo sejam mais ou menos institucionalizadas e dadas como certas no cotidiano popular, as expectativas constitutivas podem ser reforçadas à medida que mecanismos de institucionalização artificiais trabalhem para alcançar esse fim. Por institucionalização, Zucker (1986) entende um processo de reconstrução e de autonomização de significados sociais como componentes estruturantes do "mundo externo", e não mais apenas como convicções pessoais do agente que confia. Nas palavras da autora,

> This process of reconstruction has been called institutionalization: the process of redefining acts as exterior when intersubjective understanding causes them to be seen as part of the external world and objective when they are repeatable by others without changing the common understanding of the acts (ZUCKER, 1986, p. 11).

Instrumentos formais de direito como a lei, a regulação ou o contrato representam mecanismos eficazes de criação e disseminação de significados e de expectativas em comum nesse sentido. Não tanto pelo fato de esses instrumentos atuarem como garantidores ou executores (*enforcers*) de um estado de coisas, mas pelo fato de representarem sistemas de regras que constroem significados em comum que definem, por

sua vez, expectativas, papéis sociais e modos de comportamento culturalmente disseminados (MÖLLERING, 2006, p. 360). Contudo, não apenas mecanismos formais de direito são capazes de disseminar significados compartilhados e expectativas em comum. Também a cultura de uma organização, seu método de governança (ainda que não formalizado), acordos informais, relações pessoais, regras sociais, *standards* técnicos, enfim, toda a rede organizacional de um contexto social é capaz de criar condições que fornecem significados compartilhados e expectativas sociais que promovem, como consequência, o aumento de confiança social (MÖLLERING, 2006, p. 362).

Às condições mencionadas, Karlstrøm (2014) chamou de materialidades institucionais e fez perceber que o ecossistema das criptomoedas e, sobretudo, do *bitcoin*, embora carente de instituições formais de direito que lhe deem conformação específica, é fortemente imerso em condições desse tipo. As materialidades institucionais a que se referiu Karlstrøm (2014) dizem respeito a todas aquelas condições do mundo físico, e não do espaço virtual, que funcionam como instrumentos de viabilidade da arquitetura do sistema *bitcoin*, de sua incorporação aos mercados e ao cotidiano popular, e que, por essa razão, criam um sistema cultural repleto de significado e de expectativas em relação ao uso da criptomoeda. Divididas entre materialidades procedimentais, de mercado e sociais, todas as formas concebidas pelo autor prestam-se a descrever, em última análise, a maneira como o *bitcoin* se institucionaliza no espaço físico, se interconecta com a economia e com o mundo ao seu redor e dissemina, por conta disso, expectativas mais ou menos compartilhadas a respeito da tecnologia.

Dedicado a investigar a relação entre essa rede de significado institucionalizada e o aumento ou decréscimo da confiança no *bitcoin*, este trabalho faz um levantamento descritivo de cada uma dessas condições e analisa como elas podem concorrer para fornecer um ambiente de confiança ou, simetricamente, de desconfiança ao investimento no *bitcoin*, seja ele formalmente considerado uma moeda ou não. Para a elaboração do relatório descritivo, a pesquisa baseou-se em levantamento de dados na internet, em periódicos especializados e em matérias jornalísticas. Todos os dados, como será visto a seguir, foram sistematizados aproveitando-se a classificação de Karlstrøm (2014), que dividiu, conforme explicado, as referidas condições materiais de produção de significados entre materialidades procedimentais, de mercado e sociais.

3 Imersão institucional do *bitcoin*

3.1 Materialidades procedimentais

A primeira condição material à qual o *bitcoin* se encontra associado diz respeito ao seu suporte técnico, a começar pela função criptográfica empregada pela tecnologia. Sabe-se que o modelo de criptografia adotado, que funciona com base na função algébrica denominada SHA-256, é resultado de anos de pesquisas envolvendo matemática avançada e ciência da computação (KARLSTRØM, 2014). Apesar de a função matemática ter sido aclamada inquebrantável até o momento, o que garantiria ao sistema elevada proteção contra fraude, não se pode excluir a hipótese de falha ainda que tendente a zero. Embora essa possibilidade seja remota hoje em dia, é possível que, com o desenvolvimento da computação quântica, que já começa a se tornar uma realidade possível (GILES; KNIGHT, 2018), a probabilidade de ameaça à função SHA-256 au-

mente para níveis consideráveis (QUANTUM…, 2017). O curso natural do desenvolvimento tecnológico, inclusive, já tornou obsoletos modelos criptográficos anteriores ao do *bitcoin* que foram durante muito tempo considerados indestrutíveis. Muito utilizada por empresas de segurança virtual, a função criptográfica SHA-1, anterior ao modelo sob análise, já foi considerada inviolável do ponto de vista técnico até o início do ano de 2017 quando especialistas em criptografia descobriram uma colisão no sistema que ameaçava sua manutenção como mecanismo de segurança de *sites* e de sistemas virtuais em geral (GOOGLE…, 2017).

Além disso, mesmo desconsiderando a hipótese incerta sobre o futuro do desenvolvimento tecnológico, não seria possível atribuir ao modelo de criptografia utilizado pelo *bitcoin* indestrutibilidade total. Embora não se trate propriamente de uma falha que ameaça a integridade do sistema, Bos, Halderman, Heninger, Moore, Naehring e Wustrow (2014) provaram graficamente a possibilidade de pequenos *bugs* na função adotada que devem ser constantemente reparados por desenvolvedores habilitados a trabalharem sobre o código-fonte do *bitcoin*. Um desses defeitos diz respeito à colisão de senhas de carteiras virtuais[10], fato que inviabilizaria o reconhecimento das aplicações pela rede. Nesse caso, uma vez movimentadas unidades ou frações de *bitcoins* para a carteira contaminada, as criptomoedas se perderiam para sempre visto que dessa carteira não haveria como remeter fundos.

Além dos problemas relacionados à sustentação da criptografia do *bitcoin*, há pelo menos mais um conjunto de fatores externos à rede que dá viabilidade técnica ao sistema. Relacionado à manutenção da *blockchain* especificamente, esse conjunto de fatores diz respeito às materialidades técnicas necessárias para se fazer rodar a engrenagem de autenticação e de registro distribuídos da tecnologia. Como se sabe, a composição da rede é formada por servidores espalhados pelo mundo, os quais não precisam de qualquer permissão para agregar força computacional bruta ao sistema para, com isso, colaborar com o trabalho de sustentação da rede. No entanto, embora a rede seja tecnicamente aberta à participação de qualquer indivíduo ou empresa, é preciso que requisitos materiais específicos sejam satisfeitos.

Em primeiro lugar, o trabalho de mineração requer uma rede de computadores em operação que se comunicam por meio do protocolo *bitcoin*. Em virtude de a atividade obedecer a um procedimento matemático imposto pelo código do *software* cujo grau de dificuldade aumenta com o passar do tempo (NAKAMOTO, 2008), observou-se,

[10] Carteiras virtuais são aplicativos de internet que servem para armazenar criptomoedas.

como decorrência natural, que o poder computacional necessário para a realização da atividade aumentou proporcionalmente. Como consequência, o exercício da atividade de mineração passou a exigir o uso de máquinas cada vez mais potentes e especializadas no serviço (VIGNA; CASEY, 2015). Computadores do tipo *desktop* se tornaram, por essa razão, incapazes de agregar poder computacional suficiente para o trabalho de mineração (GERVAIS; KARAME; CAPKUN; CAPKUN, 2014).

Devido a essa mesma questão, não apenas a capacidade das máquinas teve de aumentar para dar vazão à realização da atividade. Além da adaptação do aparato tecnológico ao desenvolvimento da mineração, o que por si só já funciona como uma restrição à entrada de novos participantes na disputa[11], o consumo de energia elétrica necessário ao funcionamento do maquinário também teve de ser ajustado. Máquinas que demandam maior atividade em menor tempo demandam cada vez mais energia elétrica para funcionar (HERN, 2018). Essa característica das máquinas não é apenas incidental. Ela faz parte da própria concepção do projeto *bitcoin*. A adição de energia elétrica para o desenvolvimento da atividade de mineração gera um custo econômico para a produção de uma unidade da criptomoeda, sem o qual o ativo pouco valor teria devido à facilidade da sua extração (VIGNA; CASEY, 2015).

Tendo sido incorporados à sistemática de funcionamento do sistema de modo intencional ou não, tanto a conectividade de supercomputadores à rede quanto o alto consumo de energia elétrica representam condições materiais de funcionamento do *bitcoin*. Faz parte, portanto, da viabilidade técnica da rede o emprego de materialidades externas ao ecossistema virtual. A dependência de condições de viabilidade técnica exteriores ao âmbito da tecnologia não afasta por si só o caráter desintermediado da rede. No entanto, ela demonstra que, mesmo em se tratando de uma rede que promete eliminação do intermediário, ela, ainda assim, somente ganha existência quando imersa numa teia de serviços e produtos muitas vezes proibitivos ao consumidor médio, organizada por terceiros intermediários. Diferentemente da ideologia construída em torno do *bitcoin*, que predizia o caráter infalível da tecnologia, vê-se, por outro lado, que até mesmo a viabilidade técnica do sistema está sujeita ao cumprimento de condições de possibilidade variáveis ao longo do tempo. Com isso, não se está querendo dizer que o sistema tem falhas que corrompem sua integridade técnica, mas, sim, que seu pro-

[11] No caso do *bitcoin*, o poder de processamento exigido hoje em dia para uma máquina agregar força computacional suficiente para minerar é tão alto e dependente de tecnologia especializada que a atividade em si tornou-se um negócio altamente competitivo e acessível apenas a entrantes com grande capacidade de investimento (VIGNA; CASEY, 2015).

cesso de institucionalização é diretamente dependente da rede técnica que serve como pano de fundo do sistema.

3.2 Materialidades de mercado

Não apenas de materialidades técnicas depende a existência e disseminação do *bitcoin*. Para além dos dispositivos tecnológicos por meio dos quais a criptomoeda ganha funcionalidades específicas, há também ao seu redor uma arquitetura social programada para lhe dar usabilidade. Esta, porém, ao contrário das materialidades procedimentais, não está localizada em nenhum dispositivo tecnológico. As materialidades de mercado se referem à organização social de pessoas que se formam em torno da rede para lhe conferir aplicabilidade prática no cotidiano dos usuários (KARLSTRØM, 2014). De modo bastante sintético, neste trabalho as materialidades de mercado foram divididas em (1) comunidade, e (2) serviços facilitadores do manejo da rede.

A comunidade referida é composta tanto por desenvolvedores quanto pelos já mencionados mineradores. Ambos os grupos podem ser considerados em alguma medida responsáveis pela estrutura de governança do *bitcoin*, muito embora a rede tenha sido concebida com o propósito de eliminar qualquer tipo de governabilidade diferente das regras de funcionamento originalmente programadas. O grupo de desenvolvedores, ao contrário do que propõe o desenho técnico da arquitetura do *bitcoin*, é restrito a alguns poucos participantes. Os mineradores, por outro lado, embora prescindam de permissão para atuarem como tais, são filtrados por uma série de condicionantes de ordem técnica como já exposto anteriormente. Veja-se cada um dos grupos e por que eles indiretamente compõem o pano de fundo da governança do *bitcoin*.

Qualquer que seja o código de computador, ele demanda atualizações com o passar do tempo. Algumas para consertar pequenas falhas, outras para introduzir modificações estruturais que lhe emprestem melhor aplicabilidade na vida cotidiana dos usuários. Em geral, códigos *open-source*, como o do *bitcoin*, são depositados em um repositório ao qual têm acesso algumas pessoas apenas. No caso da rede, seu código-fonte fica hospedado na plataforma GitHub, que impõe uma série de regras aos integrantes para execução de modificações no protocolo do *bitcoin* (OERMANN; TÖLLNER, 2015). São três as categorias de participação que a plataforma permite: a de administradores da organização, a de membros (*development team* ou *core developers*) e a de não membros. Administradores são aqueles responsáveis por permitir ou excluir a participação de não membros basicamente. Até o momento, é incerto quem são os responsáveis por essa tarefa, uma vez que a plataforma não

exibe seus nomes. O grupo de membros, por outro lado, é composto por apenas sete pessoas. Todas elas são, de alguma maneira, entusiastas e especialistas que colaboram com a tarefa de melhoramento do código desde o surgimento da criptomoeda. São elas, ao fim e ao cabo, as incumbidas de aceitar ou recusar qualquer modificação no código do *bitcoin*. O grupo de não membros, por fim, é formado por pessoas aceitas na plataforma, hoje em número de 371 (BITCOIN…, c2018), que sugerem modificações do código ao grupo dos membros.

Segundo Oermann e Töllner (2015, p. 12), é importante conhecer a estrutura de modificação em nível fundamental do protocolo, pois ela desnuda o modelo de institucionalização centralizada de uma rede desenhada para funcionar descentralizadamente. Apenas para se ter uma ideia da concentração de poder que detêm os membros (*development team* ou *core developers*), basta pensar que qualquer modificação no código, incluindo as de nível estrutural, passa necessariamente por sua aprovação. No geral, expõem Oermann e Töllner (2015), reparos de pequenos *bugs* são feitos por seus integrantes individualmente sem que os demais sejam sequer consultados. Por outro lado, qualquer alteração que afete a natureza da tecnologia em nível estrutural deve ser decidida por consenso (OERMANN; TÖLLNER, 2015, p. 9). Além disso, é o grupo dos *core developers* o responsável por avaliar as sugestões de melhoramento feitas pelos não membros. Quando alguma sugestão é feita, ela deve igualmente passar pelo crivo do time para que seja implementada.

Uma outra forma de participação nas decisões de modificação da rede se dá pelo chamado *Bitcoin Improvement Proposal* (BIP) (OERMANN; TÖLLNER, 2015, p. 10). Diferentemente de um encaminhamento de sugestão concreta de alteração, o BIP consiste em uma proposta (*concept paper*) de criação de novas funcionalidades para o sistema *bitcoin* que sequer foram desenhadas em linhas de códigos. Diante da submissão de um BIP, decidem os membros, por maioria simples, acerca da sua admissibilidade para análise ou não. Uma vez admitida, ela será analisada e, caso se torne eventualmente um projeto concreto de modificação do protocolo, deverá passar pelos mesmos critérios de alteração que qualquer mudança substancial. Como forma de se garantir a publicidade das iniciativas, todos os BIPs, assim como todas as sugestões no geral, são gravadas nos fóruns de discussão da GitHub e no site da *Bitcoin Foundation* (OERMANN; TÖLLNER, 2015, p. 9).

Não apenas o seleto grupo de desenvolvedores influencia a concepção dos projetos incorporados ao *bitcoin*. Também uma estrutura centralizada de tomada de decisões pode ter grau de ingerência razoável sobre a tecnologia. Trata-se da *Bitcoin Foundation*, acima referida, que foi criada com os propósitos de, entre outros, promover a uniformização de

políticas sobre o protocolo e proteger a integridade da rede. Constituída por uma diretoria (*Board of Directors*) composta por sete membros, um dos quais indicado por membros fundadores, três por membros que compõem a categoria das empresas que desenvolvem produtos baseados em *bitcoin* para o mercado e mais três por membros individuais da fundação, não se sabe ao certo qual o grau de influência que ela exerce sobre as modificações do protocolo da rede uma vez que suas decisões não são publicadas (OERMANN; TÖLLNER, 2015, p. 12). De modo direto, evidentemente, a fundação não tem o poder de influenciar a rede segundo lhe convenha. No entanto, sabendo que quatro membros do *development team* da GitHub compõem o *Board* da fundação e são parcialmente financiados pela mesma instituição (VIGNA; CASEY, 2015, p. 149), então não se descarta a hipótese de influência indireta (OERMANN; TÖLLNER, 2015, p. 11).

É importante, contudo, esclarecer que qualquer alteração promovida no protocolo, seja ela influenciada ou não por forças desconhecidas, somente passa a vigorar mediante a aceitação dos mineradores, que, juntamente com os desenvolvedores, integram a referida comunidade. São os mineradores que decidem atualizar o código que roda em suas máquinas e são eles, em última análise, os responsáveis por dar aplicabilidade às alterações concebidas e executadas pelos membros do *development team*. Caso todos os mineradores decidam fazê-lo nos exatos termos propostos, então passam a vigorar as alterações sugeridas. No entanto, se parcela razoável do grupo decide não fazê-lo ou, então, decide executar reformas diferentes das planejadas, daí emerge a possibilidade de uma divisão na rede (VIGNA; CASEY, 2015, p. 149). O efeito prático desse processo é a criação de uma segunda rede, diferente da original, com regras de funcionamento próprias.

Além do poder de criar uma nova rede, os mineradores têm ainda o poder de afetar a configuração original da rede padrão. Da mesma forma que a reunião de 51% da capacidade de processamento global de todo o sistema pode provocar alterações fraudulentas na rede, ela também pode fazê-lo para fins de atualização e modificação de qualquer natureza. O princípio é basicamente o mesmo. No caso de reunião de poder de processamento bruto acima dos 51%, maior será a capacidade de o(s) servidor(es) que congrega(m) tamanha força computacional agregar(em) poder computacional ao sistema para rodá-lo (VIGNA; CASEY, 2015). Nesse caso, aumenta a possibilidade de os desviantes modificarem estruturalmente a rede.

Esse aspecto do sistema é particularmente sensível no que se refere à governança da tecnologia. Concebida para escapar à intermediação de uma autoridade centralizadora, a comunidade de mineradores revela

invariavelmente traços característicos de um intermediário na medida em que promove constantemente alterações no protocolo mediante a formação de maioria. Muito embora a rede tenha sido criada para evitar a concentração de poder, a hipótese aventada não é meramente teórica. Na tabela, observa-se que a rede já promove acidentalmente uma concentração geográfica de mineradores. A maioria dos mineradores espalhados pelo mundo se concentra majoritariamente nos Estados Unidos, na China e na Europa.

Tabela

Concentração de servidores (mineradores) por país

Distribuição global de servidores de *bitcoin*	
12.153 servidores alcançados na data de 17 de março de 2018 às 16h 48min 56s	
Lista dos 9 maiores países em *ranking* de concentração de servidores	
Estados Unidos	2674 (22%)
China	2175 (17,9%)
Alemanha	1985 (16,33%)
França	686 (5,64%)
Holanda	502 (4,13%)
Reino Unido	417 (3,43%)
Canadá	406 (3,34%)
Rússia	387 (3,18%)
Singapura	230 (1,89%)

Fonte: Global… (c2018).

Contudo, mais alarmante do que a concentração de mineradores por país ou região é a concentração de poder de processamento por *pools* de mineração. Nesse caso, os mineradores se associam deliberadamente para aglutinar poder computacional e, com isso, entregar ao sistema maior força bruta do que isoladamente conseguiriam. Seus esforços podem ser, dependendo do caso, administrados por um coordenador, o que necessariamente introduz um elemento de intermediação na prestação da atividade. De acordo com Gervais, Karame, Capkun e Capkun (2014), se apenas um *pool* de mineração congregar mais que 51% do poder de processamento global da rede, então a associação, organizada por um terceiro, pode efetivamente influenciar o processo de confirmação de transações e automaticamente controlar a *blockchain*[12].

[12] Estudo conduzido por Eyal e Sirer (2013) comprovou que o patamar de 51% pode ser ainda menor caso uma parcela de mineradores deliberadamente se associe e pratique

Por meio desse processo de concentração de poder já foram produzidas ao menos 21 mudanças na *blockchain* que deram origem a regras de funcionamento do sistema diferentes das originais (LIST…, 2018).

Além da referida comunidade que se formou ao redor do *bitcoin*, há ainda, conforme exposto anteriormente, mais um grupo de indivíduos que se organizou em torno da rede e que, assim como os desenvolvedores e mineradores, dão aplicabilidade à tecnologia em âmbito social. São os facilitadores do manejo da rede, que adaptam determinadas funcionalidades do sistema para lhe conferir maior usabilidade. Encaixam-se nessa categoria determinadas modalidades de carteiras virtuais e as *exchanges*. Os serviços de carteiras virtuais, por um lado, surgem da necessidade prática de manuseio da rede. Normalmente, explicam Böhme, Christin, Edelman e Moore (2015, p. 221), carteiras convencionais de *bitcoin* não são simples de instalar e, dependendo do tipo, elas impõem uma série de ônus ao usuário. Assim, os serviços de carteiras virtuais surgiram da necessidade prática de manuseio simples e seguro da rede de serviços especializados em armazenagem de *bitcoins*. Basicamente, tais serviços, também chamados de serviços de carteiras digitais, visam aumentar a praticidade e o nível de segurança da estocagem e da movimentação de *bitcoins*, evitando, porém, os ônus que uma carteira administrada pelo próprio usuário geraria. Diferentemente de uma carteira individual, esse tipo de serviço é administrado por um terceiro que, normalmente, cobra encargos financeiros dos usuários do serviço.

Por outro lado, há também os terceiros que se colocam na cadeia de movimentação de valores e não apenas oferecem serviços de armazenagem de *bitcoins*, mas também facilitam a troca de moeda fiduciária por criptomoedas e vice-versa. Conhecidas como casas de câmbio ou *exchanges*, os serviços dessa natureza surgiram da necessidade prática de efetuar essas trocas de modo seguro e eficiente. Os intermediários da transação geralmente fornecem uma plataforma por meio da qual compradores e vendedores anunciam suas ofertas e demandas. Mediante o cruzamento de interesses e das solicitações dos usuários, os administradores da plataforma, que mantêm o controle sobre toda a movimentação de criptomoeda e moeda fiduciária no âmbito do sistema, efetuam as trocas assumindo o risco da transação (BÖHME; CHRISTIN; EDELMAN; MOORE, 2015, p. 220). Diferentemente de quase todo tipo de atividade que se organizou em torno da rede *bitcoin*, as casas de câmbio têm constituição definida por lei e consistem essencialmente em empresas. Sofrem, portanto, incidência direta da re-

uma estratégia chamada *selfish mining*. Desde a comprovação da hipótese dos pesquisadores, diversos foram os projetos apresentados para se corrigir a vulnerabilidade do sistema.

gulação estatal. Devido a essas características, Moore e Christin (2013, p. 26) referiram-se às *exchanges* como verdadeiras autoridades centralizadoras cujo sucesso ou derrocada têm o poder de afetar positiva ou negativamente o ecossistema da rede *bitcoin*.

3.3 Materialidades sociais

Materialidades procedimentais e de mercado constituem importantes variáveis da escalabilidade do *bitcoin*. No entanto, nenhuma delas isoladamente poderia afetar tanto a aceitação por parte dos usuários quanto a terceira forma de materialidade descrita por Karlstrøm (2014). De acordo com o autor, não somente a sofisticação tecnológica e a organização do mercado ao redor do sistema *bitcoin* são suficientes para fazê-lo penetrar na vida social e torná-lo parte do cotidiano popular. Para além das duas formas de materialidades expostas anteriormente, Karlstrøm (2014) faz alusão a um terceiro de tipo de imbricação social da tecnologia denominada materialidade social. Segundo o autor, materialidades sociais consistem essencialmente naquilo que as pessoas em geral pensam e reproduzem a respeito da tecnologia. Em outras palavras, seriam uma forma de opinião coletiva a seu respeito, isto é, sua reputação (KARLSTRØM, 2014).

Embora de difícil determinação, sabe-se que a opinião pública acerca do *bitcoin* sofre inegável influência dos meios de comunicação. Tanto a internet quantos os jornais em geral têm-se prestado a solidificar uma espécie de opinião coletiva mais ou menos generalizável acerca da tecnologia, o que muito contribui para sua disseminação em larga escala ou até mesmo para a contenção do seu uso. Contudo, não apenas a mídia se presta a esse papel. Outro fator que afeta positiva ou negativamente a percepção social do *bitcoin* é a forma como muitos países têm tratado, embora de forma provisória e descoordenada, do tema da legalidade das criptomoedas. De acordo com Bryans (2014), tanto a mídia quanto as respostas regulatórias temporárias que muitos países têm dado à utilização da criptomoeda em suas respectivas jurisdições têm sido responsáveis pela construção social da imagem do *bitcoin*. Coincidência ou não, ambos os mecanismos afetam a reputação da tecnologia mediante a associação de seu uso com a legalidade ou a ilegalidade *lato sensu*.

No caso da mídia, a correlação estabelecida fica evidente diante da variação do preço do *bitcoin* quando episódio envolvendo utilização da criptomoeda para fins ilícitos ganha notoriedade e repercussão internacional nos meios de comunicação. A título de exemplo, mencione-se o caso amplamente divulgado pela mídia da utilização de *bitcoins* para a compra e venda de produtos ilegais por meio do já desmantelado mercado virtual *Silk Road*. Segundo Hern (2013), do jornal *The Guardian*, o preço da criptomoeda perdeu aproximadamente um quarto do seu valor, quando, no dia 3 de outubro de 2013, foi anunciada publicamente a prisão de Ross Ulbricht, traficante internacional de drogas que operava no referido mercado virtual por meio de *bitcoins*. Na época, anunciava o jornal, o *bitcoin* valia aproximadamente $145,70 dólares segundo a cotação da maior *exchange* dos Estados Unidos. Logo após a repercussão pública do fato ilícito, entretanto, o preço caiu para uma média de $109,76 dólares na mesma casa de câmbio, ainda segundo a reportagem.

Também ganharam especial notoriedade casos de "sequestro" de dados pela internet cuja recompensa fora estabelecida em *bitcoins* (GIBBS, 2017). Esse é o caso do *ransomware* conhecido mundialmente pelo nome de *Wannacry*, cujos criadores, após terem "se-

questrado" milhares de dados pessoais de computadores privados por meio da ferramenta, exigiram o pagamento de recompensas em *bitcoins* para a devolução das informações. Embora nenhuma característica da rede *bitcoin* em si tenha sido afetada, a mera associação pública da sua utilização a um fato ilícito provocou uma repercussão negativa na reputação da criptomoeda, que pôde ser sentida também por meio da análise da variação do preço.

De modo geral, acredita-se que a mídia, especialmente mediante a associação do uso do *bitcoin* a algum fato ilícito ou lícito, representa um importante vetor da opinião pública em relação à imagem da criptomoeda. Mas, como já salientado, não apenas a abordagem midiática de casos paradigmáticos exerce influência sobre o que se pensa em termos abstratos acerca do *bitcoin*. Tão importante quanto, senão até mais relevante, seria, segundo Bryans (2014), a imagem da criptomoeda que muito países, em especial os que abrigam grande nicho mercado para a tecnologia, evocam por meio da regulação. No geral, vige ainda grande incerteza no campo teórico acerca da natureza jurídica do ativo (CUNHA FILHO; VAINZOF, 2017). No entanto, diversas jurisdições têm-se posicionado, ainda que de maneira provisória, a respeito do assunto, facilitando ora uma posição mais permissiva em relação ao uso da criptomoeda em território nacional, ora uma posição mais restritiva. Tanto uma quanto a outra são também acompanhadas de uma sensível variação no preço do ativo, o que denota maior ou menor confiança dos usuários na tecnologia.

O primeiro exemplo notável de regulação que afetou negativamente o ecossistema das criptomoedas como um todo foi a restrição chinesa de os bancos operantes no país negociarem tanto com criptomoedas diretamente quanto com *exchanges*. Minutos após a decisão do dia 5 de dezembro de 2013, que veio acompanhada de uma declaração do governo chinês que levanta incerteza acerca do *status* jurídico das criptomoedas, o valor do *bitcoin* caiu imediatamente cerca de 10% na principal *exchange* do país, saindo de 7 mil yuans por unidade para 6,3 mil (RABINOVICH, 2013). Mais recentemente ainda, a cotação do *bitcoin* experimentou queda de mais de 10% em seu valor após o ministro das finanças sul-coreano declarar a intenção de banir completamente a circulação de criptomoedas do país asiático (AZEVEDO, 2018).

Por outro lado, o *bitcoin* e demais criptomoedas semelhantes foram valorizadas em 2017 pelo público em geral quando do reconhecimento oficial por parte do Japão de que os ativos funcionariam em território nacional como método de pagamento, tendo, portanto, poder liberatório das obrigações civis. Além de regular o âmbito de atuação das *exchanges* japonesas com o objetivo de prevenir a lavagem de dinheiro, o Japão foi o primeiro e até agora o único país a reconhecer oficialmente os efeitos das criptomoedas em território nacional por meio de lei. Logo após a publicação da medida, estima-se que o ativo tenha valorizado mais de 150% em relação ao mês anterior. De acordo com o analista Charles Hayter (FEBRE…, 2017), o novo *status* jurídico das criptomoedas no Japão "aumentou a confiança em uma moeda [*bitcoin*] que até pouco tempo era considerada ativo de risco".

Em linhas gerais, são esses alguns dos aspectos do ecossistema das criptomoedas que demonstram compor, sem a exclusão de outros fatores, a imagem da tecnologia em meio ao público. Tanto a associação midiática do uso de *bitcoins* com atividades lícitas ou ilícitas quanto o posicionamento de alguns países em relação ao uso de criptomoedas contribuem para o maior ou menor nível de aceitação da tecnologia no meio social.

A análise das materialidades procedimentais e de mercado, assim como das materialidades sociais, leva à compreensão de que a existência e a aplicabilidade em larga escala da tecnologia depende não apenas da estrutura tecnológica que suporta o *bitcoin*, mas, sobretudo, de uma série de condicionantes institucionais que se localizam fora do âmbito técnico, como a mídia e o direito.

Conclusão

Diferentemente do que celebram alguns tecnoentusiastas e a mídia em geral, o *bitcoin* não se revelou totalmente imune a influências que transcendem sua constituição tecnológica. Apesar de a tecnologia, por conta de seu *design* técnico apenas, ter reivindicado seu caráter apolítico e anti-ideológico, uma ligeira análise de seu modo de reprodução social revelou intensa dependência de aspectos externos à sua estrutura tecnológica *per se*. O primeiro conjunto de condições externas das quais o *bitcoin* se mostra dependente está relacionado com a própria manutenção da sua estrutura tecnológica. Denominadas por Karlstrøm (2014) materialidades procedimentais, as condições que dão possibilidade de existência à rede *bitcoin* dizem respeito à sustentação da criptografia, assim como da própria *blockchain*. O segundo conjunto de condições materiais ao qual o *bitcoin* se encontra sujeito, por outro lado, está relacionado à organização social que se formou ao redor da rede com o propósito de lhe conferir aplicabilidade prática e maior usabilidade no cotidiano popular. E, por fim, a terceira condição material encontrada diz respeito à percepção coletiva da imagem da criptomoeda, que é suscetível tanto à influência midiática quanto ao posicionamento de governos e Estados nacionais a respeito de sua legalidade.

A descrição das materialidades demonstra que, a despeito de a tecnologia estar inserida num contexto jurídico de incerteza, ela se encontra imersa num conjunto de condições técnicas, de mercado e sociais que moldam o que Dodd (2017) chamou de vida social do *bitcoin*, mas que bem poderia ser interpretado como um processo de institucionalização informal no sentido anteriormente exposto. Com isso, revela-se que não apenas do nível de avanço tecnológico do sistema depende a escalação da confiança no ativo. Partindo da ideia de que instituições formais e informais representam também variável relevante do processo de produção de confiança social, conclui-se que a confiança no ativo se mostra igualmente dependente da consolidação ou da desintegração de condicionantes materiais do *bitcoin*. Mais precisamente, pode-se dizer que quanto mais as condições técnicas estejam consolidadas, quanto

mais a governança e a rede de produtos e serviços que se erigiu ao redor do *bitcoin* estejam desenvolvidas e quanto mais a criptomoeda esteja publicamente associada a atividades lícitas, tanto mais a ideia do *bitcoin* como um ativo de confiança encontra terreno fértil para o crescimento.

Sobre o autor

Marcelo de Castro Cunha Filho é mestre em Direito e Inovação pela Universidade Federal de Juiz de Fora, Juiz de Fora, MG, Brasil; doutorando em Sociologia Jurídica pela Universidade de São Paulo, São Paulo, SP, Brasil; bolsista de doutorado da Fundação de Amparo à Pesquisa do Estado de São Paulo, SP, Brasil.
E-mail: mcunhafilho@yahoo.com.br

Como citar este artigo

(ABNT)
CUNHA FILHO, Marcelo de Castro. *Bitcoin*: uma tentativa de construção da confiança por meio da tecnologia. *Revista de Informação Legislativa*: RIL, Brasília, DF, v. 56, n. 221, p. 37-60, jan./mar. 2019. Disponível em: http://www12.senado.leg.br/ril/edicoes/56/221/ril_v56_n221_p37

(APA)
Cunha, M. de C., Fº. (2019). *Bitcoin*: uma tentativa de construção da confiança por meio da tecnologia. *Revista de Informação Legislativa: RIL*, *56*(221), 37-60. Recuperado de http://www12.senado.leg.br/ril/edicoes/56/221/ril_v56_n221_p37

Referências

ATZORI, Marcella. Blockchain technology and decentralized governance: is the state still necessary? [*s. n., s. l.*], p. 1-37, Dec. 2015. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2709713. Acesso em: 30 nov. 2018.

AZEVEDO, Rita. Possível proibição da Coreia do Sul derruba preço da *bitcoin*. *Exame*, São Paulo, 11 jan. 2018. Disponível em: https://exame.abril.com.br/mercados/possivel-proibicao-da-coreia-do-sul-derruba-preco-da-bitcoin/. Acesso em: 29 nov. 2018.

BITCOIN development. *BitcoinCore*, [*s. l.*], c2018. Disponível em: https://bitcoin.org/en/development. Acesso em: 28 nov. 2018.

BÖHME, Rainer; CHRISTIN, Nicolas; EDELMAN, Benjamin; MOORE, Tyler. Bitcoin: economics, technology, and governance. *Journal of Economic Perspectives*, Nashville, v. 29, n. 2, p. 213-238, 2015. Disponível em: https://pubs.aeaweb.org/doi/pdfplus/10.1257/jep.29.2.213. Acesso em: 29 nov. 2018.

BOS, Joppe W.; HALDERMAN, J. Alex; HENINGER, Nadia; MOORE, Jonathan; NAEHRING, Michael; WUSTROW, Eric. Elliptic curve cryptography in practice. *In*:

INTERNATIONAL CONFERENCE ON FINANCIAL CRYPTOGRAPHY AND DATA SECURITY, 18., 2014, Christ Church. *Anais* […]. Christ Church: [*s. n.*], 2014. p. 157-175. Disponível em: https://eprint.iacr.org/2013/734.pdf. Acesso em: 29 nov. 2018.

BRASIL. *Lei nº 12.865, de 9 de outubro de 2013*. Dispõe sobre os arranjos de pagamento e as instituições de pagamento integrantes do Sistema de Pagamentos Brasileiro (SPB). Brasília, DF: Presidência da República, [2013]. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Lei/L12865.htm. Acesso em: 3 nov. 2018.

BRYANS, Danton. Bitcoin and money laundering: mining for an effective solution. *Indiana Law Journal*, Bloomington, v. 89, n. 1, p. 441-472, 2014. Disponível em: https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=11100&context=ilj. Acesso em: 29 nov. 2018.

CORTEZ, Tiago Machado. *Moeda, Estado e direito*: o papel do Estado na ordem monetária e seu controle. 2004. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2004.

CUNHA FILHO, Marcelo de Castro; VAINZOF, Rony. A natureza jurídica "camaleão" das criptomoedas. *Jota*, [São Paulo], 21 set. 2017. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/direito-digital/a-natureza-juridica-camaleao-das-criptomoedas-21092017. Acesso em: 29 nov. 2018.

DE FILIPPI, Primavera; LOVELUCK, Benjamin. The invisible politics of bitcoin: governance crisis of a decentralized infrastructure. *Internet Policy Review*, [Berlin], v. 5, n. 3, Sept. 2016. DOI: 10.14763/2016.3.427. Disponível em: https://policyreview.info/node/427/pdf. Acesso em: 29 nov. 2018.

DODD, Nigel. The social life of bitcoin. *Theory, Culture & Society*, [*s. l.*], p. 1-26, 2017. Disponível em: http://eprints.lse.ac.uk/69229/1/Dodd_The%20social%20life%20of%20Bitcoin_author_2017%20LSERO.pdf. Acesso em: 29 nov. 2018.

DURAN, Camila Villard. *A moldura jurídica da política monetária*: um estudo de caso. 2012. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2012. Disponível em: http://www.teses.usp.br/teses/disponiveis/2/2139/tde-02102012-161336/pt-br.php. Acesso em: 29 nov. 2018.

EYAL, Ittay; SIRER, Emin Gün. Majority is not enough: bitcoin mining is vulnerable. *In*: INTERNATIONAL CONFERENCE ON FINANCIAL CRYPTOGRAPHY AND DATA SECURITY, 18., 2013, Christ Church. *Anais* […]. Christ Church: [*s. n.*], 2013. p. [1-18]. Disponível em: https://www.cs.cornell.edu/~ie53/publications/btcProcFC.pdf. Acesso em: 29 nov. 2018.

FEBRE do ouro digital no Japão faz valor do *bitcoin* disparar. *Exame*, [São Paulo], 22 jun. 2017. Disponível em: https://exame.abril.com.br/mercados/febre-do-ouro-digital-no-japao-faz-valor-do-bitcoin-disparar/. Acesso em: 4 dez. 2018.

GERVAIS, Arthur; KARAME, Ghassan O.; CAPKUN, Srdjan; CAPKUN, Vedran. Is bitcoin a decentralized currency? *IEEE Security and Privacy*, [Champaign], v. 12, n. 13, p. 1-11, 2014. Disponível em: https://eprint.iacr.org/2013/829.pdf. Acesso em: 30 nov. 2018.

GIBBS, Samuel. WannaCry: hackers withdraw £108,000 of bitcoin ransom. *The Guardian*, [London], 3 Aug. 2017. Disponível em: https://www.theguardian.com/technology/2017/aug/03/wannacry-hackers-withdraw-108000-pounds-bitcoin-ransom. Acesso em: 30 nov. 2018.

GILES, Martin; KNIGHT, Will. Google thinks it's close to "quantum supremacy": here's what that really means. *MIT Technology Review*, [Washington, DC], Mar. 9, 2018. Disponível em: https://www.technologyreview.com/s/610274/google-thinks-its-close-to-quantum-supremacy-heres-what-that-really-means/. Acesso em: 30 nov. 2018.

GLOBAL bitcoin nodes distribution. *Bitnodes*, [*s. l.*], c2018. Disponível em: https://bitnodes.earn.com/. Acesso em: 28 nov. 2018.

GOOD, David. Individuals, interpersonal relations, and trust. *In*: GAMBETTA, Diego (ed.). *Trust*: making and breaking cooperative relations. Oxford, UK: Blackwell, 1988. p. 31-48.

GOODHART, Charles A. E. Two concepts of money: implications for the analysis of the optimal currency areas. *European Journal of Political Economy*, [*s. l.*], v. 14, n. 3, p. 407-432, Aug. 1998.

GOOGLE encoraja a indústria a utilizar a criptografia SHA-256. *CryptoID*, São Paulo, 6 mar. 2017. Disponível em: https://cryptoid.com.br/banco-de-noticias/google-encoraja-industria-utilizar-criptografia-sha-256/. Acesso em: 29 nov. 2018.

HARDIN, Russell. Trustworthiness. *Ethics*, [Chicago], v. 107, n. 1, p. 26-42, Oct. 1996.

HERN, Alex. Bitcoin price plummets after Silk Road closure. *The Guardian*, [London], 3 Oct. 2013. Disponível em: https://www.theguardian.com/technology/2013/oct/03/bitcoin-price-silk-road-ulbricht-value. Acesso em: 30 nov. 2018.

_____. Bitcoin's energy usage is huge – we can't afford to ignore it. *The Guardian*, [London], 17 Jan. 2018. Disponível em: https://www.theguardian.com/technology/2018/jan/17/bitcoin-electricity-usage-huge-climate-cryptocurrency. Acesso em: 30 nov. 2018.

KARLSTRØM, Henrik. Do libertarians dream of electric coins?: the material embeddedness of bitcoin. *Distinkton*: Journal of Social Theory, [*s. l.*], v. 15, n. 1, p. 23-36, 2014. DOI: 10.1080/1600910X.2013.870083. Disponível em: https://brage.bibsys.no/xmlui/bitstream/handle/11250/2393381/virtual-money.pdf?sequence=3&isAllowed=y. Acesso em: 30 nov. 2018.

KEYNES, John Maynard. *A treatise on money*. London: Macmillan, 1950. v. 1.

KNAPP, Georg Friedrich. *The state theory of money*. San Diego: Simon, 2003.

LIST of bitcoin forks. *CryptoCompare*, [*s. l.*], 1th Mar. 2018. Disponível em: https://www.cryptocompare.com/coins/guides/list-of-bitcoin-forks/. Acesso em: 29 nov. 2018.

MCGINNIS, John O.; ROCHE, Kyle. Bitcoin: order without law in the digital age. *Northwestern Public Law*, [*s. l.*], n. 17-06, p. 1-59, Mar. 2017. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2929133. Acesso em: 30 nov. 2018.

MÖLLERING, Guido. Trust, institutions, agency: towards a neoinstitutional theory of trust. *In*: BACHMANN, Reinhard; ZAHEER, Akbar (ed.). *Handbook of trust research*. Northampton, MA: Edward Elger, 2006. p. 355-376. Disponível em: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.492.2509&rep=rep1&type=pdf. Acesso em: 30 nov. 2018.

MOORE, Tyler; CHRISTIN, Nicholas. Beware the middleman: empirical analysis of bitcoin-exchange risk. *In*: INTERNATIONAL CONFERENCE ON FINANCIAL CRYPTOGRAPHY AND DATA SECURITY, 17., 2013, Heidelberg. *Anais* […]. Heidelberg: [*s. n.*], 2013. p. 1-8. Disponível em: https://fc13.ifca.ai/proc/1-2.pdf. Acesso em: 30 nov. 2018.

NAKAMOTO, Satoshi. Bitcoin: a peer-to-peer electronic cash system. *Bitcoin*, [*s. l.*], 2008. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 29 nov. 2018.

OERMANN, Markus; TÖLLNER, Nills. NoC internet governance case studies series: the evolution of governance structure in cryptocurrencies and the emergence of code-based arbitration in bitcoin. *In*: GASSER, Urs; BUDISH, Ryan; WEST, Sarah Myers (ed.). *Multistakeholder as governance groups*: observations from case studies. Cambridge, MA: Berkman, 2015. p. 1-13. Disponível em: https://www.hans-bredow-institut.de/uploads/media/Publikationen/cms/media/1cdcee016e866b642dd72bb578c871296cdc852e.pdf. Acesso em: 29 nov. 2018.

PUBLIC trust in government remains near historic lows. *Pew Research Center*, Washington, DC, May 3, 2017. Disponível em: http://www.people-press.org/2017/05/03/public-trust-in-government-remains-near-historic-lows-as-partisan-attitudes-shift/1-19/. Acesso em: 28 nov. 2018.

PUTNAM, Robert D. *Bowling alone*: the collapse and revival of American community. New York: Simon & Schuster, 2000.

QUANTUM computers pose imminent threat to bitcoin security. *MIT Technology Review*, [Washington, DC], Nov. 8, 2017. Disponível em: https://www.technologyreview.com/s/609408/quantum-computers-pose-imminent-threat-to-bitcoin-security/. Acesso em: 30 nov. 2018.

RABINOVICH, Simon. China proíbe bancos de realizar transações com *bitcoins*. *Folha de S.Paulo*, [São Paulo], 5 dez. 2013. Disponível em: http://www1.folha.uol.com.br/mercado/2013/12/1381149-pequim-proibe-bancos-de-realizar-transacoes-com-bitcoins.shtml. Acesso em: 29 nov. 2018.

SWAN, Melanie. *Blockchain*: blueprint for a new economy. Sebastopol, CA: O'Reilly, 2015.

TAPSCOTT, Don; TAPSCOTT, Alex. *Blockchain revolution*: como a tecnologia por trás do *bitcoin* está mudando o dinheiro, os negócios e o mundo. São Paulo: Ed. SENAI, 2017.

TWOMEY, Peter. Halting a shift in the paradigm: the need for bitcoin regulation. *Trinity College Law Review*: TCLR, [Dublin], v. 16, p. 67-90, 2013. Disponível em: http://heinonline.org/HOL/LandingPage?handle=hein.journals/trinclr16&div=8&id=&page=. Acesso em: 30 nov. 2018.

VIGNA, Paul; CASEY, Michael J. *The age of cryptocurrency*: how bitcoin and digital money are challenging the global economic order. New York: St. Martin's Press, 2015.

WIKE, Richard; SIMMONS, Katie; STOKES, Bruce; FETTEROLF, Janell. Many unhappy with current political system. *Pew Research Center*, Washington, DC, Oct. 16, 2017. Disponível em: http://www.pewglobal.org/2017/10/16/many-unhappy-with-current-political-system/. Acesso em: 28 nov. 2018.

WILLIAMSON, Oliver E. Calculativeness, trust, and economic organization. *Journal of Law and Economics*, [Chicago], v. 36, n. 1, p. 453-486, Apr. 1993. Disponível em: http://www.jstor.org/stable/725485. Acesso em: 30 nov. 2018.

ZUCKER, Lynne G. Production of trust: institutional sources of economic structure, 1840-1920. *Research in Organizational Behaviour*, [Amsterdam], v. 8, p. 53-111, 1986.