

A IMPOSSIBILIDADE DE REGULAÇÃO JURÍDICA NACIONAL DO BLOCKCHAIN: RUMO À UM DIREITO CRIPTOGRÁFICO?

THE IMPOSSIBILITY OF NATIONAL LEGAL FRAMEWORK TO REGULATE BLOCKCHAIN TECHNOLOGY: TOWARDS CRYPTOGRAPHIC LAW?

Álvaro Osório do Valle Simeão^I

Marcelo Dias Varella^{II}

^I Centro Unificado de Brasília (UNICEUB), Brasília, DF, Brasil. Doutorando em Direito. E-mail: alvarosorio1@hotmail.com

^{II} Centro de Ensino Unificado de Brasília (UNICEUB), Programa de Pós-Graduação em Direito, Brasília, DF, Brasil. Doutor em Direito. E-mail: marcelodvarella@gmail.com

Resumo: O artigo explica a tecnologia descentralizada da cadeia de blocos (blockchain), a percepção do direito estrangeiro e internacional sobre o tema e as tentativas de regulação em diferentes países. Utiliza-se a bibliografia nacional e estrangeira, bem como as discussões no plano legislativo. As características da tecnologia e as discussões internacionais de países em que a mesma está mais desenvolvida conduzem à conclusão que apenas é possível regular o blockchain por meio do direito transnacional, não apenas público, mas também privado.

Palavras-chave: Cadeia de blocos. Criptomoedas. Ciberespaço. Regulação.

Abstract: The article explains the main concepts of blockchain technology, the perception of foreign and international law on the subject and the attempts of regulation in different countries. We use the national and foreign most cited references as well as the discussions in the legislative area. The characteristics of technology and the international discussions of countries in which the debate is more developed lead to the conclusion that it is only possible to regulate the blockchain through transnational law, not only public, but also private.

Keywords: Blockchain. Cryptocoins. Cyberspace. Regulation.

Sumário: Introdução. 1 Novas e poderosas mãos invisíveis no ciberespaço. 2 A falibilidade do direito estatal em regular aplicações em cadeia de blocos: o exemplo das criptomoedas. 3 A regulação transnacional minimalista da cadeia de blocos a partir da *lex mercatoria* e da *lex cryptographia*. 3.1 A ilicitude pelo anonimato. 3.2 *Pacta sunt servanda* no ciberespaço. 3.3 A responsabilização das corretoras e dos hackers. 3.4 Prevenção de monopólios e gestão de custos ambientais. Considerações Finais. Referências.

Introdução

Aplicativos que utilizam cadeia de blocos (*blockchain*) e viabilizam o estabelecimento de contratos inteligentes exigem regulamentação minimalista transnacional futura, atendo-se a um conceito de boa-fé objetiva que transcenda o multiculturalismo.

Há já um direito não positivado que nasce a partir do protocolo e dos condicionamentos entre as próprias partes contratantes no ciberespaço. Esses acordos e sua repetição massiva fomenta o costume negocial no meio virtual desmaterializado (*lex mercatoria* digital).

Para além disso, as transações na *blockchain* têm gerado uma norma entre as partes, com baixo nível de abstração e protegida por criptografia pesada, que autores chamam de *lex cryptography*, ou seja, regras administradas por meio de contratos inteligentes e organizações autônomas¹.

Mas em ambos os casos o Estado se encontra alijado do seu papel histórico de criador do direito, ainda que essas normas endógenas, já existentes, não bastem para proteção de direitos fundamentais dos novos comerciantes digitais.

Aplicativos que utilizam a tecnologia subjacente da cadeia de blocos no ciberespaço representam um avanço impactante por fixar um caminho ineditamente viável para a realização de transações seguras na *internet* sem a presença de um intermediário (*middleman*), fato que gera imediatamente uma pergunta: Qual o caminho para regular essas aplicações e a própria cadeia de blocos?

O presente texto argumenta no sentido da inadequação de qualquer regulação estatal à *blockchain*, uma vez que as transações realizadas sob essa plataforma são planificadas em escala mundial e executadas fora de um espaço físico materializado sobre o qual possa incidir uma única soberania.

Ainda que a cadeia de blocos tenha potencial para fragilizar a proteção de direitos fundamentais, entre os quais o direito de propriedade intelectual, vez que ocorre uma reprodução de informação sem pagamento de direitos autorais a cada nó adicionado à rede, verifica-se que a proteção desses direitos se projeta para o ambiente transnacional com base numa ética mínima, sendo necessário

1 WRIGHT, Aaron; FILIPPI, Primavera de. *Decentralized blockchain technology and the rise of lex cryptography*. Mimeo. Disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664. Acesso em 01/12/2017.

reconhecer a ineficácia das normas internas em regular um aplicativo que se encontra planetariamente disseminado.

Ao Estado só resta um papel de usuário da cadeia de blocos, pois as regulações nacionais apenas adicionam restrições geradoras de desigualdade entre os usuários tendo por base o local em que residem ou se encontram, que não coincide com o sítio virtual dos negócios implementados pelas partes. É o que se observa em relação às criptomoedas, que são viabilizadas pela tecnologia subjacente da cadeia de blocos.

O desenvolvimento criptográfico constante, que ocorre pelo próprio uso, como se observa na cadeia de blocos, dá pistas de como essa inovação pode ser útil na execução e controle administrativo de políticas públicas, sobretudo em países em desenvolvimento. Os contratos inteligentes podem ser ferramenta para aumento da organização, gestão e transparência das ações governamentais, com consequente aumento da normatividade constitucional, mas isso depende da implementação de uma norma internacional disciplinadora de certos aspectos pragmáticos que cercam a *blockchain*.

O presente texto se divide em três partes. Na primeira faz-se uma abordagem técnica e descritiva sobre as características da cadeia de blocos e as possibilidades criadas por essa tecnologia para as relações interpessoais tangentes à figura do Estado.

Na segunda parte se pretende demonstrar que a regulação dos programas que rodam em cadeia de blocos não deve estar na lista de prioridades nacionais, pois as normas internas voltadas para esse intento já nasceriam ineficazes. Aos Estados restaria figurar como usuários dessa tecnologia tanto no âmbito interno – ferramenta para otimização de políticas públicas – como no plano internacional – ferramenta para processamento de transações comerciais bilaterais e multilaterais entre nações, assim como estabelecimento de tratados e convenções internacionais.

Na terceira parte elencam-se tópicos para uma regulação transnacional minimalista em relação aos aplicativos que fazem uso da cadeia de blocos, tomando por base o exemplo das moedas digitais. Defende-se, para tanto, uma positivação mínima que esteja atenta, inicialmente, ao próprio costume já existente entre as partes contratantes no ciberespaço.

1 Novas e poderosas mãos invisíveis no ciberespaço

O ciberespaço resulta da descentralização da informação propiciada pela rede mundial de computadores e uma questão nuclear que surgiu paralelamente a esse advento sempre foi a da confiança interpessoal nesse ambiente, uma vez que nunca existiu um mecanismo central de autenticação dos fenômenos virtuais.

Até o surgimento da cadeia de blocos, a fiabilidade das transações que se efetuavam na *internet* baseava-se, quase que unicamente, nas assinaturas eletrônicas, que são meios de identificação pessoal por certificação digital submetida a uma autoridade pública, geralmente um órgão colegiado que regula e fiscaliza essa atividade de registro, de modo que tal procedimento não se afasta muito do que historicamente se conhece como fê pública, esteio maior da atividade cartorária².

A noção conceitual de cadeia de blocos (*blockchain*) parte justamente da eliminação da figura do terceiro, ou seja, do intermediário certificador da operação, conforme proposta contida no artigo “*Bitcoin: A Peer-to-Peer Eletronic Cash System*”³, de autoria não identificada⁴.

Nesse texto foram fixadas premissas que viabilizaram transações seguras no ciberespaço, sem intermediário, pela utilização de redes P2P (*Peer-to-Peer / pessoa a pessoa/ par a par*), que por não se basearem em uma arquitetura de cliente a servidor possuem a grande vantagem de não ter uma função de rede centralizada. Todos os participantes estão interconectados podendo acessar dados de qualquer outro partícipe, o que coloca a disponibilidade da informação em nível difuso máximo.

Na dinâmica operacional da cadeia de blocos tudo nasce da intenção negocial entre duas partes, que pode ser a compra de uma unidade de valor, a fixação de um contrato, a oferta de um voto, a prolação de uma opinião sobre algo e qualquer coisa que, em outros

-
- 2 Ideia basal contida, por exemplo, na Medida Provisória Brasileira nº 2.200-2, de 24 de agosto de 2001, que instituiu a Infraestrutura de Chaves Públicas Brasileiras: ICP/Brasil.
 - 3 NAKAMOTO, Satoshi. *Bitcoin: A Peer-to-Peer Eletronic Cash System*. Mai. 2008. Disponível em: <<https://bitcoin.org/bitcoin.pdf>>. Acesso em: 7 nov. 2017.
 - 4 A identidade física e nacionalidade de Satoshi Nakamoto nunca foram comprovadas. Após fixar as bases da *blockchain* e possibilitar a criação da moeda digital *bitcoin*, suas manifestações no ciberespaço foram paulatinamente diminuindo até o desaparecimento, em meados de 2010. A respeito: MUSE, Alexander. *How the NSA identified Satoshi Nakamoto*. Ago. 2010. Disponível em: <https://medium.com/cryptomuse/how-the-nsa-caught-satoshi-nakamoto-868affcef595>. Acesso em: 8 nov. 2017.

tempos, precisasse ser registrada ou atestada por um intermediário de confiança, mas que nesse universo computacional será transformada em um código aberto criptografado, o que significa dizer que a operação estará acessível, mas sem que se possa saber quem são os contratantes, a não ser os próprios, uma vez que eles escolheram seus “endereços” de identificação.

Externada a vontade negocial no ambiente virtual da *blockchain* e tornadas anônimas as partes pela incidência da criptografia, a transação será enviada para todos os computadores que já fizeram, algum dia, operação na mesma área de interesse (mesma cadeia), mas ainda estará pendente de validação.

Para essa validação, que gerará o registro existencial do negócio (*blockchain protocol*), é preciso que a vontade criptografada seja analisada por computadores mineradores, que nada mais são do que máquinas, públicas ou privadas, que a cada espaço de tempo⁵, considerado o seu poder de processamento, são vencedoras de uma competição matemática que lhes dá o direito de incluir operações pendentes na cadeia de blocos.

Como a competição ocorre a cada espaço de tempo há uma mudança constante na figura do computador validador, de modo que não se pode concluir que haja uma centralização da função de validação das operações.

Esses competidores tencionam ganhar algo a cada vez que vencem a disputa, até porque gastam muita energia elétrica em equipamentos caros e com alto poder de análise matemática combinatória. No caso das moedas digitais eles ganham moeda digital⁶, mas no caso de outras aplicações a remuneração pode ocorrer a partir de qualquer ativo econômico previamente fixado no momento em que a cadeia de blocos se iniciou.

Assim, existem duas categorias de partícipes na cadeia de blocos, a saber: os partícipes transacionais, que querem validar e registrar um negócio na cadeia de blocos, e os partícipes mineradores, que objetivam ser recompensados por vencerem a disputa algorítmica e daí serem validadores das transações.

A validação da operação parte da verificação do consenso, ou seja, do preenchimento de requisitos estabelecidos no início da cadeia

5 No caso das moedas digitais esse espaço de tempo tem sido de dez minutos.

6 Daí os termos “mineração” e “mineradores” no mercado de criptomonedas.

de blocos, da verificação dos endereços dos proponentes e da verificação da sequência de operações que já foram feitas precedentemente naquele ambiente, gerando um código parêlo com a oficialização da data do negócio e a identificação do mesmo, que agora passa a ser mais um bloco na cadeia.

Validada a operação, parte-se para tornar imutável esse negócio, que só poderá ser infirmado por um novo negócio entre as mesmas partes ou cujo objeto seja o mesmo. A imutabilidade ocorre pela incidência de uma função matemática (*hash*) sobre o conjunto de informações criadas pelos partícipes transacionais e validadas pelos partícipes mineradores.

A função matemática nova terá o poder de impedir modificações negociais sem que todos os partícipes concordem. Isso derivará da dependência do código alfanumérico atual em relação àquele gerado pela incidência da função matemática sobre o negócio anterior, ou seja, o registro atual depende do anterior e assim por diante até o primeiro negócio validado e registrado (o primeiro bloco).

Diante desse quadro fático, podemos conceituar a cadeia de blocos como sendo um livro eletrônico de registro distribuído, imutável e sem autoridade de controle que gera um protocolo de confiança calcado na abertura da informação sobre o negócio jurídico feito em ambiente virtual, numa rede computacional formada por pares equipotentes.

A cadeia de blocos projeta a fiabilidade para além das certificações digitais adotadas por um Estado, pois a utilização do programa que roda nesse ambiente gera um registro, que pode ter natureza contábil ou jurídica, que é imediata e automaticamente distribuído e gravado em todos os equipamentos de informática que já fizeram a operação ou farão, em escala planetária de milhões de computadores, de modo que quanto mais transações se fizer, mais segurança e confiança a *blockchain* proporciona ao usuário, pois mais difusa se torna a informação sobre o acordo celebrado e mais complexa fica a criptografia que incide sobre ele⁷.

Não existe um proprietário ou gestor da informação contábil ou jurídica, mas um mero hospedeiro, pois a cada negócio fechado em ambiente de ciberespaço, utilizando os programas ligados à *blockchain*, o computador passa a ter o histórico de todas as transações já feitas naquele mercado, o que afasta a insegurança jurídica sobre a avença

7 NAKAMOTO, Satoshi. *Bitcoin: A Peer-to-Peer Eletronic Cash System*. Mai. 2008. Disponível em: <<https://bitcoin.org/bitcoin.pdf>>. Acesso em: 7 nov. 2017.

e permite a exigência de cumprimento no próprio ambiente do processamento de dados (obediência à *lex cryptographia*).

A rede efetua a transação entre as partes, colocando essa informação em uma cadeia contínua de prova de trabalho criptografada pelo sistema⁸, em linguagem computacional, de modo que o registro contábil acumulado não pode ser alterado.

A própria cadeia de informação, formada por “nós” equipotentes, gera a segurança e confiança do sistema, pois o negócio entre as partes alimenta um banco de dados público, único, cronológico e compartilhado pelos participantes de um *software* específico, e tudo isso sem que exista uma autoridade de controle (Estado, Banco Central ou cartório).

Trata-se de uma organização autônoma que opera sobre a rede computacional sem intervenção humana que represente autoridade, a propiciar um equilíbrio dependente entre igualdade e liberdade que pode ser denominado “princípio da equipotência libertária”.

O princípio da equipotência libertária é o postulado segundo o qual, no ciberespaço, diferentemente do que ocorre no espaço físico real⁹, é possível a criação e reprodução de condições de igualdade que geram confiança entre as partes, premissa para a verdadeira liberdade de contratar.

Apresunção de boa-fé objetiva, presa a um padrão ético de conduta variável culturalmente, é alçada a um novo patamar ante a facilidade de comprovação do pacto firmado e das suas condições, de modo a fundir

8 Impende comentar que a tecnologia de criptografia utilizada é de *crowdsourcing*, ou seja, a cada hospedagem da informação, em um novo computador, adiciona-se um dado criptográfico, de modo que quanto mais transações se efetivarem mais difícil se torna quebrar o algoritmo inteligente que protege a informação, que passa a ser randômica. O *hacker* teria de percorrer toda a cadeia de prova de trabalho em nível planetário e teria de ter acesso a todo novo negócio virtual, em tempo real, o que excede a perspectiva do razoável.

9 O dilema que marca o equilíbrio entre Liberdade e Igualdade é discutido por pensadores como Aristóteles, Stuart Mill, Maquiavel, Montesquieu, Espinosa e Marx. Alexis de Tocqueville, ao focar a novel república norte-americana, anota como aspecto básico e necessário para a democracia a igualdade de condições. Na América estariam presentes os pressupostos da existência da democracia, quais sejam: o equilíbrio entre poderes, a liberdade, o respeito ao direito e, principalmente, a igualdade na vontade popular (*one head, one vote*). Mas o grande problema, como também assevera Tocqueville, é que enquanto a liberdade na América aparece naturalmente para a sociedade, a conquista da igualdade depende de fatores externos aos seres humanos. A liberdade, assim, não implica igualdade, que precisa do patrocínio do Estado para nascer, e já nasce a partir de critérios sempre criticáveis.

parte e fiscal num mesmo usuário, marginalizando autoridades centrais em campos como comunicação, política e comércio.

Atores como Estado, cartórios e bancos passam a não ser essenciais para tarefas como a emissão de moeda ou execução de contratos não cumpridos, pois a norma criada entre os contratantes está difundida em todo o universo virtual da cadeia de blocos.

São exemplos de programas que rodam em cadeia de blocos o *Bitcoin*, plataforma para mineração de moedas digitais, o *Ethereum*, um programa hábil a minerar criptomoedas e firmar contratos inteligentes, o *Follow my vote*, que se destina a realizar eleições, e o *BiltHealth*, para registro e acompanhamento de prontuários médicos¹⁰.

Foque-se o caso das moedas virtuais. A mineração dessas moedas só é possível pela validação do consenso, ou seja, com atenção a toda cadeia histórica de negócios precedentemente fechados. Esse consenso é a prova de trabalho que influenciará diretamente na disponibilidade daquele bem, independentemente de lastro material¹¹.

Não há, assim, como alguém ter risco diferenciado em relação à moeda e nem como alguém ser forçado a participar desse mercado, de modo que vige uma liberdade de contratar que guarda correlação com a igualdade entre os partícipes, garantida pelo consenso e pela inexistência de autoridade central. Essa liberdade e igualdade também se prende ao fato de que tais moedas não são emitidas por qualquer nação ou entidade legal, não sofrendo a influência da política econômica de um governo específico, o que aponta na direção de um “ciberliberalismo”.

No que se refere às “criptomoedas”, basta dizer que não representam expressão financeira de uma determinada soberania

10 Mas não são os únicos, pois plataformas novas, para finalidades novas, são inauguradas quase que diariamente desde 2009, com a difusão do algoritmo de Nakamoto.

11 A noção de lastro material remonta ao Acordo de Bretton Woods, realizado entre as maiores economias do mundo, em 1944, para que o dólar se tornasse a moeda oficial de troca do planeta. Naquela época o dólar era atrelado ao ouro, política monetária denominada padrão-ouro ou lastro-ouro, o que significava que cada nota de dólar correspondia a uma quantidade de ouro físico, podendo ser inclusive trocada por pessoas físicas nos bancos. Em 1971 o presidente norte-americano Richard Nixon desatrelou o dólar ao ouro, fazendo com que a moeda tivesse lastro unicamente na credibilidade internacional. Hoje em dia a maioria das moedas, inclusive as digitais, possuem lastro imaterial: a confiança no futuro e no que elas podem comprar. Em 29 de novembro de 2017 um *bitcoin* ultrapassou, pela primeira vez, o valor de dez mil dólares, o que não significa a mesma correlação no futuro.

nacional¹² e que o lastro de uma moeda digital é a sua própria procura e aceitabilidade (possibilidade de troca por mercadorias e serviços)¹³, nunca o fato dela ter sido emitida por uma autoridade monetária ligada a um Estado específico.

A noção de risco, em relação a esse tipo de ativo virtual, é diferente da noção de risco macroeconômico¹⁴. Uma situação de desequilíbrio fiscal, inflação ou desvalorização cambial, por exemplo, pode levar a desdobramentos negativos para moedas nacionais, mas não atingirão uma “criptomoeda”, o que leva à conclusão de que esses ativos possuem maior imunidade a desastres provocados por opções políticas de governo. Os riscos que envolvem negociações em cadeia de blocos são basicamente ligados a aspectos financeiros internacionais, procura e aceitação mundial, além de riscos técnicos e operacionais.

Como já se assistiu no capitalismo pós-revolução científica, a valorização do ativo ocorre pelo constructo imaginário da promessa de retorno¹⁵, ou seja, quanto mais esforços se envidam para sua aquisição, mais valorização ele terá, independentemente do lastro material que, na atualidade, é uma ilusão econômica, uma vez que os bancos normalmente são autorizados pelos governos a emprestar várias vezes o capital real e disponível por eles.

É um raciocínio simplista, portanto, fazer uma associação necessária entre criptomoedas e fraude. Seria o mesmo que acusar de fraudulento o próprio conceito de crédito, motor do desenvolvimento econômico capitalista, pois o mesmo risco de quebra de um banco típico, preso a saques concentrados no tempo, vinculados a eventos abaladores

12 A Constituição do Brasil de 1988 estabelece, em seu artigo 21, inciso VII, que emitir moeda é competência administrativa exclusiva da União, e isso se deve ao fato de que moeda é expressão econômica de soberania.

13 Alguns economistas defendem a existência de uma bolha especulativa digital: Gandel, Stephen. Opinião: bolha bitcoin vai estourar sob pressão da oferta. Disponível em <https://economia.uol.com.br/noticias/bloomberg/2017/11/28/bolha-da-bitcoin-vai-estourar-sob-pressao-de-oferta-gadfly.htm>. Acesso em: 1 dez. 2017.

14 Como declarou Benoit Coeure, membro da Comissão Executiva do Banco Central Europeu, as pessoas que investem em moedas digitais estão arriscando seu dinheiro, mas não há riscos macroeconômicos mais amplos, acrescentando que os bancos têm pouca exposição aos bitcoins e que, no passado, eles foram os “vetores para a transmissão de riscos sistêmicos” ao mercado financeiro. A propósito: *Membro do BCE não vê riscos macroeconômicos com bitcoins*. Disponível em: <https://www.terra.com.br/economia/membro-do-bce-nao-ve-riscos-macroeconomicos-com-bitcoins,520a57825aa450363f2cea2525c44d256bavr04z.html>. Acesso em 13/12/2017.

15 HARARI, Yuval Noah. *Sapiens: uma breve história da humanidade*. L&PM: Porto Alegre, 2017, p. 316-317

da confiança de retorno ou honra dos depósitos feitos, é o que se pode colocar em relação ao mercado virtual de moedas não estatais.

Os riscos da renda variável, ligados à oferta e procura de ações, é também o mesmo que permeia o valor de uma criptomoeda, que será tão mais alto quanto maior for o interesse de mineração e a disponibilidade do ativo que, em regra, é quantitativamente finito (princípio da raridade)¹⁶. Se o movimento de venda da moeda digital for muito grande em pouco tempo o seu valor de mercado cairá.

A diferença é que esse tipo de ativo não possui garantias públicas. Não existe um fundo garantidor do crédito coordenado pelo governo ou por um banco central. A única garantia é a prova de trabalho desde o primeiro negócio efetuado no ciberespaço, o que implica dizer que a capacidade de troca do ativo virtual, por bens e serviços reais, é fator de afastamento do seu caráter meramente especulativo.

Destaque-se que, no início das operações com esses ativos, em 2009 e 2010, pequenos equipamentos, como um computador pessoal, rendiam muita moeda virtual aos mineradores, que venciam muito facilmente a competição matemática de validação dos negócios, mas com o aumento da raridade da moeda a mineração encontra-se restrita a equipamentos grandes e poderosos, que consomem grandes quantidades de energia, distantes da realidade doméstica¹⁷.

Desse modo, a aquisição hoje se dá, principalmente, pela comercialização de moedas virtuais já mineradas, ou seja, já extraídas da cadeia de blocos, o que precipitou o surgimento de corretoras e bolsas, também em meio virtual, para comercialização desses ativos e troca dos mesmos por moedas nacionais.

Disso decorre que as criptomoedas, hoje, continuam imunes a riscos políticos, ou seja, aqueles decorrentes de intervenções governamentais, mas não existe imunidade contra fraudes praticadas por corretoras, bolsas e sítios eletrônicos que façam a ponte entre os ativos existentes no ciberespaço e o mundo real.

16 A projeção inicial do *bitcoin*, fixada na própria cadeia de blocos, é de que a emissão dessa moeda não ultrapasse vinte uma milhões de unidades.

17 Segundo a *Power Compare*, empresa sediada na Nova Zelândia e que se ocupa da análise comparativa entre companhias, projetos específicos e preços, a mineração de *bitcoin* já é responsável por 0,13% do consumo total global de eletricidade. Fonte: Revista Infomoney, disponível em <http://www.infomoney.com.br/mercados/bitcoin/noticia/7112594/mineracao-bitcoin-consome-mais-energia-que-159-paises-juntos>. Acesso em: 9 fev. 2018.

Há também riscos estruturais e finalísticos no que diz respeito à cadeia de blocos, relacionados com ataques de *hackers*, defeitos de armazenamento de informação, ilicitudes pelo anonimato propiciado pela rede criptográfica e garantia de manutenção das condições iniciais do sistema, o que aponta na direção da necessidade de regulação para além das normas costumeiras e criptográficas criadas pelas próprias bases técnicas da *blockchain*.

2 A falibilidade do direito estatal em regular aplicações em cadeia de blocos: o exemplo das criptomoedas

A inexistência de garantias, pela inexistência de intermediários públicos nas transações via cadeia de blocos, assim como o isolamento virtual dos negócios, sem que os mesmos se projetem em bens e serviços reais, são fatores que potencializam os riscos ante o caráter cíclico dos aspectos econômicos, com prejuízos que podem se projetar política e socialmente, daí a preocupação cada vez maior dos Estados com a regulação desse tipo de operação informatizada.

As restrições normativas, em nível nacional, dos contratos fechados em aplicativos que usam cadeia de blocos tem sido, contudo, um grande fator de volatilidade econômica. A cada notícia de novos regulamentos, em diferentes países, há uma oscilação negativa dos valores de moedas digitais e uma diminuição de utilização de contratos inteligentes em geral. Ao contrário, quando estabelecimentos e instituições reguladas pelo poder público passam a aceitar e a operar esse tipo de ferramenta, há um incremento valorativo e quantitativo das mesmas.

A colocação de dois eventos em confronto comprova tais fatos: em 10 de dezembro de 2017, quando a Bolsa de Chicago passou a admitir negociações de contratos futuros em *bitcoin* houve um salto valorativo da moeda de 21% em menos de 48 horas. Já as meras especulações de restrições regulatórias pelos governos da Coreia do Sul e da China, em 16 de janeiro de 2018, redundou numa queda diária de mais de 14%, no que se refere ao *bitcoin*.

Apesar disso, as regulações nacionais se espalham em muitos países. Uma das normas mais conhecidas e que produziu mais impacto foi a introduzida pelo Departamento de Serviços Financeiros de Nova York, em 2014, e que criou a necessidade de uma licença pública para intermediar operações com criptomoedas já mineradas (*BitLicense*),

assim consideradas qualquer tipo de unidade que for usada como meio de troca ou forma de valor existente apenas em meio digital¹⁸.

O Estado de Nova Iorque não fez incidir a necessidade de licença a pessoas que mineram moedas virtuais diretamente na *blockchain* e nem interferiu nas transações individuais, entre possuidores, utilizando a rede *peer to peer*, pois isso seria completamente ineficaz.

Contudo, o Estado passou a exigir licença das corretoras e bolsas que intermediam a compra de moedas já mineradas, o que indica que a preocupação da autoridade pública, nesse caso, está voltada para a vigilância sobre a corretagem. Para além disso, criou-se também uma taxa de processamento em prol do Departamento Financeiro do Estado de Nova Iorque, o que demonstra interesse arrecadatório. Essa licença passou a ser exigida, a partir de 2015, por outros Estados norte-americanos, entre os quais Massachusetts e Califórnia.

A iniciativa normativa de Nova Iorque indica que o poder público reconhece que os ativos criptográficos vieram para ficar como novos meios de pagamento, e que a sua tecnologia subjacente de cadeia de blocos é uma força potencialmente transformadora de vários aspectos da sociedade, incluindo políticas públicas e empreendedorismo privado.

Contudo, a regulação de Nova Iorque fechou corretoras e bolsas que não preenchiam os requisitos de funcionamento para obter a *BitLicense* e tem dificultado a implementação e o financiamento de *startups* de criptomoedas ante a burocracia e o alto custo relacionado com a taxação inicial para obtenção da licença e adequação das empresas, o que tem feito com que várias iniciativas, nesse campo, tenham migrado para outros Estados da federação norte-americana ou outros países¹⁹.

No Brasil se encontra em discussão, na Câmara dos Deputados, o Projeto de Lei nº 2.303, de 2015, que busca implantar controle sobre ativos criptográficos de pagamento (ACP) em geral. Tem havido discussões sobre a taxação das operações com moedas virtuais, mas o texto inicial propõe uma regulação infralegal prudencial pelo Banco Central que tenha o objetivo primordial de impedir lavagem de dinheiro

18 Item “p”, Seção 200.2 Definições, Parte 200 Moedas Virtuais, Capítulo I Regulamentos do Superintendente de Serviços Financeiros, Título 23 Departamento de serviços financeiros – Códigos, regras e regulamentos do Departamento de Serviços Financeiros do Estado de Nova Iorque. Disponível em <http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf>. Acesso em: 01 fev. 2018.

19 Fonte: <https://www.btcsoul.com/noticias/bitlicense-muito-papel-pouco-sentido/>. Acesso em: 2 fev. 2018.

e outras atividades ilícitas e a proteção do consumidor em face das corretoras, bolsas e *hackers*.

O projeto brasileiro reconhece expressamente competência ao Conselho de Controle de Atividades Financeiras – COAF para fiscalizar e regular esses “arranjos de pagamento”, termo utilizado pelos deputados federais²⁰.

O Japão optou por uma política mais liberal, ao tratar as criptomoedas como dinheiro, aplicando legislações financeiras já existentes sobre transações com *yen* aos ativos virtuais, o que vai na direção de um incentivo público às *fintechs*, que são todas as iniciativas tecnológicas para otimizar o mercado financeiro, sobretudo utilização da cadeia de blocos para agilidade e rapidez nos pagamentos sem descurar da eficiência, custo, segurança e transparência.

Outros países, como Barbados, adotaram regulamentação que permite inclusive o incremento das reservas estratégicas internacionais do país pela aquisição de criptomoedas, como forma de diversificação para pulverização de riscos econômicos sistêmicos²¹. Especula-se, por outro lado, que países fechados, como a Coreia do Norte, estejam financiando seu desenvolvimento armamentista, ao arrepio dos tratados internacionais, por meio do acúmulo de criptomoedas²².

Ponto importante e comum a todos esses países é o que permeia a eficácia dessas regulações nacionais. Normas internas que venham a regular o uso em geral de aplicativos em cadeia de blocos significarão a submissão das operações a uma autoridade nacional de controle, desvirtuando a natureza extraterritorial das operações, com possibilidade de imposição de riscos macroeconômicos aos ativos negociados e diminuição da liberdade e igualdade entre os usuários com base no local da transação.

Esses efeitos indesejados já são sentidos em face de algumas ações estatais restritivas. Em dezembro de 2017 o Banco Central chinês proibiu ofertas iniciais de moedas digitais (ICO – *Initial Coin Offering*).

20 Texto disponível em <http://www.camara.gov.br/sileg/integras/1361896.pdf>. Acesso em: 2 fev. 2018.

21 Fialdini advogados associados. Texto disponível em <https://pagamento.me/as-moedas-virtuais-e-sua-regulamentacao-em-outros-paises-parte-2/>. Acesso em: 2 fev. 2018.

22 UMPIERES, Rodrigo Tolotti. Coreia do Norte conseguiu mais de US\$ 200 milhões em bitcoin, diz especialista, *Revista Eletrônica Infomoney*. Disponível em <http://www.infomoney.com.br/mercados/bitcoin/noticia/7317718/coreia-norte-conseguiu-mais-200-milhoes-bitcoins-diz-especialista>. Acesso em: 8 mar. 2018.

Essa medida, obviamente, só se estendeu ao território chinês. A eficácia, contudo, só vem ocorrendo no sentido da paralisação das atividades de lançamento de novas moedas ou empreendimentos *blockchain* sediados e registrados na China, mas as ofertas continuaram a ocorrer, patrocinadas por chineses e voltadas para apoiadores/compradores chineses, com a única diferença de que eram registradas e sediadas em outros países. Em muitos casos os empreendedores e compradores não precisaram sequer sair da China para continuar a operar os aplicativos *peer to peer*, e o governo não pôde acusar desrespeito às suas normas restritivas.

A ineficácia das regulações nacionais se prende ao fato muito simples de que na cadeia de blocos não existe uma delimitação físico-geográfica sobre a qual o poder do Estado possa atuar. Há um desvanecimento dos conceitos de espaço e tempo pelo advento dessa nova tecnologia²³.

A *internet* alarga o processo de influência intercomunitário e os próprios Estados, quando pequenos, podem ter suas economias desestabilizadas pela movimentação brusca de grandes somas de capital em tempo exíguo, o que põe em xeque a posição histórica do controle público.

As “nuvens de informação” facilitam a criação de identidade cultural a partir de interesses comuns, desmistificando a dicotomia entre nacional e estrangeiro, com o deslocamento do sentido sistêmico de contrato social para o plano da transnacionalidade.

O ciberliberalismo não se liga ao absentismo estatal e nem acredita na utópica espera da intervenção social, abraçando o exercício da liberdade individual e coletiva de controlar o Estado pelo aumento da transparência financeira e acompanhamento das políticas de governo com base na fiscalização propiciada pela rede mundial de computadores. Basta ver o impacto político cotidiano das informações retiradas dos portais governamentais que publicam os gastos públicos.

O lugar da cadeia de blocos é o ciberespaço, e não existe o conceito clássico de soberania ou poder público nesse ambiente. A cadeia de blocos tem criado seu próprio direito, precisa e pode criar suas próprias instituições jurisdicionais arbitrais, para além da legitimação do estado-nação-territorial, o que significa dizer que só uma regulação

23 VARELLA, Marcelo Dias. *Internacionalização do Direito: Direito Internacional, globalização e complexidade*. Tese de Livre-Docência aprovada pela Universidade de São Paulo. São Paulo, 2012, p. 50

global é capaz de preservar a liberdade e a igualdade entre aqueles que decidem utilizar seu hardware para manter em funcionamento uma cadeia computacional de blocos em escala planetária²⁴.

O ciberespaço é constituído pela conjugação de todas as ferramentas utilizáveis na rede mundial de computadores, criando um universo paralelo aos fenômenos físicos em que os usuários podem agir com liberdade e igualdade de condições, posto que as diferenças culturais, legais e de tempo e espaço não prevalecem, como historicamente ocorre no mundo real²⁵.

O espaço virtual não é físico ou geográfico, de modo que ele se assemelha a uma nova fronteira, mas que não pode ser conquistada por uma única nação, pois isto redundaria em alijamento indevido de todas as outras nações. Trata-se do campo do múltiplo, ou campo da transnacionalidade²⁶.

3 A regulação transnacional minimalista da cadeia de blocos a partir da *lex mercatoria* e da *lex cryptography*

Existe o que regular no âmbito dos aplicativos em cadeia de blocos, mas essa regulação é global ou não é viável. Isso é detectável por algumas premissas que cercam o fenômeno.

A primeira delas é a de que, no ciberespaço, os Estados soberanos são apenas mais uma pessoa, ou um nó na cadeia de blocos, de modo que nesse ambiente dificilmente haverá a preservação de condições ou cláusulas exorbitantes em favor do poder público ou possibilidade de uma influência soberana hegemônica como se pode observar nas relações internacionais clássicas, baseada unicamente na força militar ou econômica.

A segunda premissa é a de que, da mesma forma que a cadeia de blocos propicia contratos entre partes privadas, não se enxerga impedimento no sentido de que o poder público se valha da *blockchain*

24 JOHNSON, David R; POST, David. *Law and borders: the rise of law in cyberspace*. Stanford Law Review, v. 48, n.5, 1996, p. 1367-1402.

25 SOUZA, Ranidson Gleyck Amâncio. Território das criptomoeças: limites à regulação estatal quanto à circulação de moedas no ciberespaço e possíveis alternativas. *Revista Brasileira de Políticas Públicas*, v. 7, n. 3, dez. 2017, p. 61 a 78.

26 COEURÉ, Benoît. **The end of easy money**. Davos Bloomberg Panels. Disponível em: <https://www.bloomberg.com/news/videos/2018-01-26/davos-panel-the-end-of-easy-money-video>. Acesso em: 29 jan. 2018.

para firmar contratos administrativos ou concretizar políticas públicas quando o ente federado se coloca como partícipe de um negócio em ambiente virtual, um hospedeiro ou validador do protocolo negocial, de modo que o princípio da equipotência libertária se impõe às próprias nações quando se trata de firmar um contrato ou até mesmo um tratado ou convenção internacional por meio da cadeia de blocos.

A terceira premissa é no sentido de que a cadeia de blocos não é um produto, um fornecedor ou uma implementação única, mas um conceito que pode ser criado e administrado por qualquer um, incluindo o próprio Estado. Trata-se de uma ferramenta para implemento e verificação de vontades no ciberespaço, de modo que as aplicações são muitas, da coleta de votos a registro de prontuários médicos, o que pode incluir o registro de licitações, contratos administrativos com empreiteiras e a concessão de benefícios ligados à seguridade social.

Desse modo, a cadeia de blocos tem natureza operacional, de simples meio para a execução da interação entre iguais, não dispensando aspectos normativos internos relacionados com cada área em que a ferramenta for aplicada. As bases do conceito de *blockchain* é que não são passíveis de legislação pelos Estados nacionais.

Nesse particular a normatização eficaz é aquela que for feita em ambiente transnacional com atenção à autorregulação consensual já existente na própria *internet*, pois não existe controle governamental único sobre ações *on line* que independem de localização física de quaisquer das partes contratantes (e muitas vezes uma das partes nem sabe onde fisicamente a outra está).

O cenário regulatório em torno da tecnologia *blockchain* se beneficiaria significativamente de uma convenção internacional que determinasse quais regimes de proteção aos investidores e consumidores são aplicáveis e em que locais vítimas de fraude ou falsas declarações podem iniciar seus processos.

As condições prévias para tal convenção estão indiscutivelmente instaladas. Existe uma convergência significativa entre o que se observa a cada dia nos Estados Unidos da América e os regimes de regulamentação de valores mobiliários da União Europeia. Substancialmente falando, a regulamentação de valores mobiliários em ambos os lados do Atlântico se destina a proteger a boa-fé objetiva.

Apesar desta convergência substancial, ainda existem fricções consideráveis entre estes dois regimes e entre os regimes de valores

mobiliários de outros países, a indicar necessidade de uniformização. Os EUA, por exemplo, tendem a restringir seus esforços normativos aos residentes nos EUA e a empresas dos EUA. Já o esforço de regulação da União Europeia tende a uma amplitude que independe da residência ou da nacionalidade dos negociadores virtuais.

A paisagem internacional atual, no que se refere à regulação das organizações de cadeias de blocos, quando presas a forças hegemônicas, sofrem um duplo risco: primeiro, que os regimes regulatórios sobrepostos exponham excessivamente os desenvolvedores e empreendedores de *startups* à insegurança jurídica territorial (desvio regulamentar); e, segundo, que o conteúdo contraditório dos regimes mine efetivamente a proteção dos investidores e dos consumidores (perplexidade regulatória).

Um outro problema poderia vir a ser o da adesão a essa potencial Convenção Internacional. A solução passaria pelos benefícios da ratificação, que deveriam exceder em muito os benefícios idiossincráticos da não ratificação. De um modo geral, uma convenção deveria ser acompanhada por uma regulamentação proibitiva unilateral, encerrando efetivamente o mercado nacional para os participantes da *blockchain* que não estiverem em conformidade com a norma geral e minimalista transnacional²⁷.

Uma Convenção Internacional para a regulação da cadeia de blocos não poderá olvidar, por outro lado, o fato de que já existe um direito costumeiro a permear as operações que se valem dessa tecnologia, sobretudo aquelas relacionadas com as criptomoedas. Essa lei entre as partes, no ambiente virtual, é reconhecível pelo direito brasileiro ante o que dispõe o artigo 4º da Lei de Introdução ao Código Civil, que reconhece o costume como fonte normativa.

O costume negocial aponta na direção de uma desnecessidade de regulação supranacional exaustiva e no sentido de que, semelhantemente ao que ocorre entre comerciantes situados em nações distintas, quando nenhum deles pode invocar a norma do seu país para solução de conflito específico, assim também deve ser reconhecida a existência de uma *lex mercatória* virtual, que resultará naturalmente em autorregulação entre

27 HACKER, Philipp. THOMALE, Chris. *Crypto-securities regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law*. Berlim e Heidelberg, 2017. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3075820. Acesso em :08 mar. 2018

as partes²⁸. Mas para além da autorregulação há o que ser regulado por meio do direito transnacional, como se passa a expor.

3.1 A ilicitude pelo anonimato

As atividades no ciberespaço que se valem da cadeia de blocos têm o poder de gerar anonimato, ainda que a operação possua rastreabilidade pelo próprio registro aberto que identifica a transação. É o que se verifica com as moedas criptografadas, pois como explica Nakamoto, o sistema é “completely decentralizaed, with no central server or trusted parties, because everything is based on crypto proof instead of trust”²⁹.

Assim, a identificação pessoal do responsável pelo negócio é praticamente impossível, o que gera uma vantagem inicial, relacionada com a preservação do direito fundamental de intimidade e vida privada, mas uma desvantagem no que toca aos fins para os quais a moeda ou o contrato são usados. Esses fins podem ser ilícitos³⁰.

As criptomoedas³¹, por esse anonimato que propiciam, já facilitaram transações na *dark web* relacionadas com compra de drogas, prostituição, financiamento de atividades terroristas e lavagem de dinheiro³².

28 SOUZA, Ranidson Gleyck Amâncio. Território das criptomoedas: limites à regulação estatal quanto à circulação de moedas no ciberespaço e possíveis alternativas. *Revista Brasileira de Políticas Públicas*, v. 7, n.3, dez. 2017, p. 61 a 78.

29 NAKAMOTO, Satoshi. *Bitcoin open source implementation of P2P currency*. P2P Foundation (Feb. 11, 2009). Disponível em <http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source>. Acesso em: 5 dez. 2017.

30 FILIPPI, Primavera de. The interplay between decentralization and privacy: the case of blockchain technologies. *Journal of Peer Production*, Issue 7: Alternative Internets. Posted on 17 oct 2016. Disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2852689. Acesso em: 5 dez. 2017.

31 O sítio eletrônico chamado *silkroad*, ou “caminho da seda”, que propunha transações anônimas na *dark web*, redundou em acusações formais contra os seus fundadores, entre os quais Ross Ulbricht, que trabalhava sob o codinome “*Dread Pirate Roberts*”. Ele foi preso em 2015 e condenado à prisão perpétua, sem possibilidade de obter liberdade condicional, sob acusações de lavagem de dinheiro, tráfico de drogas e invasão a computadores — facilitando também o trabalho de grandes cartéis de drogas. Junto com ele foram apreendidos cerca de 3,6 milhões de dólares em *bitcoins*. A propósito: *Criador do site Silk Road é condenado à prisão perpétua*. Disponível em: <http://g1.globo.com/tecnologia/noticia/2015/05/criador-do-site-silk-road-e-condenado-prisao-perpetua.html>. Acesso em: 5 dez. 2017.

32 NICA, Octavian; PIOTROWSKA, Karolina; SCHENK-HOPPÉ, Klaus Reiner. *Cryptocurrencies: Economic Benefits and Risks*. Universidade de Manchester, FinTech working paper n° 2. Outubro de 2017. Disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3059856. Acesso em 05 dez 2017.

Como já exposto, a mineração e a transferência *peer to peer* estão imunes a exigências de cadastro e identificação, bastando que sejam feitas em código aberto ratificado pelos mineradores, ou seja, não existe imunidade quanto ao uso da tecnologia de cadeia de blocos para transferências de valores com fins vedados pelo próprio direito internacional. Os mercados virtuais sozinhos não impedem a ilicitude dos fins, o que afeta a confiança do sistema, ainda que já existam tecnologias em desenvolvimento para amenização do problema.

A *startup civic33*, por exemplo, possibilita a identificação segura em diversos ambientes, impedindo fraudes. O sistema permite o uso de *QR code* para validar cada operação. Assim, o usuário se autentica em um dispositivo móvel (um celular por exemplo), usando sua digital ou face. A cada operação gera-se um código de validação, ou seja, confirma-se com a digital e o código gerado, como já fazem alguns bancos, a exemplo do Banco do Brasil.

Note-se que neste caso o Estado participa com o primeiro processo de identificação. A partir daí a empresa privada, usando a tecnologia *blockchain*, permite que o mesmo cidadão se identifique de forma simples e segura em qualquer lugar do mundo. Essa mesma tecnologia também permite o fluxo das informações pessoais a cada operação, simplificando cadastros. Por consequência, pode permitir a assinatura de contratos e a realização de pagamentos sem a necessidade de autenticação de firma ou acesso direto a conta bancária. Tudo pode se tornar automático e seguro.

Procura-se construir, no Brasil, um sistema de autenticação público, a partir da plataforma do cidadão, utilizando-se, entre outros, a base de dados de identificação de digitais do Tribunal Superior Eleitoral.

Essa mesma identificação poderia se proliferar com o uso da tecnologia de cadeia de blocos, seja diretamente, seja por meio de *startups*, para eventuais interessados, como já exposto acima. Essa possibilidade de identificação e rastreabilidade pode ser objeto de regulação em algumas situações.

Mas ainda que possam ser criados sistemas mais seguros de validação da identidade, por meio de criptografia, esse ponto, que se refere à prevenção do uso de moedas digitais para operacionalização do comércio de produtos ilícitos e lavagem de dinheiro, com possibilidade

de persecução penal para punição dos autores dessas condutas, é um primeiro ponto que desafia regulação transnacional³³.

3.2 *Pacta sunt servanda* no ciberespaço

Um segundo tópico de regulação geral, que se pode salientar, diz respeito à manutenção das condições iniciais da cadeia de blocos, ou seja, a preservação de direitos contra mudanças supervenientes das bases de lançamento da aplicação que se vale da *blockchain*.

Exemplificativamente, as plataformas normalmente limitam, de forma antecipada, a quantidade de moedas virtuais a serem emitidas em determinada rede. No caso do *bitcoin*, por exemplo, há uma limitação algorítmica ligada a vinte e um milhões de unidades de valor, o que significa garantia ao usuário contra fluxo emissor inflacionário que desvalorize o investimento. Após atingida a mineração total dessa quantia, não haveria mais mineração, mas apenas troca entre possuidores, a guindar para cima o valor das transações.

Mas como não há notícia de que alguma moeda digital tenha chegado a seu limite numérico, é impossível antecipar a maneira pela qual se poderá fazer uma expansão quantitativa daquele mercado sem violação de certas garantias fundamentais dos primeiros adquirentes.

A regulação de qualquer oferta adicional de moeda, após a proximidade do termo quantitativo final, é um ponto de regulação transnacional, sobretudo quando se vislumbra uma moeda digital como ativo global, ou seja, que permita transações entre as próprias nações sem que se faça uso de quaisquer das moedas dos países contratantes.

3.3 A responsabilização das corretoras e dos *hackers*

Quando as moedas criptográficas foram criadas a principal forma de aquisição se dava por meio da “simbiose de mineração”, em que o principal objetivo era manter o funcionamento da estrutura descentralizada da moeda, ou seja, a *blockchain*. Cada “minerador” conservava seus ganhos no disco rígido do seu computador, o que significava um risco, uma vez que esses dispositivos de armazenamento não são infensos a falhas eletrônicas ou a invasões de *hackers*.

33 LEE, Emily. *Financial inclusion: a challenge to the new paradigm of financial technology, regulatory technology and Anti-money laundering law*. Universidade de Hong Kong. Journal of business law, volume 6, p. 473-498, Hong Kong, 2017.

As corretoras de criptomoedas têm adquirido protagonismo no mercado por dois fatos: a) é preciso projetar o valor das criptomoedas no mundo físico, ou seja, fomentar e facilitar a sua troca por moedas nacionais, mercadorias e serviços; b) manter o registro contábil de uma operação com moedas digitais em ambiente de *hardware* doméstico implica assunção do risco inerente ao equipamento.

Verifique-se que as corretoras não são essenciais para a negociação de criptomoedas, assemelhando-se mais a uma casa de câmbio. As moedas podem ser transferidas de uma pessoa a outra anonimamente, o que ocorre por meio de endereços criados e criptografados na cadeia de blocos para transações individuais.

O que as corretoras fazem é, primeiro, transformar as criptomoedas em valores equivalentes em moeda nacional, e em segundo simplificar o processo, por meio de programas mais operacionais, com registro da operação em suas máquinas, assumindo o risco de defeito no equipamento. Esses dois processos são realizados em troca de uma taxa de custódia e de comissões que, em regra, superam em muito as cobradas na intermediação bancária de outros ativos financeiros³⁴.

Ocorre que a intermediação de moedas já colocadas no mercado pela cadeia de blocos traz para os clientes dessas empresas os riscos próprios da delegação de operação, sobretudo o furto do registro contábil armazenado na *blockchain* que, em última análise, é a única garantia de quem investiu³⁵.

Corretoras e bolsas de criptomoedas normalmente só aparecem como um sítio eletrônico financeiro, o que dificulta o processo judicial de responsabilização cível dessas pessoas jurídicas no caso de negligência, imperícia ou mesmo dolo no trato dos ativos virtuais de terceiros. Nada impede, por exemplo, que haja a encenação de um ataque de *hackers* e a utilização desse falso ataque como justificativa para fuga de responsabilidade.

34 A corretora “mercado bitcoin”, segunda maior do Brasil em 13/12/2017, cobra atualmente 1,99% de todos os depósitos feitos em real, na sua plataforma, para troca por *bitcoins*. A propósito: <https://www.mercadobitcoin.com.br/comissoes-razos-limites/>. Acesso em: 13 dez. 2017.

35 No início de 2014 a maior corretora de *bitcoins* do mundo, a japonesa Mt.Gox, simplesmente saiu do ar levando consigo todos os *bitcoins* dos usuários. As autoridades financeiras do Japão se limitaram educadamente a dizer que não podiam fazer nada, recusando-se a intervir ou ajudar. A propósito: VENTURA, Felipe. *Mt. Gox, maior casa de câmbio para bitcoins, desaparece com dinheiro dos usuários*. Disponível em: <http://gizmodo.uol.com.br/mt-gox-bitcoin/>. Acesso em: 13 dez. 2017.

É extremamente difícil aferir a verdade no campo da simulação virtual, sobretudo quando as operações de conversão de ativos entre o ciberespaço e o mundo real das moedas nacionais é feito de maneira tecnicamente monopolizada, por um único *insider*.

Por outro lado, a responsabilização dos atores de um *hack* real é igualmente difícil, pois como não existe autoridade de controle e o anonimato é a regra entre os usuários, não há como se valer dos mecanismos estatais típicos de punição dos ilícitos praticados por um invasor virtual, salvo por analogia, o que nem todo país permite, em face do princípio da legalidade estrita do direito penal.

3.4 Prevenção de monopólios e gestão de custos ambientais

Houve um tempo, há cerca de apenas seis a oito anos, em que a mineração de moedas virtuais era um passatempo doméstico que rendia algo, mas não muito. Atualmente a mineração de moedas digitais, no ambiente da cadeia de blocos, é uma atividade que ocasiona um imenso gasto de energia elétrica, *commodity* do mundo real produzida tanto pelo poder público como por pessoas privadas³⁶.

Uma pergunta que tem surgido, no campo das criptomoedas, é se atualmente vale a pena, sob ótica econômica, minerar esses ativos. Essa indagação deriva do fato de que a cada dia é necessário mais recursos: maior poder de processamento, melhor equipamento envolvido e maior gasto energético para a extração de criptomoedas.

A falta de uma resposta precisa para essa pergunta desencoraja muitos investidores, mas auxilia outros a aumentarem a sua fatia percentual de mineração e, conseqüentemente, de influência sobre a criptomoeda e a cadeia de blocos que a envolve.

Segundo vários sítios eletrônicos especializados, a China aposta que ainda vale a pena, e isso tem gerado uma concentração da atividade de mineração de criptomoedas cada vez maior na iniciativa privada daquele país. As empresas chinesas têm formado *pools* de mineração, ou seja, grupos privados de mineração cooperativos entre si, em vários pontos do mundo.

36 São raros os ordenamentos que fixam um monopólio de produção energética absoluto. No Brasil a iniciativa privada já é responsável por mais de 60% da capacidade de geração de energia instalada. A maior geradora de energia privada do Brasil é a empresa chinesa CTG – China Three Gorges, após a aquisição dos ativos da Duke Energy. Fonte: <http://www1.folha.uol.com.br/mercado/2017/09/1923143-empresas-privadas-ja-detem-60-da-geracao-de-energia-do-brasil.shtml>. Acesso em: 22 fev. 2018.

Em março de 2017 quatro grupos cooperativos de mineração chineses – F2pool, Antpool, BTCC e BWpool - eram responsáveis pela mineração de cerca de 57,5% de toda a moeda bitcoin do planeta³⁷. Durante o ano de 2017 e 2018 a empresa líder do Antpool, chamada Bitmain, conseguiu desenvolver o primeiro chip de computador moldado para a mineração em cadeia de blocos (chip ASIC), o que fez com que a empresa, sozinha, passasse a validar cerca de 30% de todas as transações no ecossistema virtual bitcoin³⁸.

A Bitmain restringe o acesso de terceiros à tecnologia de processamento ASIC e tem desenvolvido fazendas de mineração fora da China, como na Suíça, em que uma jurisdição mais “amigável” e um ambiente regulatório favorável estão fazendo com que um número cada vez maior de *startups* e empresas usuárias de *blockchain* e criptomoedas se estabeleçam na região.

A cidade de Zug permite o pagamento de impostos e serviços com moedas virtuais³⁹. Semelhantemente ao que ocorreu na Califórnia na década de 70 e 80, quando uma parcela do seu território passou a ser conhecida como o “Vale do Silício”, o Cantão de Zug tem sido chamado de “Vale das Criptomoedas”⁴⁰.

Essa realidade aponta para duas possibilidades: a) em um determinado momento, no futuro, quem detiver maior capacidade energética, maior poder de processamento ou melhor equipamento pode se transformar em um ator majoritário da mineração de ativos virtuais, seja uma empresa ou um país; e b) a mineração de moedas virtuais revela um risco crescente de custo ambiental.

37 Conforme Revista eletrônica Guia do bitcoin, edição de 9 de março de 2017. Disponível em: <https://guiadobitcoin.com.br/entenda-o-que-sao-pools-de-mineracao-e-quais-sao-as-melhores/>. Acesso em: 22 fev. 2018.

38 POLLOCK, Darryn. *Monopólio de mineração da Bitmain compromete a natureza descentralizada do Bitcoin*. Disponível em: <https://br.cointelegraph.com/news/bitmain-mining-monopoly-compromises-bitcoins-decentralized-nature>. Acesso em: 22 fev. 2018.

39 Crypto Valley is an ecosystem centered in and around the Swiss canton of Zug with active connections to international centers of blockchain innovation in London, Singapore, Silicon Valley and New York. A propósito, vide: <https://cryptovalley.swiss/>. Acesso em: 22 fev. 2018.

40 Facilidade de licença de atuação, redução de impostos sobre ganhos de capital e aumento de disponibilidade de crédito são os fatores que favoreceram o surgimento do Vale do Silício e são os mesmos que favorecem a criação de um “criptocurrencies valley” no centro da Suíça. A propósito, vide: NOVAES, Rafael. *Conheça a história do Vale do Silício e suas primeiras empresas*. Disponível em <http://www.psafec.com/blog/conheca-vale-silicio/>. Acesso em: 22 fev. 2018

Custos ambientais compreendem os gastos relacionados direta ou indiretamente com a proteção do meio ambiente tendo em vista a necessidade de extração e produção de bens econômicos⁴¹.

Uma vez que as moedas digitais se projetem como um ativo global de negociação, é possível que países ou empresas detentoras de maior tecnologia de produção energética ou com muito poder de processamento de dados passem à condição de monopolizadores da atividade de validação de transações na *blockchain*, com o objetivo de concentrar a titularidade de criptomoedas como bens estratégicos em termos de relações comerciais e internacionais.

Assim, a positivação internacional de mecanismos de prevenção dessas práticas monopolistas merece atenção no diploma que vier a estabelecer uma regulação mundial das aplicações em cadeia de blocos, sobretudo no que se refere à sua aplicação para lançamento e manutenção de moedas virtuais.

Por outro lado, os impactos ambientais motivados pelo aumento de demanda energética para mineração de criptomoedas precisa ser mensurado e precisam ser estabelecidas fórmulas de compensação de custos entre países como forma de equilibrar a disputa pela validação das transações. Esse é outro ponto de regulação transnacional.

Considerações finais

O ciberespaço, enquanto local desmaterializado que deriva do surgimento da rede mundial de computadores, caracteriza-se como um espaço de comunicação equipotente entre seus usuários, onde as pessoas estão protegidas da subordinação política e podem dar vazão à sua liberdade de contratar e negociar sem imposições estatais, mas desde que haja uma proteção mínima calcada na mundialização do direito, pois onde há risco deve existir regulação.

A ferramenta descentralizada da cadeia de blocos integra um conjunto de fenômenos recentes, que vão da globalização ao surgimento da *internet*, da heterodoxia das Constituições à influência mundial de grupos privados, e todos esses fenômenos atentam contra a visão de soberania absoluta das nações, a atestar a redução do poder estatal no seu papel de produtor do direito.

41 CALLADO, A. L. C. *A importância da gestão dos custos ambientais*. Disponível em <http://www.biblioteca.sebrae.com.br>. Acesso em: 21 fev. 2018.

O controle desses fatos disruptivos unicamente pelo direito transnacional é marca da interdependência que se desenvolve no seio de uma economia globalizada. Os governos sofrem uma erosão em sua autoridade política em face da porosidade das fronteiras, da dificuldade de controle de fluxos monetários, de mercadorias e informação. Trata-se de um caminho sem volta.

A *blockchain* nunca poderá, conceitualmente, ser uma instituição estatal, pois mesmo que o Estado seja seu criador a adesão não impositiva à mesma é que marcará o seu funcionamento, e essa relação entre usuários sempre partirá de uma horizontalidade coordenada, nunca de uma verticalidade subordinante.

As tentativas de regulação nacional das aplicações em cadeia de blocos esbarram, portanto, na falta de eficácia pela imaterialidade do local de aplicação, que é o ciberespaço, onde já existe uma densidade normativa multicultural, aberta, múltipla e relacional⁴²: a autorregulação costumeira dos usuários e as próprias condições iniciais para desenvolvimento criptográfico da *blockchain*.

Contudo, o anonimato garantido aos que transacionam nesse ambiente pode ser o motor de práticas ilícitas, sobretudo no campo financeiro. A manutenção das condições iniciais garantidas aos usuários que decidiram aderir à rede deve ser garantida. A fixação de proteção contra corretoras e *hackers*, com possibilidade de punição da má-fé, é necessária. Os riscos estruturais de monopólio e custos ambientais precisam ser gerenciados.

A enumeração de temas relacionados com cadeia de blocos que merecem regulação transnacional não é exaustiva e serve tão-somente para ratificar as opiniões no sentido de que a fonte normativa não deve estar exclusivamente em um Estado-nação⁴³.

Esses pontos pedem regulação transnacional, assim entendida a norma que seja feita a partir da contribuição igualitária de todos os envolvidos e interessados, ainda que não se dispense a anuência dos Estados e sua força cogente de execução. Em outros termos, a norma

42 MASSEY, Doreen. *Pelo espaço: uma nova política da espacialidade*. Tradução de Hilda Pareto Maciel e Rogério Haesbaert. Rio de Janeiro: Bertrand Brasil, 2008, p. 95.

43 COEURÉ, Benoît. *The end of easy money*. In: Davos Bloomberg Panels. Disponível em <https://www.bloomberg.com/news/videos/2018-01-26/davos-panel-the-end-of-easy-money-video>. Acesso em: 29 jan. 2018.

reguladora da cadeia de blocos deve ser produzida no meio privado, mas implementada pelo Direito estatal.

Referências

CALLADO, A. L. C. *A importância da gestão dos custos ambientais*. Disponível em: <http://www.biblioteca.sebrae.com.br>. Acesso em: 21 fev. 2018.

COEURÉ, Benoît. *The end of easy money*. In: Davos Bloomberg Panels. Disponível em <https://www.bloomberg.com/news/videos/2018-01-26/davos-panel-the-end-of-easy-money-video>. Acesso em: 29 jan. 2018.

FILIPPI, Primavera de. The interplay between decentralization and privacy: the case of blockchain technologies. *Journal of Peer Production*, Issue 7: Alternative Internets. Posted on 17 oct 2016. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2852689. Acesso em: 5 dez. 2017.

GANDEL, Stephen. *Opinião: bolha bitcoin vai estourar sob pressão da oferta*. Disponível em: <https://economia.uol.com.br/noticias/bloomberg/2017/11/28/bolha-da-bitcoin-vai-estourar-sob-pressao-de-oferta-gadfly.htm>. Acesso em: 1 dez. 2017.

HACKER, Philipp. THOMALE, Chris. *Crypto-securities regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law*. Berlim e Heidelberg, 2017. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3075820. Acesso em: 8 mar. 2018.

HARARI, Yuval Noah. *Sapiens: uma breve história da humanidade*. L&PM: Porto Alegre, 2017.

JOHNSON, David R; POST, David. Law and borders: the rise of law in cyberspace. *Stanford Law Review*, v. 48, n. 5, 1996.

LEE, Emily. Financial inclusion: a challenge to the new paradigm of financial technology, regulatory technology and Anti-money laundering law. *Journal of Business Law*, v. 6, p. 473-498, 2017.

MASSEY, Doreen. *Pelo espaço: uma nova política da espacialidade*. Tradução de Hilda Pareto Maciel e Rogério Haesbaert. Rio de Janeiro: Bertrand Brasil, 2008.

MUSE, Alexander. *How the NSA identified Satoshi Nakamoto*. Ago. 2010. Disponível em: <https://medium.com/cryptomuse/how-the-nsa-caught-satoshi-nakamoto-868affcef595>. Acesso em: 8 nov. 2017.

NAKAMOTO, Satoshi. *Bitcoin: A Peer-to-Peer Eletronic Cash System*. Mai. 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 7 nov. 2017.

NAKAMOTO, Satoshi. Bitcoin open source implementation of P2P currency. P2P Foundation (Feb. 11, 2009). Disponível em <http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source>. Acesso em: 5 dez. 2017.

NOVAES, Rafael. *Conheça a história do Vale do Silício e suas primeiras empresas*. Disponível em: <http://www.psafe.com/blog/conheca-vale-silicio/>. Acesso em: 22 fev. 2018.

NICA, Octavian; PIOTROWSKA, Karolina; SCHENK-HOPPÉ, Klaus Reiner. Criptocurrencies: Economic Benefits and Risks. Universidade de Manchester, *Fintech Working Paper*, n. 2, out. 2017. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3059856. Acesso em: 5 dez. 2017.

POLLOCK, Darryn. *Monopólio de mineração da Bitmain compromete a natureza descentralizada do Bitcoin*. Disponível em: <https://br.cointelegraph.com/news/bitmains-mining-monopoly-compromises-bitcoins-decentralized-nature>. Acesso em 22 fev. 2018.

SOUZA, Ranidson Gleyck Amâncio. Território das criptomoedas: limites à regulação estatal quanto à circulação de moedas no ciberespaço e possíveis alternativas. *Revista Brasileira de Políticas Públicas*, v. 7, n. 3, dez. 2017.

TAKAR, Téó. Empresas que começaram “no fundo do quintal” dominam mercado de bitcoins no Brasil. Disponível em: <https://www.uol/economia/especiais/corretoras-de-bitcoins.htm#faturando-alto-com-bitcoins>. Acesso em: 13 dez. 2017.

TOCQUEVILLE, Alexis. *A democracia na América*. São Paulo: Martins Fontes, 1998.

UMPIERES, Rodrigo Tolotti. Coreia do Norte conseguiu mais de US\$ 200 milhões em bitcoin, diz especialista. *Revista Eletrônica Infomoney*. Disponível em: <http://www.infomoney.com.br/mercados/>

[bitcoin/noticia/7317718/coreia-norte-conseguiu-mais-200-milhoes-bitcoins-diz-especialista](#). Acesso em: 08 mar. 2018.

VARELLA, Marcelo Dias. *Internacionalização do Direito: Direito Internacional, globalização e complexidade*. Tese de Livre-Docência aprovada pela Universidade de São Paulo. São Paulo, 2012.

VENTURA, Felipe. Mt. Gox, maior casa de câmbio para bitcoins, desaparece com dinheiro dos usuários. Disponível em: <http://gizmodo.uol.com.br/mt-gox-bitcoin/>. Acesso em: 13 dez. 2017.

WRIGHT, Aaron; FILIPPI, Primavera de. *Decentralized blockchain technology and the rise of lex cryptographia*. Mimeo. Disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664. Acesso em: 1 dez. 2017.

Recebido em: 18 de julho de 2018.

Aceito em: 06 de dezembro de 2018.