ISSN Impresso 1809-3280 | ISSN Eletrônico 2177-1758
www.esmarn.tjrn.jus.br/revistas

BLOCKCHAIN, VULNERABILIDADE NAS RELAÇÕES JURÍDICAS NEGOCIAIS E A ALTERNATIVA AO MODELO HIERÁRQUICO DE CERTIFICAÇÃO DIGITAL

BLOCKCHAIN, VULNERABILITIES IN LEGAL BUSINESS RELATIONS AND THE ALTERNATIVE TO THE HIERARCHICAL DIGITAL CERTIFICATION MODEL

Roberto Pôrto Nogueira*
Guilherme Mesquita Estêves**

RESUMO: O Brasil adota o modelo hierárquico de certificação digital, no qual a fonte de legitimação de todos os certificados emitidos é, em última análise, a autoridade certificadora raiz, assim definida por normativa federal. Significa que a confiança pretendida para a cadeira de certificação se fundamenta na previsão normativa do monopólio da regulação. Assim, o problema de estudo consiste em saber se a tecnologia *blockchain* pode contribuir para a proposta de um modelo de certificação digital que contemple a tutela da vulnerabilidade nas relações negociais de Direito Privado havidas em ambiente eletrônico, especialmente na promoção de modelo mais participativo e inclusivo. O artigo objetiva propor, por meio do raciocínio lógico-dedutivo aplicado a um estudo teórico-dogmático interdisciplinar, possibilidades da tecnologia *blockchain* e suas potenciais repercussões para o panorama das eventuais vulnerabilidades, novos direitos e novos sujeitos em relações negociais marcadas pela certificação digital. A

* Doutor e mestre em Direito Privado pela Pontifícia Universidade Católica de Minas Gerais (PUC-Minas). Especialista em Direito Tributário pela Faculdade de Direito Milton Campos Belo Horizonte. Pesquisador do Núcleo de Estudos Novos Direitos Privados (NDP) e do Centro de Estudos em Biodireito (CEBID/UFOP). Professor do Curso de Graduação e Mestrado Acadêmico em Novos Direitos, Novos Sujeitos da Universidade Federal de Ouro Preto (UFOP). Apoiado por Auxílio Pesquisador UFOP 2017-2018-2019. Ouro Preto – MG – Brasil.

** Mestrando em Direito da Universidade Federal de Ouro Preto (UFOP). Pesquisador do Núcleo de Estudos Novos Direitos Privados (NDP) e do Centro de Estudos em Biodireito (CEBID/UFOP). Ouro Preto – MG – Brasil.

relevância do trabalho evidencia-se na medida em que o modelo hierárquico rígido pode representar barreira à participação de atores com premissas ou finalidades diversas, o que engendra posições de exclusão. Conclui-se que a *blockchain*, ao promover a descentralização da informação, a pluralização dos responsáveis pela cadeia de confiança e a multiplicação das portas de acesso, apresenta-se como tecnologia promissora à contribuição para a tutela de vulnerabilidades e para a integração de novos sujeitos, no contexto da revelação de alternativas ao modelo hierárquico de certificação digital.
Palavras-chave: *Blockchain*. Vulnerabilidade. Certificação digital. Tecnologia da informação. Relações negociais.

ABSTRACT: Brazil adopts the hierarchical model of digital certification, in which the source of legitimization of all certificates issued is, at the end, the root certification authority, defined by federal regulations. It means that the trust intended for the certification network is based on the normative which establishes the monopoly of the regulation. Thus, the study problem consists in knowing if the blockchain technology might contribute to the proposal of a digital certification model that contemplates the protection of the vulnerability in the Private Law business relationships in the electronic environment, especially in the context of the promotion of a more participatory and inclusive model. The article aims to propose, through logical-deductive reasoning applied to an interdisciplinary theoretical-dogmatic study, possibilities of blockchain technology and its potential repercussions for the panorama of occasional vulnerabilities, new rights and new subjects in business relations influenced by digital certification. The relevance of the work is evident since the rigid hierarchical model might represent an obstacle to the participation of players with different premises or purposes, which engenders positions of exclusion. It is concluded that blockchain, by promoting the decentralization of information, the pluralization of those responsible for the chain of trust and the multiplication of access doors, is a promising technology to contribute to the protection of vulnerabilities and to the integration of new subjects, once it reveals alternatives to the hierarchical model of digital certification.
Keywords: Blockchain. Vulnerability. Digital certification. Information technology. Business relationships.

SUMÁRIO: 1 INTRODUÇÃO; 2 ESTRUTURA E FUNCIONAMENTO DA *BLOCKCHAIN*; 3 NOTÍCIA SOBRE O PANORAMA TÉCNICO DA *BLOCKCHAIN*; 4 VULNERABILIDADE, RELAÇÕES NEGOCIAIS E CONTRATOS INTELIGENTES; 5 A CERTIFICAÇÃO DIGITAL NO BRASIL E AS ALTERNATIVAS DA *BLOCKCHAIN*; 6 CONCLUSÃO; REFERÊNCIAS.

1 INTRODUÇÃO

Regimes jurídicos materiais, processuais e probatórios (documentais) no Direito preparam-se para viabilizar o acontecimento amparado de relações jurídicas negociais constituídas em meio digital, de modo que já são de conhecimento da comunidade jurídica as noções próprias de tecnologia que envolvem assinatura e certificação digital, atreladas a aspectos de criptografia assimétrica, tidas por eficientes no Brasil quando hierarquicamente estruturadas em um sistema de chaves controlado, gerido e prevalentemente mantido pelo poder público. Se a economia precisa lidar com tecnologias que articulam moedas e mercados digitais, é bem verdade que ao Direito cabe regular relações jurídicas, aperfeiçoar seus modelos e superar conflitos oriundos desse cenário.

O panorama transformado da economia, em razão da utilização de criptomoedas, tanto como forma de pagamento e investimentos quanto na firmação de contratos inteligentes alicerçados na tecnologia *blockchain*, revela novas lacunas jurídicas. Nesse tocante, parte das técnicas que envolvem o mercado impactado por criptomoedas guarda semelhanças com as tecnologias já úteis ao Direito na atualidade.

Ocorre que criptomoedas e contratos inteligentes, ao promoverem novos modelos, novos sujeitos e mesmo novos direitos, carecem de regulamentação jurídica adequada, de modo que os principais desafios de percepção jurídica do fenômeno tecnológico referem-se, precisamente, à tecnologia conhecida como *blockchain* e suas possibilidades. Ganha relevo, assim, a elucidação das vicissitudes

instituídas pela *blockchain*, como modelo tecnológico que investe na descentralização da criação e preservação da informação emergente na rede como medida de segurança, vale dizer, de solidificação dos pilares de confiança. Nessa medida, indaga-se como essa tecnologia pode contribuir para a tutela da vulnerabilidade nas relações negociais de Direito Privado havidas em ambiente eletrônico.

A *blockchain* pode provocar mudanças significativas nas interações humanas, sobretudo nas de cunho negocial, cabendo ao Direito aferir as possibilidades que se descortinam a partir da utilização dessa tecnologia.

Busca-se o traçado de um panorama sobre a tecnologia *blockchain*, com ênfase na observância de potenciais impactos de seu uso no contexto das relações negociais marcadas pelo emprego de certificação digital, em especial na dimensão da vulnerabilidade de sujeitos contratantes.

Em uma perspectiva teórica, que considera a interface entre tecnologia e Direito, objetiva-se investigar e elucidar, em revisão de literatura, a estrutura e a função mais evidentes da *blockchain*, para, propositivamente, permitir alusões ao redesenho de modelos jurídicos havidos no âmbito das relações negociais, e, especialmente, de percepção do fenômeno e dos espaços de exercício de liberdades. Pela via do raciocínio lógico-dedutivo, parece possível desvendar ou levantar linhas discursivas, argumentativas, práticas e formativas de arquétipos úteis à comunidade jurídica que, fatalmente, há de deparar-se com celeumas advindas do emprego da tecnologia em alusão.

Cabe, nesse propósito, a abordagem dos aspectos estruturais e técnicos da *blockchain* a fim de que seja contextualizada a posterior análise de vulnerabilidades em relações negociais e em contratos inteligentes. Há, por fim, o enfrentamento dos meandros da temática da

certificação digital no Brasil e a construção de proposições alternativas por meio da descentralização possibilitada pela *blockchain.*

2 ESTRUTURA E FUNCIONAMENTO DA *BLOCKCHAIN*

Em uma conceituação preliminar sumária, pode-se dizer que a *blockchain* é um banco de dados que se diferencia dos tradicionais pela estrutura descentralizada que resulta da pluralização de seus mantenedores. Trata-se de uma forma de armazenar registros de agentes, de objetos contratuais, de termos de avenças, para operacionalização de transações e até mesmo para a constituição ou manutenção de unidades de troca, ligadas a titulares específicos. Assim, a estrutura das bases de dados mais comuns, utilizadas no trato negocial no contexto de mercado, comporta aspectos subjetivos e objetivos.

As relações negociais podem admitir uma plêiade de subjetividades juridicamente categorizadas, a depender do regime normativo aplicável. Diante da complexidade do trato negocial da atualidade, é ordinário que as relações sejam firmadas entre sujeitos desconhecidos entre si ou mesmo entre pessoas cuja credibilidade dependa mais de sua reputação no mercado do que de posturas pessoais mais particulares. Isso faz com que sejam necessários intermediários para a facilitação das tratativas ou para figuração como terceiro escolhido pelas partes, apto a calcular ou minimizar riscos envolvidos. Usualmente, esse terceiro intermediador obtém a remuneração de seus serviços na medida de sua atuação, o que costuma integrar, inclusive, a manutenção de base de dados, sob sua responsabilidade. Esses intermediadores, que podem laborar individualmente ou em cadeia, com ou sem a dependência de ente estatal, figuram em tais relações como "terceiro envolvido". Erige-se, a partir disso, uma relação de confiança, pois os sujeitos em questão confiam que o "terceiro envolvido" responsabilize-se na medida de sua prometida participação.

Significa que há centralização subjetiva de responsabilidades, vale dizer, ainda que a responsabilidade por tais registros seja compartilhada, os sujeitos são conhecidos e o espectro subjetivo aparece bem delimitado.

Cabe explicar, por exemplo, que, em contratos empresariais relacionados a cartões de crédito, os sujeitos que transacionam confiam que a companhia administradora controlará e implementará as ações necessárias à movimentação financeira correlata à negociação, sendo certo que, por seus serviços e por sua apreciação e minimização dos riscos envolvidos na seleção dos agentes aptos a operar em sua cadeia de negócios, recebe remuneração, que varia desde o recebimento de frutos civis até a percepção de prestação financeira por venda de serviços e produtos específicos. Em todo caso, as partes admitem o uso dos cartões de crédito com a confiança no potencial patrimonial das administradoras e bancos envolvidos para arcar com responsabilidades contratualmente firmadas.

Do mesmo modo, em transações mercantis nas quais emprega-se o pagamento em dinheiro, trata-se de hipótese em que se privilegia o papel-moeda como unidade de troca, cuja aceitação depende, invariavelmente, da credibilidade do poder público, que aparece como "terceiro envolvido". As partes tendem a confiar no potencial de troca do papel-moeda, que corresponda a uma determinada fração da riqueza.

Com um desenho diverso, surge em 2008 a tecnologia *blockchain*, que visa à descentralização como medida de segurança e de confiança. As redes fundadas nessa tecnologia funcionam de forma pública, compartilhada e universal, não havendo a figura de terceiros intermediários. Logo, o acesso é franqueado aos interessados à participação na manutenção ou teste da segurança da base de dados, bem como é livre o uso do modelo para uso de moedas eletrônicas para pagamento de obrigações oriundas de contratos, eletrônicos ou não.

Além dessa publicidade, dá-se o compartilhamento amplo da possibilidade de validação recíproca entre os sujeitos integrados. Por fim, a adesão subjetiva à rede é universal, sem restrições que não sejam de ordem meramente tecnológica (há requisitos tecnológicos para a integração subjetiva ao modelo, além de aspectos de programação computacional que são preservados ao grande público).

O modelo da *blockchain* é estruturalmente diverso dos tradicionais, na medida em que emprega tecnologia específica que busca assegurar integridade e autenticidade das informações, valendo-se da descentralização subjetiva para implementar, igualmente, uma descentralização objetiva, o que significa que as próprias bases de dados e os elementos estruturais de sua composição são dissipados no espaço, para admitir pluralidade de formatos técnicos e de situações geográficas.

Destaca-se, assim, a nova tecnologia como significativamente relevante em países onde há problema de confiança no governo. Afinal, esse formato público, universal e compartilhado parece apto a transportar o referencial subjetivo da confiança, que passa pelo fenômeno de descentralização, acarretando o deslocamento de sua imputação, que se afasta de alguns sujeitos (pessoas naturais, jurídicas de direito público ou privado), para promover o alargamento do espectro de sujeitos responsáveis pela chancela da informação. Vale dizer, o problema da confiança foi o principal combustível para o surgimento da rede *blockchain*, e é o que continua atraindo cada vez mais pessoas a se utilizar da tecnologia (GATES, 2017). O conceito de *blockchain* é recorrentemente confundido com o de *bitcoin*; porém, há distinção.

Instituições públicas e bancos de dados centralizados tendem a funcionar melhor quando há confiança nas instituições jurídicas e no poder público, engendrada no cenário de um Estado de Direito. Diante da eventual fragilidade dessa estrutura, tem-se que bases de dados descentralizadas, construídas na tecnologia *blockchain*, tendem a agregar

força à credibilidade das instituições centralizadas. Tais instituições perdem o monopólio da confiança, passando a figurar como mais um de seus agentes, uma vez que todos os envolvidos podem acessar e chancelar transações, o que promove o aperfeiçoamento do ambiente de transparência. Não é sem razão que a noção de confiança tem sido o mote nuclear da tecnologia *blockchain*, que propõe municiar um sistema de acreditação entre pessoas, sem a necessidade de intermediários envolvidos nas transações (GATES, 2017).

3 NOTÍCIA SOBRE O PANORAMA TÉCNICO DA *BLOCKCHAIN*

A origem do termo *blockchain* merece um aparte explicativo: refere-se a uma cadeia de blocos que se interconectam à medida que mais informações são adicionadas à rede. Uma série de transações ocorre de modo simultâneo, de forma que elas são então agrupadas e adicionadas em um novo bloco. Este novo bloco é então adicionado em uma posição subsequente ao bloco anterior. Com essa conexão dos blocos de informações, cria-se uma corrente de blocos. Desse cenário deriva a ideia de *blockchain*. Um novo bloco sempre se refere ao bloco anterior, e este, por sua vez, refere-se ao anterior, de forma a remontarem ao bloco inicial, também chamado de "bloco genesis" (NORMAN, 2017). Em um ambiente descentralizado, qualquer pessoa pode navegar pelos blocos e ter acesso às informações ali impressas, não havendo nenhum banco de dados central ou autoridade relacionada aos blocos, o que garante um grau elevado de transparência à rede. Qualquer controvérsia de informações entre usuários da rede pode ser solucionada de forma razoavelmente simples, bastando que se faça uma remissão ao bloco em que a informação foi inserida. Os blocos adicionados à *blockchain* não podem ser adulterados, pois eles estão permanentemente ligados à cadeia de blocos, tornando-se parte de um todo. Conforme dito, cada bloco se refere ao bloco imediatamente anterior, de forma que, caso alguém

consiga comprometer a integridade do registro eletrônico, ele perde a identificação com a cadeia, deixando, nessa medida, de ser chancelado pela rede. Isso significa que, a menos que todos os blocos anteriores e posteriores àquele sejam igual e validamente modificados para corresponderem entre si, e que consigam se fazer equivaler, desse modo, aos blocos pregressos, seria praticamente impossível do ponto de vista computacional a quebra dessa estratégia de segurança. Tal iniciativa demandaria, além de tempo extremamente longo, enorme energia computacional (GATES, 2017). Dessa forma, o número de blocos posteriores a uma transação também pode ser visto como confirmação de que dada informação permanecerá intacta dentro da *blockchain*.

Sempre que um novo bloco de transações é adicionado, todos os usuários que compartilham cópias da *blockchain* veem o banco de dados ser atualizado com o registro das novas informações. Como a rede é aberta (pública e universal) e descentralizada (compartilhada), todos os envolvidos podem ter acesso a uma cópia dos registros e verificar a verossimilhança de eventuais novidades informativas (blocos).

A descentralização da rede implementa o panorama de "consenso distribuído", que consiste no fato de que, para que uma transação seja aceita e adicionada à *blockchain*, é preciso que a maioria das pessoas da rede concordem, objetivamente (por aferição da correspondência e coerência entre dados pregressos e novos), com a ocorrência de transação regular (tecnicamente válida). A exigência de que a totalidade da rede concorde com uma transação seria inviável, pois poderia haver alguém com propósito de fraudar informações para se beneficiar de alguma forma. Por isso, na maioria das *blockchain*s em funcionamento atualmente, exige-se o consenso de mais de 50% dos envolvidos na rede para que uma transação seja considerada tecnicamente válida e o bloco seja adicionado à rede (GATES, 2017).

Requerimentos de novas transações são constantemente enviados para a rede a fim de serem validadas e incluídas na *blockchain*. Para que se validem tais transações e o novo bloco seja adicionado, os computadores da rede devem resolver um problema computacional. Com a resolução do problema, o bloco se torna válido e é, então, adicionado à *blockchain*. São vários os computadores que tentam resolver o referido problema computacional, mas somente aquele que o fizer primeiro poderá adicionar o bloco, recebendo por isso uma recompensa que é comumente um montante na moeda virtual (criptomoeda, no caso da *bitcoin*), usada naquela rede (NORMAN, 2017). A esse processo é dado o nome de mineração. A recompensa é garantida aos mineradores que conseguem resolver o problema computacional, também chamado de prova de trabalho, que corresponde ao esforço exitoso de adicionar um bloco válido à rede.

Os mineradores contribuem para a manutenção e continuidade da rede com recursos computacionais, tempo e energia elétrica. Essa prova de trabalho é um desafio matemático com um nível de dificuldade preestabelecido pela rede e a solução é facilmente verificável após a resolução do problema (GATES, 2017). O sistema de prova de trabalho demanda vasto poder computacional e, consequentemente, muita energia, motivo pelo qual tem sido criticado e até mesmo substituído por outros métodos (prova de participação e prova de capacidade, alheios ao estudo) em algumas redes *blockchain* (TAKASHIMA, 2017).

A *blockchain*, portanto, tem um afluxo de segurança por sua sujeição ao falseamento. A busca pela solução de problemas matemáticos funciona como um sistema de teste e de crescimento continuado da estrutura da rede.

Em suma, *blockchain* é uma nova tecnologia de armazenamento de dados por meio da qual os blocos de informação são ligados entre si, criptograficamente, a fim de evitar adulteração. Preserva, assim, a

integridade do registro eletrônico. A autenticidade é assegurada pela descentralização e chancela da informação mantida ou acrescida pela maioria dos usuários ou participantes.

Como dito, o principal exemplo de uso da tecnologia *blockchain* é o da moeda *bitcoin*. Porém, a tecnologia vai muito além da criação de uma unidade digital de troca voltada para uso no mercado, podendo ser empregada para outros fins. Em termos teleológicos, a despeito de intentar a mesma preservação e segurança das bases de dados, a tecnologia em comento pode contemplar, ainda, finalidades ligadas à edificação de modelos negociais mais eficientes, com a supressão de intermediários e, por conseguinte, com redução de custos. Cabe, portanto, aludir possibilidades dessa tecnologia à tutela de relações jurídicas negociais que envolvem vulneráveis e às alternativas ao processo de certificação aplicável a essa experiência, havida em meio eletrônico.

4 VULNERABILIDADE, RELAÇÕES NEGOCIAIS E CONTRATOS INTELIGENTES

O prefixo *vulnus* significa fragilidade, fragilidade esta advinda da desigualdade existente entre membros da sociedade, que, ao mesmo tempo que possuem aspectos em que se igualam, apresentam diferenças (MARQUES; MIRAGEM, 2012). E se o Direito tem como uma de suas metas constitucionalmente firmadas a superação de desigualdade, um dos caminhos possíveis e a análise e a proteção da vulnerabilidade e das posições jurídicas por ela marcadas.

A igualdade que, inobservada, tende a deflagrar vulnerabilidades, é a igualdade que contempla a isonomia, a equidade, a diversidade, com imprescindibilidade da perspectiva do pluralismo epistemológico. Desse modo, apenas "é viável materializar a igualdade se a diferença for percebida, a vulnerabilidade, reconhecida e as oportunidades, distribuídas de maneira a contrapesar e viabilizar,

efetivamente, iguais liberdades fundamentais" (FIUZA; NOGUEIRA; SILVA, 2016, p. 162, v. 1).

A despeito da proximidade da vulnerabilidade com a noção de igualdade, dela se distingue. A vulnerabilidade não depende de processos comparativos. Lado outro, somente é pertinente falar em vulnerabilidade no contexto de admissão de peculiaridades subjetivas (FIUZA; NOGUEIRA; SILVA, 2016, v. 1).

> O paradigma da igualdade parte de uma visão macro, do homem e da sociedade, noção mais objetiva e consolidada, onde a desigualdade se aprecia sempre pela comparação de situações e pessoas, de acordo com a máxima aristotélica: tratar igualmente os iguais, e desigualmente os desiguais, na medida da sua desigualdade, para alcançar o justo. Já a vulnerabilidade é filha deste princípio, mas noção flexível e não consolidada, com os traços de subjetividade que a caracterizam: a vulnerabilidade não necessita sempre de uma comparação entre situações e sujeitos. Poderíamos afirmar, assim, que a vulnerabilidade é mais um estado da pessoa, um estado inerente de risco ou um sinal de confrontação excessiva de interesses identificado no mercado, é uma situação permanente ou provisória, individual ou coletiva, que fragiliza, enfraquece o sujeito de direitos, desequilibrando a relação. A vulnerabilidade não é, pois, o fundamento das regras de proteção do sujeito mais fraco, é apenas a "explicação" destas regras ou da atuação do legislador, é a técnica para as aplicar bem, é a noção instrumental que guia e ilumina a aplicação destas normas protetivas e reequilibradoras, à procura do fundamento da igualdade e da justiça equitativa (MARQUES; MIRAGEM, 2012, p. 117).

A vulnerabilidade, portanto, é critério multidimensional, plural e aberto às expressões de dignidade da pessoa, que não demanda,

necessariamente, categorização ou comparação. Assim, identificada, a vulnerabilidade pode explicitar a lacuna na concretização da proposta constitucional de sociedade solidária e democrática, para embasar políticas públicas, normativas ou não, bem como para auxiliar no filtro e na interpretação de regimes jurídicos aplicáveis.

Tal vulnerabilidade pode integrar o âmbito das relações jurídicas negociais e obrigações correlatas. O contrato é uma das fontes de obrigação, devido às suas múltiplas formas e inúmeras repercussões no mundo jurídico (GONÇALVES, 2004, v. 3). Trata-se de espécie de negócio jurídico fundado na vontade humana, com balizas impostas pelo ordenamento jurídico; em outras palavras, o contrato é um acordo de vontades para o fim de adquirir, resguardar, modificar ou extinguir direitos e obrigações.

Com a suposta superação do liberalismo econômico e implementação do Estado Social, ficou mitigada a obrigatoriedade do contrato como objeto de consentimento mútuo, regido pela autonomia da vontade, de forma que a teoria contratual está, atualmente, permeada pela chamada "função social" do contrato, que possibilita a intervenção estatal no acordo de vontades com o mister de relativizar desigualdades. Paulo Nalin (2011, p. 58) destaca o surgimento dessa visão intervencionista do Estado com o objetivo de proteger os interesses sociais:

> E nesta perspectiva, a teoria do direito contratual clássica, aquela em que se valoriza a autonomia privada, em nome de um modelo econômico liberal, cede espaço à proteção pelo Estado dos interesses sociais. Cresce a intervenção estatal nas relações privadas, a fim de garantir a proteção dos interesses sociais nas relações interprivadas.

A constante intervenção estatal nas relações jurídicas privadas é justificada para assegurar a supremacia da ordem pública, relegando o individualismo a um plano secundário (GONÇALVES, 2004, v. 3). Surge um dirigismo contratual que, em tese, interessa a toda a coletividade. Segundo Caio Mário (PEREIRA, 2003, v. 3), a função social do contrato serve precipuamente para limitar a autonomia da vontade quando tal autonomia esteja em confronto com o interesse social e esse deva prevalecer.

Conforme panorama explicitado, pode-se observar que as relações jurídicas negociais entre particulares são, hodiernamente, permeadas pela intervenção estatal, no sentido de se garantir a ordem pública, com correção de discrepâncias entre as partes contratantes e mitigação de vulnerabilidades, tudo conforme os princípios da função social do contrato e da boa-fé objetiva, ambos encampados no Código Civil (BRASIL, 2002).

Nesse contexto, chama-se a atenção para o potencial inovador das relações jurídicas negociais travadas por meio de uma *blockchain*. Através desta tecnologia, que possibilita um ambiente de negócios seguro, transparente e confiável, eventuais vulnerabilidades de sujeitos contratantes tendem a ser minimizadas, uma vez que o espectro de proteção da informação e dos termos de contrato é alargado e subjetivamente dissipado. A substituição de um interventor por inúmeros guardiões pode, igualmente, contribuir para o reconhecimento ou rechaçamento de determinada prática em desacordo com o panorama contratual.

De fato, os escândalos envolvendo governos, em conluio com instituições financeiras e grandes corporações, colocam em evidência a fragilidade da proteção proporcionada por um ente centralizado por meio de leis e regulações que permeiam, cada vez mais, a vida dos cidadãos. A sociedade civil, nesse contexto, vê-se obrigada a buscar soluções para os

inúmeros problemas ocasionados pelo padrão centralizado de transferência de dados e transações comerciais. É nesse contexto que a arquitetura *blockchain* surge para assumir um novo papel: o de facilitador (para a otimização da segurança, privacidade, transparência e velocidade) e de *gatekeeper* (guardião) na "Era da Confiança" (PISCINI; HYMAN; HENRY, 2017). Ao permitir a execução de aplicativos e contratos de maneira segura – garantindo a interação direta entre indivíduos desconhecidos em uma rede distribuída e sem a necessidade de intermediários ou validadores de confiança –, as infraestruturas *blockchain* eliminam incertezas e introduzem uma nova maneira de conferir confiança às interações humanas, com potencial mitigador de vulnerabilidades nas relações negociais.

Há, ainda, que se falar em inclusão de sujeitos no contexto dos negócios acontecidos em meio eletrônico, que se valem de certificação digital. Se, com tecnologias que adotam a lógica da *blockchain*, o reconhecimento da autenticidade como fator de confiança não depende, exclusivamente, da estrutura pública formatada pelo Estado, o sistema torna-se multiportas, vale dizer, com maiores chances de ingresso de sujeitos antes excluídos pela falta de acesso aos mecanismos tradicionais de certificação digital no Brasil. Essa mudança na titularidade de quem confere autenticidade à documentação das relações negociais retira parcela do poder antes destinada a entes estatais que atuam como intermediários, transferindo-o às pessoas que participam de determinada transação ou que com ela contribuem na medida de sua prerrogativa de verificação da integridade da cadeia de dados.

A *blockchain* promove um ambiente em que há desnecessidade de intermediários para suprir hipossuficiências decorrentes de relações negociais. As plataformas de contratação automáticas, também chamadas *smart contracts*, permitem que usuários realizem trocas com menor custo e maior efetividade. Na programação de um contrato inteligente, um

ativo é transferido ao próprio programa, na medida em que o programa executa seu próprio código. Há a validação automática e o código determina a destinação do ativo, conforme confirmações admissíveis e programadas de cumprimento de obrigações contratuais (KATANO; HARO, 2018). A *blockchain* replica o documento, transmitindo a cada usuário da rede uma cópia autenticada, concedendo-lhe o atributo da imutabilidade, o que significa não poder ser alterado por apenas um dos interessados.

Um importante atributo dos *smart contracts* é esta imutabilidade sistêmica, que não se confunde com a possibilidade de revisão contratual, por acordo entre as partes ou pelos efeitos próprios da inafastabilidade da jurisdição. Nesse tocante, os contratos inteligentes proporcionam segurança às relações negociais, o que traz consequências positivas não só às partes contratantes, mas também à seara econômica, como diminuição do fator-risco e queda das taxas de juros remuneratórios (KATANO; HARO, 2018).

Logo, sem prejuízo de outros mecanismos de tutela da vulnerabilidade, a *blockchain* pode revelar-se potencializadora da proteção dos vulneráveis, na proporção em que dissipa a responsabilidade pela manutenção da informação e pela chancela da autenticidade da prova da relação jurídica negocial.

5 A CERTIFICAÇÃO DIGITAL NO BRASIL E AS ALTERNATIVAS DA *BLOCKCHAIN*

A sistemática de certificação digital pode ser formada em dois modelos, o hierárquico e o cruzado. O primeiro, hierarquicamente constituído, assemelha-se à disposição de uma árvore invertida, sendo que a posição mais alta é de uma entidade na qual todos devem, necessariamente, confiar, ainda que por força de determinação legal. No segundo modelo, a base é a confiança recíproca entre entidades, de modo a inexistir hierarquia (MENKE, 2005). A credibilidade legitimar-se-ia

por outros fatores sociais, que não a hierarquia ou o próprio Direito (NOGUEIRA; MAGALHÃES, 2009).

Como já se disse outrora (NOGUEIRA; MAGALHÃES, 2009), a hierarquia, usualmente, relaciona-se ao fato da existência de uma autoridade certificadora raiz, esta entendida como aquela detentora de tecnologia para operacionalização da criptografia assimétrica e manutenção de chave privada de extensão suficiente à promoção de um altíssimo nível de segurança, para que, além de certificar sua própria chave pública correspondente à sua chave privada mantida no mais extremo sigilo e segurança, possa certificar, ainda, as chaves públicas das autoridades certificadoras a ela submetidas que, por sua vez, emitirão certificados digitais aos usuários finais. Esses certificados são empregados em assinaturas digitais necessárias à preservação da autenticidade, integridade e não repúdio de declarações de vontade e de sua documentação eletrônica.

No modelo inverso, o cruzado, as autoridades certificadoras reconhecem-se umas às outras, criando uma cadeia de confiança, de modo que, caso alguma delas deixe de certificar a autenticidade de determinada chave pública, esta cai em descrença, deixando, assim, de ser aceita como válida (NOGUEIRA; MAGALHÃES, 2009).

O Estado preferiu tomar o controle das atividades de certificação digital no país, ao adotar, flagrantemente, um modelo internacionalmente conhecido como modelo hierárquico.

Houve, assim, a criação de uma Infra-Estrutura de Chaves Públicas, que se forma com o objetivo principal de dar suporte à atribuição de certificados digitais a um universo de usuários:

> O conjunto ou modelo formado de autoridades certificadoras, políticas de certificação e protocolos técnicos compõem o que se convencionou chamar de "Infra-estrutura de Chaves Públicas" ou simplesmente ICP.

> Uma infra-estrutura de chaves públicas não é apenas um feixe de leis, mas um conjunto de regimes normativos, procedimentos, padrões e formatos técnicos, que viabilizam o uso em escala da criptografia de chaves públicas em rede digital aberta (REINALDO FILHO, 2006, p. 60).

A origem remota da Infra-Estrutura de Chaves Públicas Brasileira pode ser posicionada no Decreto nº 3.587, de 5 de setembro de 2000, que instituiu a Infra-Estrutura de Chaves Públicas do Poder Executivo (MENKE, 2005). A Infra-Estrutura de Chaves Públicas Brasileira tem lastro na Medida Provisória nº 2.200-1, de 2001, reproduzida, em sua maior parte, na Medida Provisória nº 2.200-2 (BRASIL, 2001).

Logo, de acordo com a previsão do art. 5º da Medida Provisória em enfoque, à Autoridade Certificadora Raiz, primeira autoridade da cadeia de certificação, executora das Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil, compete emitir, expedir, distribuir, revogar e gerenciar os certificados das Autoridades Certificadoras de nível imediatamente subsequente ao seu, gerenciar a lista de certificados emitidos, revogados e vencidos, e executar atividades de fiscalização e auditoria das Autoridades Certificadoras, das Autoridades de Registro e dos prestadores de serviço habilitados na Infra-Estrutura de Chaves Públicas, em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor da ICP-Brasil, e exercer outras atribuições que lhe forem cometidas pela autoridade gestora de políticas (NOGUEIRA; MAGALHÃES, 2009).

A organização da Infra-Estrutura de Chaves Públicas Brasileira é composta dessa autoridade gestora de políticas e por uma cadeia de autoridades certificadoras composta pela Autoridade Certificadora Raiz

(AC-Raiz), pelas Autoridades Certificadoras de nível imediatamente inferior (AC) e pelas Autoridades de Registro (AR).

A Infra-Estrutura de Chaves Públicas Brasileira tem como autoridade certificadora raiz o Instituto Nacional de Tecnologia da Informação (ITI).

Compõem a estrutura nacional terceiros de confiança, que executam a tarefa de operacionalizar e gerenciar o ciclo de vida dos certificados (MENKE, 2005). Para a formação dessa estrutura descendente e centralizada, a Autoridade Certificadora Raiz conta com as demais Autoridades Certificadoras de segundo nível e com as Autoridades de Registro.

As Autoridades Certificadoras (AC) são entidades credenciadas a emitir certificados digitais vinculando pares de chaves criptográficas ao respectivo titular, às quais compete emitir, expedir, distribuir, revogar e gerenciar os certificados, bem como colocar à disposição dos usuários listas de certificados revogados e outras informações pertinentes e manter registro de suas operações. Ademais, devem dispor de um ambiente seguro para a realização de atividades basais de suas operações:

> Da mesma forma que a AC Raiz, as autoridades certificadoras devem dispor de ambiente seguro, onde realizarão as atividades críticas como as de emissão e de revogação de certificados. Esse ambiente seguro, que deverá ter no mínimo seis níveis compartimentados, não pode ser identificado externamente como tal, para evitar possíveis tentativas de acesso indevido. As instalações físicas deverão ter equipamentos de apoio, como máquinas de ar condicionado, geradores, *no-breaks,* baterias, estabilizadores, sistemas de aterramento e de proteção contra descargas atmosféricas, equipamentos para sistemas de emergência, entre outros, tudo para garantir a continuidade dos serviços (MENKE, 2005, p. 112).

As Autoridades de Registro (AR), por sua vez, são entidades operacionalmente vinculadas a determinada Autoridade Certificadora, às quais compete identificar e cadastrar usuários na presença destes, encaminhar solicitações de certificados às ACs e manter registros de suas operações (MENKE, 2005).

Significa que, no modelo hierárquico, a fonte de legitimação de todos os certificados emitidos é, em última análise, a autoridade certificadora raiz, que, no caso do Brasil, é a Autoridade Certificadora Raiz (AC-Raiz), que detém chaves criptográficas que chegam à extensão de 2048 bits, valor este que, como explica Fabiano Menke (2005), pode ser revisto na esteira do desenvolvimento do estado da técnica.

Desse modo, conforme explicitado nas linhas de estudo anterior (NOGUEIRA; MAGALHÃES, 2009), exatamente pelo interesse social no contrato eletrônico, ou, do mesmo modo, por motivo da busca de realização de um projeto jurídico para o desenvolvimento da sociedade, toda a estrutura exposta nada mais representa do que a consagração da base do princípio da função social dos contratos no que concerne ao contrato eletrônico. Na verdade, não é a função social que justifica esse modelo hierárquico explicitado acima, mas a base de justificação é a mesma, qual seja, a de existência de um projeto jurídico de interesse social, o que, por sua vez, justifica e legitima a atuação direta do Estado na consecução dos objetivos de viabilização e promoção da segurança das relações jurídicas contratuais havidas em meio eletrônico. Afinal:

> [...] o desenvolvimento econômico deve ocorrer vinculadamente ao desenvolvimento social. Um e outro são aspectos de um único desígnio, que, por sua vez, não se desliga dos deveres éticos reclamados princípio mais amplo da dignidade da pessoa humana, que jamais poderá ser sacrificado por qualquer iniciativa, seja em nome do econômico, seja em nome do social. Nada, com efeito, justifica o tratamento da pessoa humana como coisa ou

> como simples número de uma coletividade (THEODORO JÚNIOR, 2008, p. 33).

O aludido projeto de integração e inclusão social, contudo, é implementado antes pela interoperabilidade entre sistemas e equipamentos de tecnologia informática que pelo modelo hierárquico adotado.

> Verifica-se que a interoperabilidade é um apanágio necessário de qualquer infra-estrutura e pode ser definida como a capacidade que possuem os aparelhos e equipamentos que dela fazem parte de comunicarem-se entre si, independentemente de sua procedência, ou do seu fabricante (MENKE, 2005, p. 59).

Logo, em um cenário de interoperabilidade aprimorada, o modelo cruzado evidencia, exatamente, a admissão de múltiplos sujeitos na conformação da confiança *on-line*, o que pode fazer configurar proteção ampliada a posições vulneráveis e acessibilidade à participação sujeitos mais diversos.

Afinal, o modelo de cadeia construída por múltiplos participantes parece ostentar o seu potencial de inclusão de pessoas vulneráveis no contexto das relações jurídicas negociais em ambiente eletrônico, uma vez que a diversificação e plasticidade das estruturas voltadas a esse fim multiplica as portas de acesso e as possibilidades de participação.

6 CONCLUSÃO

Observa-se que o Estado tem assumido uma postura de protagonismo nas relações negociais, com a normatização de modelos hierárquicos de confiança, seja para o acontecimento, seja para a

autenticação e garantia de integridade da documentalidade de relações jurídicas negociais. Ocorre que esses arquétipos formatados de modo singular e fechado à participação e integração de múltiplos sujeitos podem agravar vulnerabilidades.

A tecnologia da *blockchain*, ao engendrar a pluralização dos responsáveis pela cadeia de confiança e a multiplicação das portas de acesso de pessoas alheias ao sistema tecnológico-jurídico de negócios *on-line*, apresenta-se como de grande potencial para contribuir para a tutela de vulnerabilidades e para a integração promocional de pessoas em situação de vulnerabilidade.

Por meio dos *smart contracts*, por exemplo, a tecnologia *blockchain* proporciona um ambiente seguro e transparente, público, compartilhado e universal, o que permite a realização de negócios entre sujeitos sem a necessidade de um intermediário centralizado. Ao resolver o problema da confiança – sem a necessidade de intermediários –, os *smart contracts* podem viabilizar a redução nos custos do negócio e o aumento da liberdade na condução de modelos contratuais alternativos.

Com base nesses alegóricos estruturais, a tecnologia em comento também oferece alternativas ao modelo hierárquico de certificação digital no Brasil. Logo, sem que seja necessário o afastamento do Poder Público, é factível a inclusão de novos agentes (novos sujeitos) na concreção da confiança, para o alargamento do espectro de segurança de dados e para a inclusão de pessoas no panorama de firmação e execução de relações jurídicas negociais.

REFERÊNCIAS

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. **Diário Oficial da União**, Brasília,11 jan. 2002. Disponível em:

http://www.planalto.gov.br/ccivil_03/LEIS/2002/L10406.htm. Acesso em: 29 fev. 2019.

_____. Medida Provisória nº 2.200-2/2001, de 24 agosto 2001. **Diário Oficial da União**, Brasília, 27 ago. 2001, p. 65. Disponível em: www.planalto.gov.br. Acesso em: 29 fev. 2019.

FIUZA, César Augusto de Castro; NOGUEIRA, Roberto Henrique Pôrto; SILVA, Leila Bitencourt Reis da. Vulnerabilidade como parâmetro interpretativo necessário à vedação do conhecimento, de ofício, da abusividade de cláusulas em contratos bancários de consumo. *In*: SÁ, Maria de Fátima Freire; NOGUEIRA, Roberto Henrique Pôrto; SCHETTINI, Beatriz (org.). **Novos direitos privados, v. 1**. .Belo Horizonte: Arraes, 2016., p. 157-169.

GATES, Mark. **Ultimate guide to understanding blockchain, bitcoin, cryptocurrencies, smart contracts and the future of money.** [*S.l.*]*:* Wise Fox Publishing, 2017.

GONÇALVES, Carlos Roberto. **Direito civil brasileiro,** v. 3. São Paulo: Saraiva, 2004.

KATANO, Arthur Yuji; HARO, Guilherme Prado Bohac de. Das consequências jurígeno-econômicas extraídas a partir da utilização dos smart contracts. *In*: **Anais do Congresso Nacional de Direito Empresarial da Toledo Prudente**, 2018. Disponível em: http://intertemas.toledoprudente.edu.br/index.php/CONGRESSO/article/view/6877/67646824. Acesso em: 29 fev. 2019.

MARQUES, Cláudia Lima; MIRAGEM, Bruno. **O novo direito privado e proteção dos vulneráveis**. São Paulo: Revista dos Tribunais, 2012.

MENKE, Fabiano. **Assinatura eletrônica**: aspectos jurídicos no direito brasileiro. São Paulo: Revista dos Tribunais, 2005.

NALIN, Paulo Roberto Ribeiro. **Do contrato**: conceito pós-moderno em busca de sua formulação na perspectiva civil-constitucional. Curitiba: Juruá, 2001.

NOGUEIRA, Roberto Henrique Pôrto; MAGALHÃES, Rodrigo Almeida. **Documento eletrônico**: teoria geral dos contratos e os títulos de crédito virtuais. Belo Horizonte: RHJ Editora, 2009.

NORMAN, Alan. **Mastering bitcoin for starters**: bitcoins and cryptocurrency technologies, mining, investing and trading. [*S.l.*: *s.n.*], 2017.

PISCINI, Eric; HYMAN, Gys; HENRY, Wendy. **Blockchain**: trust economy. [*S.l.*]: Deloitte University Press, 2017.

REINALDO FILHO, Demócrito. A ICP-Brasil e os poderes regulatórios do ITI do CG. **Revista Jurídica Consulex,** Brasília, v. 10, n. 218, p. 60-65, fev. 2006.

PEREIRA, Caio Mário Silva. **Instituições de direito civil, v. 3.** 11. ed. Rio de Janeiro: Forense, 2003.

TAKASHIMA, Ikuya. **Ethereum**: the ultimate guide to the world of Ethereum. [*S.l.: s.n.*], 2017.

THEODORO JÚNIOR, Humberto. **O contrato e sua função social.** 3. ed. Rio de Janeiro: Forense, 2008.

Correspondência | Correspondence:

Guilherme Mesquita Estêves
Rua Berilo, 36, Bairro Santa Tereza, CEP 35.450-000. Itabirito, MG, Brasil.
Fone: (31) 98887-6971.
Email: guilherme.mesquita.esteves@gmail.com

Recebido: 20/11/2018.
Aprovado: 2/8/2019.

Nota referencial:

Estêves, Guilherme Mesquita; Nogueira , Roberto Pôrto. Blockchain, vulnerabilidade nas relações jurídicas negociais e a alternativa ao modelo hierárquico de certificação digital. **Revista Direito e Liberdade,** Natal, v. 21, n. 3, p. 343-367, set./dez. 2019. Quadrimestral.