

**XXVII CONGRESSO NACIONAL DO
CONPEDI PORTO ALEGRE – RS**

**DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS
II**

JOSÉ RENATO GAZIERO CELLA

JÚLIA FRANCIELI NEVES DE OLIVEIRA

SALETE ORO BOFF

Todos os direitos reservados e protegidos. Nenhuma parte destes anais poderá ser reproduzida ou transmitida sejam quais forem os meios empregados sem prévia autorização dos editores.

Diretoria – CONPEDI

Presidente - Prof. Dr. Orides Mezzaroba - UFSC – Santa Catarina

Vice-presidente Centro-Oeste - Prof. Dr. José Querino Tavares Neto - UFG – Goiás

Vice-presidente Sudeste - Prof. Dr. César Augusto de Castro Fiuza - UFMG/PUCMG – Minas Gerais

Vice-presidente Nordeste - Prof. Dr. Lucas Gonçalves da Silva - UFS – Sergipe

Vice-presidente Norte - Prof. Dr. Jean Carlos Dias - Cesupa – Pará

Vice-presidente Sul - Prof. Dr. Leonel Severo Rocha - Unisinos – Rio Grande do Sul

Secretário Executivo - Profa. Dra. Samyra Haydêe Dal Farra Napolini - Unimar/Uninove – São Paulo

Representante Discente – FEPODI

Yuri Nathan da Costa Lannes - Mackenzie – São Paulo

Conselho Fiscal:

Prof. Dr. João Marcelo de Lima Assafim - UCAM – Rio de Janeiro

Prof. Dr. Aires José Rover - UFSC – Santa Catarina

Prof. Dr. Edinilson Donisete Machado - UNIVEM/UENP – São Paulo

Prof. Dr. Marcus Firmino Santiago da Silva - UDF – Distrito Federal (suplente)

Prof. Dr. Ilton Garcia da Costa - UENP – São Paulo (suplente)

Secretarias:

Relações Institucionais

Prof. Dr. Horácio Wanderlei Rodrigues - IMED – Santa Catarina

Prof. Dr. Valter Moura do Carmo - UNIMAR – Ceará

Prof. Dr. José Barroso Filho - UPIS/ENAJUM – Distrito Federal

Relações Internacionais para o Continente Americano

Prof. Dr. Fernando Antônio de Carvalho Dantas - UFG – Goiás

Prof. Dr. Heron José de Santana Gordilho - UFBA – Bahia

Prof. Dr. Paulo Roberto Barbosa Ramos - UFMA – Maranhão

Relações Internacionais para os demais Continentes

Profa. Dra. Viviane Coêlho de Séllos Knoerr - Unicuritiba – Paraná

Prof. Dr. Rubens Beçak - USP – São Paulo

Profa. Dra. Maria Aurea Baroni Cecato - Unipê/UFPB – Paraíba

Eventos:

Prof. Dr. Jerônimo Siqueira Tybusch (UFSC – Rio Grande do Sul)

Prof. Dr. José Filomeno de Moraes Filho (Unifor – Ceará)

Prof. Dr. Antônio Carlos Diniz Murta (Fumec – Minas Gerais)

Comunicação:

Prof. Dr. Matheus Felipe de Castro (UNOESC – Santa Catarina)

Prof. Dr. Liton Lanes Pilau Sobrinho (UPF/Univali – Rio Grande do Sul)

Dr. Caio Augusto Souza Lara (ESDHC – Minas Gerais)

Membro Nato – Presidência anterior Prof. Dr. Raymundo Juliano Feitosa - UNICAP – Pernambuco

E27

Direito, governança e novas tecnologias II [Recurso eletrônico on-line] organização CONPEDI/ UNISINOS

Coordenadores: José Renato Gaziero Cella; Salette Oro Boff; Júlia Francieli Neves de Oliveira. – Florianópolis: CONPEDI, 2018.

Inclui bibliografia

ISBN: 978-85-5505-726-7

Modo de acesso: www.conpedi.org.br em publicações

Tema: Tecnologia, Comunicação e Inovação no Direito

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Assistência. 3. Isonomia. XXVII Encontro Nacional do CONPEDI (27 : 2018 : Porto Alegre, Brasil).

CDU: 34



XXVII CONGRESSO NACIONAL DO CONPEDI PORTO ALEGRE – RS

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS II

Apresentação

No XXVII Congresso Nacional do CONPEDI, realizado de 14 a 16 de novembro de 2018, que teve lugar na Universidade do Vale do Rio dos Sinos - UNISINOS, em Porto Alegre-RS, o grupo de trabalho “Direito, Governança e Novas Tecnologias II” se destacou no evento não apenas pela qualidade dos trabalhos apresentados, mas pelo numeroso público, composto por pesquisadores-expositores e interessados, que deixou a sala repleta até o término das atividades. Foram apresentados 19 artigos objeto de um intenso debate presidido pelos coordenadores e acompanhado pela participação instigante do público presente.

Esse fato demonstra a inquietude que o tema desperta na seara jurídica. Cientes desse fato, os programas de pós-graduação em Direito empreendem um diálogo que suscita a interdisciplinaridade na pesquisa e se propõe a enfrentar os desafios que as novas tecnologias impõem ao Direito. Pode-se agrupar os trabalhos apresentados em quatro grandes temáticas, que se congregam nesta coletânea.

Houve enfoque nas possibilidades e contingências democráticas das novas tecnologias, tanto no âmbito teórico quanto no âmbito prático, com apresentações e debates dos seguintes artigos:

1. POLÍTICAS PÚBLICAS E NEUTRALIDADE DA REDE NO BRASIL;
2. OS DEPARTAMENTOS JURÍDICOS E AS EMPRESAS MULTINACIONAIS DE TECNOLOGIA DA INFORMAÇÃO (TI) QUE ATUAM EM PAÍSES EMERGENTES: A GERAÇÃO DE VANTAGENS COMPETITIVAS À LUZ DAS CAPACIDADES DINÂMICAS;
3. PROTEÇÃO DE DADOS PESSOAIS NA SOCIEDADE DA INFORMAÇÃO: UMA VISÃO SOB O ASPECTO DOS DIREITOS DA PERSONALIDADE NO BRASIL E NA UNIÃO EUROPEIA;
4. “CORPO ELETTRONICO” COMO VÍTIMA EM MATÉRIA DE TRATAMENTO DE DADOS PESSOAIS: RESPONSABILIDADE CIVIL POR DANOS À LUZ DA LEI DE PROTEÇÃO DE DADOS BRASILEIRA E DANO ESTÉTICO NO MUNDO DIGITAL;

5. O VOTO DISSIDENTE DE SOCIO MINORITARIO COMO FORMA DE GESTAO DO RISCO NANOTECNOLOGICO;
6. DEMOCRACIA E TECNOLOGIA: A ELABORAÇÃO DE NOVOS INSTRUMENTOS PARTICIPATIVOS NOS MUNICÍPIOS;
7. PARTICIPAÇÃO DA SOCIEDADE CIVIL NO CONTEXTO DA UNIÃO EUROPEIA: UM ESTUDO DE CASO DA FERRAMENTA EU-PILOT;
8. DIREITO E MEDICINA: UMA VISÃO INTERDISCIPLINAR FRENTE AOS APLICATIVOS PARA MARCAÇÃO DE CONSULTAS MÉDICAS E O POSICIONAMENTO DOS CONSELHOS PROFISSIONAIS;
9. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS: NATUREZA JURÍDICA E A LEI Nº 13.079/2018;
10. GESTÃO DOS ASPECTOS JURÍDICOS DA INOVAÇÃO DISRUPTIVA;
11. REFLEXÕES SOBRE A AUTOMAÇÃO NO DIREITO: LAW TECHS;
12. POLÍTICA REGULATÓRIA PARA TECNOLOGIAS DISRUPTIVAS NO BRASIL: O CASO DA TECNOLOGIA BLOCKCHAIN E TECNOLOGIAS DE REGISTRO DISTRIBUÍDAS;
13. O PRINCÍPIO DA PUBLICIDADE E DA FUNDAMENTAÇÃO DAS DECISÕES JUDICIAIS FRENTE A UTILIZAÇÃO DE ALGORITMOS NO DESEMPENHO DA ATIVIDADE JURISDICIONAL E DOS ATOS PROCESSUAIS;
14. ACCOUNTABILITY DE FAKE NEWS: BUSCANDO A VERDADE DA NOTÍCIA FALSA;
15. DIGITALIZAÇÃO NA ERA DA SOCIEDADE DA INFORMAÇÃO – VIRTUALIZAÇÃO E DESMATERIALIZAÇÃO. SATISFAÇÃO DO INTERESSE PÚBLICO – GOVERNO ELETRÔNICO;
16. O DIREITO HUMANO À INTIMIDADE NA CONTEMPORANEIDADE E SEUS DESAFIOS NA SOCIEDADE GLOBALIZADA EM REDE;

17. EFETIVIDADE DO DIREITO À INFORMAÇÃO: DIAGNÓSTICO DA POLÍTICA ESTADUAL DE DADOS ABERTOS GOVERNAMENTAIS NO RIO GRANDE DO SUL;

18. A INCORPORAÇÃO DE DRONES PARA VIGILÂNCIA DE ESPAÇOS URBANOS BRASILEIROS: O USO PELAS FORÇAS ARMADAS E ÓRGÃOS DE SEGURANÇA PÚBLICA DA UNIÃO E DO ESTADO DE SANTA CATARINA; e

19. AUTOCOMUNICAÇÃO E CONTRAPODER: A ARQUITETURA DAS TIC COMO INSTRUMENTOS DE DIFUSÃO INFORMATIVA E O IMPACTO NA AGENDA POLÍTICA

Os artigos que ora são apresentados ao público têm a finalidade de fomentar a pesquisa e fortalecer o diálogo interdisciplinar em torno do tema “direito, governança e novas tecnologias”, que trazem consigo, ainda, a expectativa de contribuir para os avanços do estudo desse tema no âmbito da pós-graduação em Direito brasileira, apresentando respostas para uma realidade que se mostra em constante transformação.

Os Coordenadores:

Prof. Dr. José Renato Gaziero Cella – IMED

Prof. Dr. Felipe Chiarello de Souza Pinto – UPM

Profª. Dra. Salete Oro Boff - IMED / IESA / UFFS

Nota Técnica: Os artigos que não constam nestes Anais foram selecionados para publicação na Plataforma Index Law Journals, conforme previsto no artigo 8.1 do edital do evento. Equipe Editorial Index Law Journal - publicacao@conpedi.org.br.

**POLÍTICA REGULATÓRIA PARA TECNOLOGIAS DISRUPTIVAS NO BRASIL:
O CASO DA TECNOLOGIA BLOCKCHAIN E TECNOLOGIAS DE REGISTRO
DISTRIBUÍDAS**

**REGULATORY POLICE FOR DISRUPTIVE TECHNOLOGIES IN BRAZIL: THE
CASE OF BLOCKCHAIN TECHNOLOGY AND DISTRIBUTED LEDGER
TECHNOLOGIES**

Rodrigo Cardoso Silva ¹

Resumo

É possível elaborar uma legislação para a tecnologia blockchain e as tecnologias de registro distribuídas sem obstar o processo evolutivo da inovação disruptiva no país? A partir desta repercussão, o presente artigo irá analisar a tecnologia disruptiva e a posição do governo brasileiro em face da proposta de regulação para estabelecer um quadro jurídico para o futuro do blockchain no país.

Palavras-chave: Regulação de blockchain, Regulação de tecnologias de registro distribuídas, Políticas regulatórias, Lei 12.965/2014 (marco civil da internet), Indústria 4.0

Abstract/Resumen/Résumé

Is it possible to draft legislation for Blockchain and Distributed Ledger Technologies to prevent the evolution of the process of disruptive innovation in the country? About this repercussion, the present article will analyze the disruptive technology and the position of the Brazilian government in face of the proposed legislation to establish a legal scenario for the future of the blockchain in the country.

Keywords/Palabras-claves/Mots-clés: Blockchain regulation, Distributed ledger technologies regulation, Regulatory police, Law 12,965/2014 (brazilian internet civil rights law), Industry 4.0

¹ Doutorando em Tecnologias da Inteligência e Design Digital pela PUC-SP com intercâmbio no Ragnar Nurkse Department of Innovation and Governance at Tallinn University of Technology. É diretor-executivo da Turing Security.

1 INTRODUÇÃO

Desde o surgimento da moeda digital Bitcoin no ano de 2008¹, a tecnologia *blockchain* renovou a forma de gerir determinados negócios com a possibilidade de diminuição dos custos operacionais de transação, irreversibilidade das informações por terceiros e a descentralização da tomada de decisão para um modelo de consenso entre as partes.

O sistema financeiro foi o primeiro campo de atuação específico impactado com a tecnologia no seu tipo de negócio por se tratar de uma moeda nova na economia mundial. Com o advento da moeda digital em escala quase global, o sistema monetário digital passou a operar de forma não regulada por lei, ocasionando um imbróglio jurídico para as transações financeiras no setor².

Apesar disso, o cenário internacional é bastante resistente com a normatização da moeda digital³ em razão de fatos ocorridos no passado, como a dificuldade do acesso à identificação dos usuários por causa da sua plataforma tecnológica, ações ilícitas com o uso da tecnologia e outros que demandaram na perda de ativos digitais⁴.

Todos estes cenários tismaram a imagem e colocaram a aplicação do Bitcoin em dubiedade na aldeia global. Outrossim, o banco central brasileiro é contrário a regulação de moedas digitais⁵.

Não obstante, importante se faz ressaltar que o foco desta investigação científica não é sobre a legalização de moedas digitais no Brasil, mas em relação a tecnologia que está por trás do Bitcoin – o *blockchain*, que proporcionou a inovação disruptiva na economia global.

Destarte, com o passar dos anos, em meados de 2015, surgiram visionários tecnológicos que propagaram que a utilização da plataforma *blockchain* também poderia ser utilizada para outros produtos ou serviços de âmbito público ou privado.

¹ Publicado por Satoshi Nakamoto de forma brilhante, simplista e eficaz o artigo intitulado “*Bitcoin: A Peer-to-Peer electronic cash system*”, onde foi demonstrado a possibilidade de um modelo novo de moeda nas relações econômicas para a sociedade da informação e do conhecimento digital (Nota do autor).

² No decorrer dos anos, o governo norte-americano reconheceu o *Bitcoin* como uma espécie *commodities* e a União Europeia como moeda fiduciária, mas ambos sem normatização (Nota do autor)

³ De outra parte, Christine Lagarde, diretora do Fundo Monetário Internacional (FMI), posicionou-se a favor da regulação das moedas digitais em 2018 (Nota do autor).

⁴ O primeiro episódio de poder da tecnologia *Bitcoin* ocorreu com o bloqueio da conta bancária do ativista político Julian Assange - fundador do *website WikiLeaks*, pelo governo norte-americano em decorrência do vazamento de documentos das guerras do Iraque e Afeganistão que imputaram ao governo estadunidense crimes de guerra. Para solucionar a custódia do dinheiro e inibir o seu rastreamento, ativistas simpatizantes da causa propuseram o uso do *Bitcoin* para manter o *website* ativo na internet, fato que existe até hoje. Já o segundo fato ocorreu entre 2011 e 2014, quando o *website Silk Road* (localizado nos Estados Unidos) transacionou a compra e venda de substâncias entorpecentes com *Bitcoins* pelo *browser* criptográfico TOR. Por último, o terceiro evento negativo aconteceu em 2014 com a empresa de câmbio em *Bitcoins*, Mt.Gox (lotada no Japão) que suspendeu as operações dos clientes sem a devolução das moedas digitais ou qualquer tipo de ressarcimento (Nota do autor).

⁵ Posição dos agentes públicos do banco central segundo as mídias digitais (Nota do autor).

De acordo com Swan (2015), hoje a tecnologia *blockchain* contempla a transferência de muitos outros tipos de ativos digitais que vão além da moeda digital, por isso, a tecnologia pode ser classificada em dois momentos no cenário mundial. O primeiro deles é o *blockchain* 1.0 que foi a descentralização do dinheiro e outras formas de pagamentos. Já o segundo, o *blockchain* 2.0, é a descentralização dos produtos ou serviços de maneira mais generalizada.

No mesmo sentido, Melanie Swan ponderou a respeito dessas inovações disruptivas do uso da tecnologia, exemplificando, assim, as possibilidades de aplicação *blockchain* na sociedade como um todo:

“a) no âmbito geral: transações judiciais, contratos aduaneiros, arbitragem de terceiros, operações de assinatura multipartidárias; b) transações financeiras: mercado financeiro, *crowdfunding*⁶, fundos mútuos, derivados, anuidades e pensões; c) registros públicos: propriedades móveis em geral, veículos, licenças de negócios, certidões de casamentos e atestados de óbito; d) identificação: carteira de motorista, carteira de identificação, passaportes e registros de eleitor; e) registros privados: cargas, contratos, apostas e assinaturas; f) atestados: seguros, prova de propriedade, documentos com firma reconhecida; g) chaves de ativos físicos: casas, quartos de hotel, aluguel de carros e acesso ao automóvel; h) intangíveis: patentes, marcas, direitos autorais e reservas (SWAN, 2015, pág. 43)”.

Diante destas reflexões, o cenário mundial se dirige para inovações disruptivas de diversos produtos ou serviços com a tecnologia *blockchain*. Contudo, a pesquisa entende que o processo sobre o assunto ainda está bastante incipiente, especialmente, no âmbito da regulação.

Por isso, é importante observar os acontecimentos na comunidade internacional para buscar um modelo normativo da plataforma *blockchain* e tecnologias de registro distribuídas para o país.

Em abril de 2018, vinte e três países da união europeia assinaram a Declaração sobre a criação de uma Parceria Europeia de *blockchain* para fomentar o desenvolvimento tecnológico

⁶ Financiamento coletivo para fins de negócio lucrativo ou não (Nota do autor).

e jurídico dos setores públicos e privados, como também, o intercâmbio de conhecimento e experiência sobre o tema⁷.

De outra parte, os países da América Latina não possuem qualquer discurso ou medida de cooperação para implementar uma pesquisa laboratorial, seja tecnológica ou jurídica, sobre *blockchain* e tecnologias de registro distribuídas.

Igualmente, o governo brasileiro além de não ter uma agenda consolidada a respeito do uso da tecnologia na administração pública⁸, propôs em junho deste ano a regulamentação da tecnologia *blockchain* durante a audiência pública promovida pela Comissão de Ciência e Tecnologia, Comunicação e Informática da Câmara dos Deputados.

É importante lembrar que, apesar de aproximadamente dez anos de existência da tecnologia, explicar tecnicamente sobre o *blockchain* e tecnologias de registro distribuídas não é tarefa fácil, ainda mais quando o tema é direcionado para a comunidade jurídica.

Isto porque há necessidade de se entender e ter conhecimentos sólidos na área da ciência computacional, pois em linhas gerais, o *blockchain* é um conjunto de linhas de código-fonte escrito em determinada linguagem de programação – algoritmo, para definição de instruções das regras sintáticas e semânticas de um computador.

Para o operador do direito sem conhecimento ou formação em processamento de dado digital, a percepção das funcionalidades da tecnologia disruptiva está apenas condicionada aos processos da aplicação de produtos e serviços.

Este é um ponto de reflexão importante, pois a regulação em questão está diretamente relacionada com a tecnologia e, conseqüentemente, com o ambiente digital que será aplicada. Do contrário, a tendência em abranger mais os processos na camada de aplicação – produtos e serviços, do que a tecnologia em si, poderá destoar a proposta deste trabalho.

Neste sentido, a pesquisa irá se aprofundar nas questões técnicas do *blockchain* e das tecnologias de registro distribuídas para esclarecer em que pontos a regulação poderá ser elaborada em consonância com as diretrizes e princípios que estejam correlacionados com o Marco Civil da internet - Lei 12.965/2014.

⁷ Segundo Mariya Gabriel (2018), Comissária para Economia Digital e Sociedade do Parlamento Europeu, o Blockchain é uma tecnologia para promover a confiança do usuário. Isto tornou possível o compartilhamento das informações *online*, o registro transparente das transações de forma segura e permanente. A tecnologia já está sendo testada com sucesso, principalmente em serviços financeiros, e se tornará mais operacional e integrada a um número crescente de serviços digitais, como relatórios normativos, energia e logística nos próximos anos (Nota do autor).

⁸ No ano de 2017, a secretaria de Tecnologia da Informação e Comunicação, órgão do Ministério do Planejamento, Desenvolvimento e Gestão teve a pretensão de criar um grupo de trabalho interministerial para estudar a renovação dos serviços públicos, no entanto, até o presente momento o projeto não foi iniciado (Nota do autor).

2 METODOLOGIA

O método adotado para esta pesquisa científica é o documental, o sistêmico e o qualitativo em vista da abordagem jurídica e tecnológica em torno do tema que, neste caso, é um fenômeno empírico no ecossistema da internet.

2 O QUE É A TECNOLOGIA BLOCKCHAIN?

Segundo Nakamoto (2008), o *blockchain* é a tecnologia da aplicação da moeda digital Bitcoin baseada em uma rede ponto-a-ponto ou “*peer-to-peer network*”⁹ e ferramentas criptográficas. A aplicação Bitcoin oferece um ambiente onde o conceito de confiança entre as partes não seja necessário para que a operação seja realizada¹⁰, isto é, o próprio sistema estabelece um mecanismo de governança para não ocorrer fraudes onde os usuários podem transferir dinheiro uns para os outros sem a necessidade de uma autoridade central, como por exemplo, o sistema bancário ou intermediários na operações de pagamento de serviços realizados por terceiros.

Da perspectiva de arquitetura de *software*, o *blockchain* possibilitou formas novas de *software* distribuído, onde o compartilhamento de dados das transações é distribuído em uma rede ampla de participantes “não-confiáveis”.

Isto contornou o problema existente da autoridade central nas relações de negócio, que detém o poder das decisões e é o único ator de confiança (compulsória) de todo o processo.

Logo, as aplicações construídas sobre a plataforma *blockchain* podem oferecer ferramentas como a imutabilidade e a integridade de dados e informações, a identificação sob o princípio do não-repúdio¹¹, participação igualitária e a transparência das transações.

Deste ponto, vale ressaltar que o seu modelo foi construído para se ter publicidade de todo o processo, assim, a forma original da plataforma é pública, e não privada.

⁹ É uma arquitetura de redes de computadores distribuída. Cada um dos pontos ou nós da rede funciona tanto como cliente quanto como servidor, permitindo o compartilhamento de serviços ou dados sem a necessidade de um servidor central (Nota do autor).

¹⁰ O termo na língua inglesa é *trust-less*, que literalmente significa indigno de confiança (Nota do autor).

¹¹ Na área da segurança digital, baseia-se na garantia de provar que determinada ação foi realizada por um agente, podendo-se, inclusive, apresentar prova desta ação (Nota do autor).

No entanto, é importante aduzir que o *blockchain* tem limitações técnicas¹². A privacidade é afetada porque o modelo é público¹³, com efeito, as informações estão disponíveis na cadeia de blocos para todos os participantes.

No quesito velocidade de transmissão dos dados ou escalabilidade da taxa de transferência, a sua forma convencional pode operar em média de três a vinte transações por segundo. Esta característica é bastante diferente se comparado com as operações bancárias que podem lidar em média com hum mil e setecentas transações por segundo¹⁴.

Diante deste exemplo, é importante observar que a tecnologia atua como um programa conector entre a rede internet e a respectiva aplicação, oferecendo, assim, a possibilidade para a construção de outros modelos derivados. Com efeito, a aplicação Bitcoin até os dias atuais ganhou diversificados tipos de moedas digitais¹⁵ com modificações específicas na plataforma *blockchain*¹⁶.

Em tese, o *blockchain* ainda não tem condições tecnológicas para atender diversos tipos de produtos ou serviços, por exemplo, aqueles que exigem processamento em tempo real.

Ao construir aplicativos baseados em *blockchain* há a necessidade de considerar sistematicamente arquitetura do *blockchain* e avaliar o seu impacto nos atributos de qualidade para qualquer tipo de sistema. Na prática, o cenário de modelos de negócios novos com *blockchain* ainda é bastante incipiente para a pesquisa enfatizar alguma comparação¹⁷.

¹² Satoshi Nakamoto (2008) afirmou no seu artigo que a sua proposta é tinha como objetivo iniciar melhorias para o sistema monetário com ferramentas digitais que promovessem o empoderamento dos cidadãos na relação monetária e a segurança do dinheiro contra corrupção e fraudes bancárias. Em tese, a tecnologia blockchain pode não atender com eficiência operacional a adoção em escalas maiores.

¹³ O blockchain público sem permissão ou “*permission-less public blockchain*” são completamente abertos, pois usuários novos podem a qualquer momento ingressar na rede, validar transações e bloquear um minerador – nó de rede. Além disso, a infraestrutura descentralizada é um dos fatores desta inovação disruptiva. Em alguns momentos, a terminologia na língua inglesa poderá causar estranheza no entendimento da taxionomia da tecnologia. (Nota do autor).

¹⁴ A privacidade de dados e a escalabilidade são dois pontos de críticos do blockchain público. A privacidade é bastante limitada, pois não há usuários privilegiados e cada participante pode entrar na rede para acessar todas as informações e validar transações novas no blockchain. Já a escalabilidade possui limites no: a) tamanho dos dados no blockchain; b) taxa de processamento da transação; c) latência na transmissão de dados (por exemplo, uma hora no Bitcoin e três minutos no Ethereum). O número de transações incluídas em cada bloco também é limitado pela largura de banda dos nós de rede (Nota do autor).

¹⁵ Existe um movimento de pioneirismo de *startups* e *fintechs* na criação de moedas digitais em determinados países. No Brasil, a criação de moedas digitais está sendo impedido pelo Banco Central sob o argumento da insegurança jurídica. De outra parte, o governo da República da Estônia tem um projeto para a criação de sua primeira moeda digital estoniana (Nota do autor).

¹⁶ As derivações mais conhecidas são o *Ethereum* e o *Hyperledger* (Nota do autor).

¹⁷ Quase que diariamente, grandes *players* do mercado estão patenteando ideias com o uso da plataforma em diversos segmentos, por exemplo, a IBM e Microsoft (Nota do autor).

2.1 COMO FUNCIONA O BLOCKCHAIN?

O *blockchain* público se refere a uma estrutura de dados e, ocasionalmente, a uma rede ou sistema. De acordo com a sua natureza arquitetônica de armazenamento de dados, a pesquisa entende que a tecnologia atua como um banco de dados, juntamente, com a camada de aplicação.

Como uma estrutura de dados, um *blockchain* é uma lista ordenada de blocos, onde cada bloco contém uma pequena lista de transações¹⁸. Cada bloco em uma *blockchain* é encadeado de volta ao bloco anterior, contendo um *hash*¹⁹ da representação deste bloco anterior. Assim, o histórico das transações no *blockchain* não podem ser excluídos ou alterados sem invalidar a cadeia de *hashes*²⁰.

A primeira geração de *blockchain*²¹ forneceu um tipo de livro-razão²² público para armazenar transações financeiras criptograficamente assinadas²³. Havia uma capacidade muito limitada para suportar transações programáveis, e apenas pequenas partes de dados auxiliares podiam ser incorporadas às transações para outros fins, como representar ativos digitais²⁴ ou físicos²⁵.

Já a segunda geração de *blockchain* forneceu uma infraestrutura programável de uso geral mediante um registro ou *ledger* público que armazena os resultados computacionais na forma de contratos inteligentes.

Um contrato inteligente é um pedaço de código executado em cima de uma rede *blockchain* em que os ativos digitais são controlados por esse código que implementa as regras de governança da plataforma. Importante se faz ressaltar que, o termo não está associado ao conceito de contrato de uma relação jurídica.

Como já foi mencionado anteriormente, a criptologia é parte essencial no *blockchain* para garantir a integridade de uma transação. A plataforma utiliza a criptografia de chave pública e assinaturas digitais que são normalmente usadas para identificar contas de usuários e garantir a autorização de transações iniciadas em um *blockchain*. Estas transações são pacotes

¹⁸ Possivelmente vazia para serem preenchidas com informações nos registros (Nota do autor).

¹⁹ Um *hash* é uma função que recebe um valor de entrada que criará um valor de saída determinístico referente a este valor (Nota do autor).

²⁰ Nakamoto (2008) eliminou o problema do gasto duplo no Bitcoin com este modelo criptográfico, isto é, a mesma moeda digital não poderia ser usada duas vezes, equiparando-se ao modelo de moeda fiduciária tradicional.

²¹ Bitcoin.

²² Que não diz respeito ao conceito de livro-razão da área contábil (Nota do autor).

²³ Por exemplo, 5dc5acc3083bd43e166282d16bd218ff9a57813a3b13a9dca767198f79f07b38. Esta identificação pode ser consultada no Blockchain Luxembourg S.A. (Nota do autor)

²⁴ Por exemplo, reconhecimento de documentos (Nota do autor).

²⁵ Por exemplo, diamantes (Nota do autor).

de dados que armazenam parâmetros, como o valor monetário do Bitcoin, e resultados das chamadas de uma função pelos contratos inteligentes.

Hipoteticamente, uma transação é assinada pelo seu proprietário para autorizar: a) uso do ativo digital; b) carga de dados de uma transação; c) criação ou execução de um contrato inteligente. Assim, a transação assinada é enviada para um nó conectado à rede *blockchain*²⁶, que validará a transação. Se a transação for válida e, anteriormente desconhecida para o nó, o nó a propagará para outros nós na rede, que também validaram a transação e a propagaram para seus pares, até que a transação atinja todos os nós na rede.

Aqui se faz necessário a observação é em relação à criptologia, assunto amplamente discutido entre 2015 e 2016 no âmbito jurídico. A criptografia é uma área computacional em constante evolução que pode com o passar dos anos sofrer determinadas mutações na sua estrutura algorítmica²⁷. Logo, a sua análise serve para dar embasamento a tecnologia *blockchain* e, conseqüentemente, a proposta deste trabalho científico.

Neste sentido, as palavras de Ralph Charles Merkle produzidas na sua tese em 1979 que, apesar de terem sido proferidas há 40 anos, tem em seu contexto a atualidade necessária para o emergente tema em discussão.

“A criptografia é um assunto fascinante, ainda mais hoje do que no passado. As ideias novas e impensáveis sobre a distribuição de chaves públicas e assinaturas digitais abriram campos de pesquisas novos, e possibilidades novas para o mercado. Ser um dos primeiros a se aventurar nesse território virgem tem sido um grande privilégio.” (MERKLE, 1979, pag. 01)”.

O trabalho de Merkle deu origem à técnica de estruturação de dados chamada de árvores de dispersão no campo da criptologia²⁸. Além dele, há outros renomados pesquisadores que foram pioneiros na construção de algoritmos de criptografia com chave pública²⁹.

Para entender melhor o conceito sobre criptologia, a investigação recorreu a Stallings (2015) para esclarecer a ciência da escrita secreta. Segundo ele, a criptografia é a ciência que

²⁶ Na computação, cada nó de rede é um usuário conectado com o seu computador (Nota do autor).

²⁷ É importante lembrar que a Internet é uma rede colaborativa onde os participantes concordam em seguir protocolos e padrões abertos pela Internet Engineering Task Force (IETF) (Nota do autor).

²⁸ É uma função importante da base algorítmica criptográfica, pois permite identificar qualquer tipo de alteração no dado (Nota do autor).

²⁹ São eles: Martin Hellman, Whitfield Diffie, Ronald L. Rivest, Bruce Schneier e A. Shamir e L.M. Adleman – estes quatro últimos criaram o protocolo RSA. (Nota do autor).

transforma a informação original de qualquer linguagem escrita para outra informação ilegível, tornando-a conhecida apenas pelo destinatário possuidor da chave secreta.

Mas como funciona na prática? Na parametrização de uma chave, as mensagens a serem criptografadas, ou seja, converter um texto normal em um texto cifrado é denominado de encriptação. De outra parte, a restauração do mesmo texto para leitura é chamada de decifração ou deciptação (TANEMBAUM, 2011).

A evolução da escrita secreta utilizada por muito tempo pela humanidade como forma de assegurar as informações constitui atualmente em diversos modelos de encriptação. Conforme aduz Stallings (2015), uma das formas de classificar sistemas criptográficos se refere ao número de chaves utilizadas no processo. Por exemplo, se tanto o emissor quanto o receptor utilizarem a mesma chave, o sistema é classificado como encriptação simétrica. Todavia, se emissor e receptor usarem chaves diferentes, o sistema é classificado como encriptação assimétrica ou de chave pública.

No caso do *blockchain*, é importante esclarecer mais uma vez sob o olhar da criptografia que o modelo utiliza a tecnologia ponta a ponta ou *peer-to-peer* com o uso de chave pública para construir uma arquitetura de redes de computadores de elevada disponibilidade em que cada um dos pontos ou nós da rede que funciona tanto como cliente quanto como servidor, permitindo, assim, o compartilhamento de serviços e dados sem a necessidade de um servidor central. Isto é, o servidor não é o responsável pela execução de todas as funções da rede, pois todos os nós estão interconectados possibilitando que o acesso a qualquer nó tenha origem em qualquer outro nó.

O estudioso no assunto Stallings dá ênfase ao exposto acima quando diz que:

“A força de qualquer sistema criptográfico está na técnica de distribuição de chave, um termo que se refere aos meios de entregar uma chave a duas partes que querem trocar dados e informações, sem permitir que outros vejam a chave. Isto ocorre porque para que a encriptação simétrica funcione corretamente, as duas partes precisam compartilhar a mesma chave, que deve ser protegida contra o acesso de outras partes sem permissão (STALLINGS, 2015, pág. 102)”.

Como se pode observar, a tecnologia *blockchain* e tecnologias de registro distribuídas fazem uso da criptologia, logo, o *blockchain* é um modelo de protocolo criptográfico para encadeamento da lista de blocos pelo processo denominado mineração³⁰.

O processo de mineração é o procedimento de anexar blocos novos à estrutura de dados do *blockchain*. É parte essencial de uma rede *blockchain* porque depende de mineradores para agregar transações válidas em blocos e anexá-los ao *blockchain*. Os blocos novos são transmitidos por toda a rede, de modo que cada nó conterà uma réplica de toda a estrutura de dados. É importante ressaltar que toda a rede tem como objetivo chegar a um consenso sobre o último bloco a ser incluído no *blockchain*, pois do contrário, a transação não será concluída.

Este mecanismo de consenso é a regra de governança da plataforma que garante a veracidade dos fatos na rede entre participantes “não-confiáveis”. Existem diferentes mecanismos de consenso, a prova de trabalho ou “*proof-of-work*” - popularmente conhecido como “*Nakamoto consensus*”, que é o protocolo de consenso de segurança do *blockchain*³¹.

A escolha do protocolo de consenso está diretamente relacionada com a segurança e a escalabilidade na plataforma, pois toda vez que um bloco novo é gerado por um minerador, ele propaga o bloco para seus pares conectados na rede *blockchain*. Ademais, os mineradores podem encontrar blocos novos diferentes para competir e resolver a equação criptográfica através do mecanismo do protocolo de consenso. Para este enigma matemático são necessários tempo e poder computacional para resolvê-lo³².

2.2 TIPOS DE BLOCKCHAIN

Sabendo que a inovação disruptiva do *blockchain* está na descentralização de poder dos ativos digitais, mas que determinados produtos ou serviços que almejam utilizar a tecnologia precisam realizar adaptações da tecnologia no seu modelo de negócio, a plataforma em tese sofreu alterações na sua arquitetura para atendê-las.

Com isso, mais quatro tipos de *blockchain* surgiram: centralizado, centralizado parcial, descentralizado parcial e verificador. Em linhas gerais, o centralizado realiza serviços com um

³⁰ A mineração é realizada pelos nós da rede que participam do processo de validação dos blocos (Nota do autor).

³¹ Para o consenso da segurança: *proof-of-retrievability*, *proof-of-stake* e *BFT (Byzantine Fault Tolerance)*; para o consenso da escalabilidade: *Bitcoin-NG*, *Off-chain transaction protocol* e *Mini-blockchain* (Nota do autor).

³² Por exemplo, os mineradores de Bitcoin competem para resolver esse “quebra-cabeça” para cada bloco usando grandes quantidades de energia de um computador para aumentar suas chances de vencer a competição. Ou seja, quanto mais computadores maiores serão as chances de alocar um bloco e receber o incentivo econômico da regra de governança, Bitcoins (Nota do autor).

único provedor de dados (governo) ou serviços com provedores alternativas (serviços bancários, pagamentos online ou serviços na nuvem); o centralizado parcial é um *blockchain* com permissões para operações refinadas no nível da transação (por exemplo, permissão para criar ativos digitais); o descentralizado parcial atua com mineradores quem têm permissão para apenas gravar dados, enquanto nós de rede comuns (não mineradores) podem apenas fazer a leitura das informações na cadeia de blocos; por último, o verificador que exerce uma função averiguadora que pode ser introduzida para avaliar condições que não podem ser expressas em um contrato inteligente executado na rede *blockchain*.

Segundo Pautasso (2017), um verificador é um terceiro confiável para fornecer alguns tipos de informações sobre o mundo externo. Quando a validação de uma transação depende do estado externo, o verificador é solicitado a verificar o estado externo e fornecer o resultado ao validador (minerador), que então valida a condição. Ademais, o verificador pode ser implementado como um servidor fora do *blockchain* e tem permissão para assinar transações usando seu próprio par de chaves sob demanda.

Para atender essas arquiteturas novas, o modelo de *blockchain público* também sofreu duas derivações, o *consortium/community blockchain*³³ e o *blockchain privado*³⁴. A pesquisa entende que a escolha de uma tecnologia digital para determinado trabalho deve responder alguns questionamentos, principalmente aqueles que dizem respeito a necessidade de adoção desta tecnologia.

Assim, é preciso antes verificar a necessidade real de descentralização do processo, caso contrário, usa-se um banco de dados tradicional. Se a opção for a descentralização, a configuração do banco de dados em *blockchain* precisa analisar os seguintes pontos: a) analisar a necessidade de um *blockchain* original ou novo; b) analisar a necessidade de múltiplos

³³ É um consórcio para múltiplas organizações. O tipo *consortium* possui as mesmas características do modelo privado em todos os aspectos, sendo que a única diferença entre ambos é a gestão centralizada da plataforma de forma partidária e multipartidária, respectivamente (Nota do autor).

³⁴ A plataforma tem como objetivo atender uma única organização. Apesar de empresas divulgarem projetos na mídia digital, não há indicadores do sucesso destes tipos de plataformas. Para a pesquisa, o cenário pode acarretar em um fenômeno idêntico na década de noventa com a adoção da intranet. Os setores privados e públicos apostaram em redes internas com o uso da internet sob a sua infraestrutura de rede (LAN ou WAN), em vez de utilizar diretamente os serviços via internet. Com o passar dos anos as redes de intranet se tornaram obsoletas em razão dos *softwares* como serviços ou *Software as a Service (SaaS)* realizados diretamente pela internet. Coincidentemente, o mesmo fenômeno está ocorrendo com o *blockchain*. As grandes empresas do setor de computação em nuvem, como a Amazon (AWS), Microsoft (Azure) e IBM (BlueMix), observaram o potencial em oferecer serviços de *blockchain* na nuvem (*cloud*) no formato *Blockchain as a Service (BaaS)* para seus clientes. Neles, os usuários se beneficiarão de não ter que configurar a plataforma *blockchain* e os investimentos em *hardware* também não serão mais necessários (A Microsoft fez uma parceria com a ConsenSys para oferecer a plataforma Ethereum como serviço Ethereum Blockchain as a Service (EBaaS) no Microsoft Azure. Já a IBM (BlueMix) fez parceria com a Hyperledger para oferecer BaaS aos seus clientes. Por fim, a Amazon anunciou que estaria oferecendo o serviço em colaboração com o Digital Currency Group (Nota do autor).

blockchain; c) analisar o tipo adotado d) analisar o tamanho do bloco e latência; e) analisar o protocolo de consenso que será adotado; f) analisar a estrutura dos dados que será adotado g) analisar o mecanismo de incentivo econômico mais adequado; h) mensurar a necessidade de anonimato; e i) qual é o modelo de negócio ele será aplicado?

Estas reflexões ajudam a projetar um sistema com o objetivo de utilizar a tecnologia *blockchain* como plataforma de segurança digital e banco de dados irreversível. A flexibilidade, em tese, desta tecnologia traz consigo desafios tecnológicos de customização dos processos digitais e regulatórios.

2.3 (IN)SEGURANÇA DIGITAL DO BLOCKCHAIN

É preceito fundamental da tecnologia *blockchain* de que quanto mais distribuída for a rede, mais segurança ela terá contra agentes maliciosos. Segundo Nakamoto (2008) o sistema é seguro desde que os nós de rede tenham controle coletivo, isto é, mais poder de processamento de dados de forma distribuída e conjunta, do que qualquer outro grupo participante de nós de rede na categoria de agente malicioso³⁵.

Em tese, para um agente malicioso tentar fraudar a rede *blockchain* ele teria que ter mais de 51% de todo o processamento de dados da rede para realizar as alterações sem que outros nós de rede conseguissem perceber a alteração indevida.

Embora os nós de rede possam verificar as transações por conta própria, o método simplificado pode ser enganado pelas transações fabricadas por um invasor enquanto o invasor puder continuar a dominar a rede.

Uma estratégia para proteger a rede *blockchain* seria aceitar alertas de nós de rede quando eles detectarem um bloco inválido, ou seja, solicitando que o *software* ou aplicação do usuário faça um *download* do bloco inteiro alertado para confirmar a inconsistência das transações.

3 BLOCKCHAIN E TECNOLOGIAS DE REGISTRO DISTRIBUÍDAS

Há uma discussão na comunidade científica e organismos de normas e padrões técnicos nacionais e internacionais a respeito da tecnologia *blockchain* e as tecnologias de registro distribuídas.

³⁵ Esta afirmação é interessante porque a quebra do protocolo de consenso pode ser realizado, em tese, com a possibilidade de um nó de rede (malicioso) ter mais de 50% do poder de mineração da rede *blockchain* que ele faz parte para tentar adulterar um registro sem a percepção dos demais nós de rede validadores. Na prática, o processo é dispendioso e quase que impossível de ser realizado (Nota do autor).

O ponto de divergência está na acepção de ambas as tecnologias, pois uma corrente entende que os conceitos são diferentes por serem tecnologias opostas dentro do ecossistema da rede ponto-a-ponto. Já o grupo contrário compreende que as duas tecnologias operam com sincretismo, possuindo, assim, a mesma definição.

No entanto, para a pesquisa os termos podem parecer sinônimos, mas as características de cada um são diferentes. Primeiro, as tecnologias de registro distribuídas ou *distributed ledger technologies (dlt)* são uma terminologia genérica da área contábil utilizada na operação de distribuição de registros e informações públicas ou privadas.

Segundo, o *blockchain* é um modelo de protocolo criptográfico onde a tecnologia de registro distribuído foi implementada na prática pela primeira vez, e que com o passar dos anos se tornou bastante popular. Isto criou um entendimento difuso e, provavelmente, generalizado.

Assim, pode-se afirmar que a tecnologia *blockchain* é um tipo ou subcategoria das tecnologias de registro distribuídas. Esta distinção é importante em razão das renovações que estão ocorrendo com ambas as tecnologias que, conseqüentemente, poderão impactar na sua legislação.

4 ASPECTOS JURÍDICOS DO BLOCKCHAIN

Para esta investigação científica, a legislação é um processo de aperfeiçoamento contínuo que atua como instrumento de força das bases democráticas para o bem-estar da sociedade contemporânea³⁶.

Na revolução digital do século XXI, o *blockchain* e as tecnologias de registros distribuídas são o tema mais desafiador e emergente de todas as inovações tecnológicas no cenário mundial desde o ano de 2011, especialmente, no campo regulatório.

São os casos de *startups* que tentam operar como organização autônoma descentralizada³⁷, mas que precisam de uma estrutura normativa que lhes permita conduzir os negócios além do universo da *blockchain*. Por exemplo, as moedas digitais.

A proteção de dados também é um assunto latente que está intimamente relacionado com a tecnologia disruptiva. Como já foi mencionado anteriormente, a tecnologia *blockchain* na sua forma mais pura é radicalmente transparente e anônima.

³⁶ A elaboração de leis não é um fim em si mesmo (Nota do autor).

³⁷ Uma organização autônoma descentralizada ou *decentralized autonomous organization* é uma organização cujas regras são especificadas através de programas de computador conhecidos como contratos inteligentes que são executados e validados por uma blockchain (Nota do autor).

Deste modo, as regulamentações sobre privacidade de dados pessoais, tornam a arquitetura *blockchain* difícil de implementar para corporações públicas ou privadas. Com base nisso, pode-se citar o problema do direito ao esquecimento, instituto jurídico criado na Europa que já foi adotado no direito brasileiro. A problemática aqui está na imutabilidade dos dados e informações dos registros na cadeia de blocos, pois a tecnologia eliminou a possibilidade de apagar os fatos do ecossistema da internet.

Diante disto, a proposta deste trabalho científico é buscar diretrizes, princípios, garantias e deveres para uma regulação sobre a tecnologia *blockchain* e tecnologias de registros distribuídas.

Neste sentido, a pesquisa faz remeter a três questionamentos: a) Como regular a tecnologia *blockchain* e as tecnologias de registros distribuídas sem prejudicar a sua inovação tecnológica? b) Torna-se mais eficaz criar uma lei ordinária especial própria para o *blockchain* e as tecnologias de registro distribuídas ou a opção de discipliná-la no Marco Civil da Internet como um de seus princípios? c) Deve-se regular somente os produtos ou serviços que venham a utilizar o *blockchain* e as tecnologias de registro distribuídas?

Estes quesitos são importantes porque refletem a direção que o legislador deverá tomar para não criar uma norma em desconformidade com a realidade que a tecnologia disruptiva está se desenvolvendo no Brasil.

Para o legislador é importante ter em mente os aspectos tecnológicos que envolvem os conceitos técnicos das tecnologias em questão, pois serão eles que irão definir a efetividade da lei para determinados casos.

A pesquisa recomenda em primeiro lugar que estes conceitos sejam oriundos de organizações de padrões técnicos³⁸, em razão da autenticidade e credibilidade na construção das normas técnicas, dirimindo, assim, qualquer tipo de dúvida com relação a aceção conceitual de ambas as tecnologias na regulação³⁹.

O desafio maior do legislador brasileiro será elaborar uma norma sem que possa obstar os avanços tecnológicos que a própria tecnologia é capaz de promover diante de adversidades ou necessidades contemporâneas na promoção do desenvolvimento humano, econômico, social, cultural e, principalmente, inovador.

³⁸ ABNT – Associação Brasileira de Normas Técnicas e ISO – *International Organization for Standardization* (Nota do autor).

³⁹ É importante ressaltar que o ecossistema do *blockchain* e tecnologias de registro distribuídas possuem no mínimo aspectos relacionados à governança, interoperabilidade, terminologia, segurança, privacidade e identidade (Nota do autor).

O poder legislativo deve rever as formas como as leis brasileiras são construídas, optando-se pela objetividade e praticidade na formulação dos artigos de lei, em razão da interdisciplinaridade que própria norma irá se submeter para conduzir a sociedade.

No mesmo sentido, o corpo legislativo do país deverá ter consciência de que a estrutura da lei terá que ser clara na composição da arquitetura tecnológica do *blockchain* e tecnologias de registro distribuídas. Isto inclui a criptologia, banco de dados, sistema de arquivos, aplicações (sistemas), linguagens de programação, sistemas de redes e o *hardware*⁴⁰.

Além disso, as disposições preliminares poderão incorporar normas do plano doméstico e internacional. Destarte, a pesquisa entende que os seguintes institutos podem fazer parte da fundamentação inicial da regulação: transparência, descentralização, imutabilidade, não-repúdio, integridade e isonomia.

No campo dos princípios poderão ser disciplinados a privacidade, proteção de dados pessoais, segurança digital, participação consensual, responsabilização dos nós de rede e o mecanismo de incentivo econômico.

Com relação aos objetivos a referida norma poderá também disciplinar sobre os direitos e garantias dos usuários, como por exemplo, o acesso amplo e irrestrito a rede *blockchain* e tecnologias de registro distribuídas, o incentivo a inovação disruptiva e continuísmo do desenvolvimento de padrões abertos para a sociedade digital em *blockchain*.

A atuação do poder público é bastante importante nesse cenário inovador para estabelecer diretrizes, porém, sem um status concentrador. Provavelmente, esta parte da lei será um desafio porque o poder público, neste caso, não é tecnicamente identificável na rede *blockchain* como um agente público, ele é apenas um nó de rede. Então, como se deve proceder em situações dessa magnitude e que tipo de sanção o poder público poderá sofrer? Para este trabalho acadêmico, além da promoção à inovação continuada em *blockchain* e tecnologias de registro distribuídas na internet pelo poder estatal, ele deve assumir os dois papéis, de regulador neutro e um nó de rede com base na isonomia.

Por último, os aspectos sancionatórios são extremamente necessários para evitar incidentes ou danos as partes envolvidas. Com isso, a sanção não precisa estar vinculada apenas as questões monetárias, mas poderá estar consubstanciada nas regras de governança da própria

⁴⁰ O *Application Specific Integrated Circuits (ASICs)* ou Circuitos Integrados de Aplicação Específica é o melhor exemplo, pois são circuitos orientados para implementação de tarefas específicas em domínios bem definidos, por exemplo, a mineração de Bitcoins (Nota do autor).

tecnologia, por exemplo, a suspensão ou exclusão de agente malicioso em determinado bloco da rede.

Com base nos quesitos *b* e *c* citados acima, a pesquisa compreende que existem essas duas possibilidades, a criação de lei especial com os requisitos mencionados acima e a inclusão das tecnologias na Lei 12.965/2014, Marco Civil da Internet.

Existe também a hipótese do Marco Civil da Internet referenciar as tecnologias com destaque para sua especialidade disciplinada em lei⁴¹. Para a pesquisa, ambas tecnologias já possuem proteção jurídica parcial, devido a disciplina do artigo 4º, incisos III e IV, do Marco Civil da Internet.

Já com relação a normatização dos produtos ou serviços com *blockchain* e tecnologias de registro distribuídas, poderá ocorrer um falso positivo na regulamentação. Primeiramente, a criação das normas será realizada por agentes da administração direta e indireta – órgãos concentradores de poder, podendo causar certo descontrole com o uso das tecnologias. Segundo, a opção apresentada inviabilizaria e não justificaria a criação de lei especial.

Por fim, o presente trabalho expôs apenas alguns pontos em que a regulação da tecnologia *blockchain* e tecnologias de registro distribuídas poderão contemplar em projeto de lei no futuro.

5 CONSIDERAÇÕES FINAIS

O *blockchain* é uma tecnologia emergente para compartilhamento de dados transacionais e descentralizados em uma grande rede de participantes onde não precisa haver a confiança mútua.

As tecnologias permitem formas novas de arquiteturas de *software* distribuídas sem um poder concentrado, operando como um conector de *software* em uma estrutura interna que possui várias configurações⁴² e diferentes variantes.

Usar o *blockchain* e as tecnologias de registro distribuídas em diferentes cenários requer um estudo detalhado da finalidade que se pretende implementá-lo, pois existe a possibilidade de que a necessidade não seja uma tecnologia como o *blockchain*, mas um banco de dados ou sistemas convencionais.

Nesta pesquisa, pode-se analisar os aspectos tecnológicos do *blockchain* frente as suas derivações e implicações em escala quase global. Contudo, a tecnologia ainda está passando

⁴¹ Isto faz com que ambas tecnologias possam ser parte dos fundamentos ou princípios da respectiva lei (Nota do autor).

⁴² Pode-se observar três camadas: internet, *blockchain* e aplicação (Nota do autor).

por um processo incipiente, especialmente, para a sua utilização em determinados produtos ou serviços não relacionados com moedas digitais fiduciárias.

Em todo caso, a projeção do *blockchain* e das tecnologias de registro distribuídas no mercado ainda é alvo de *buzz word*⁴³, com a exposição na mídia de acordos empresariais estratégicos para pesquisa e desenvolvimentos em determinados ramos de negócio, mas sem indicadores que comprovem a sua aplicabilidade.

Diante disto, a pesquisa entende que a adoção de uma regulação para a tecnologia *blockchain* e as tecnologias de registro distribuídas é prematura, podendo ocasionar um colapso sem precedentes.

De outra parte, começar a esboçar um projeto de lei será um ato bastante salutar para ordenamento jurídico pátrio, ainda mais se vier acompanhado de consultas públicas. O acompanhamento de padrões técnicos das organizações nacionais e internacionais são importantes para se obter o máximo de conformidade conceitual das arquiteturas de sistemas em *blockchain* e tecnologias de registro distribuídos.

Com isso, pode-se ter pleno conhecimento dos possíveis efeitos das disposições legislativas no tema, de modo a maximizar o seu impacto positivo e evitar encargos desnecessários e burocracia inútil para os cidadãos, as empresas e as autoridades públicas.

A busca por uma regulação melhor não cabe exclusivamente ao Congresso Nacional. Trata-se de um esforço desenvolvido conjuntamente com os cidadãos e os Estados-Membros brasileiros, cada um destes assumindo o seu próprio papel e responsabilidades, um esforço que não se limita apenas à fase de preparação e concepção da legislação nova.

O compromisso de legislar mais eficaz deve acompanhar cada fase do ciclo de elaboração, desde as negociações legislativas nas duas casas legislativas até à transposição e aplicação pelos Estados-Membros e sociedade. Para alcançar esse objetivo, deve-se centrar todos os esforços em eficiência, transparência, simplificação e celeridade ao nível adequado.

Por fim, é importante salientar para os legisladores brasileiros que o *blockchain* e as tecnologias de registro distribuídos são tecnologias emergentes, e que irão continuar a se desenvolver de acordo com a necessidade de cada um.

REFERÊNCIAS

ALI M. et al. Blockstack: A global naming and storage system secured by blockchains. In USENIX ATC, Santa Clara, CA, 2016.

⁴³ É uma expressão na língua inglesa que denota ‘zumbido’ ou ‘barulho’ (Nota do autor).

BACK A., G. Maxwell, M. Corallo, M. Friedenbach, and L. Dashjr. Enabling blockchain innovations with pegged sidechains. 2014.

BRASIL. LEI 12.965/2014. Marco Civil da Internet. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 03 ago. 2018.

BRASIL. Câmara dos Deputados. Disponível em: <http://www2.camara.leg.br/camaranoticias/noticias/CIENCIA-E-TECNOLOGIA/559279-ESPECIALISTAS-DEFENDEM-REGULAMENTACAO-DA-TECNOLOGIA-BLOCKCHAIN-PARA-CERTIFICAR-TRANSACOES-VIRTUAIS.html>. Acessado em: 10 de junho. 2018.

BROWN R. G. The “Unbundling of trust”: How to identify good cryptocurrency opportunities?, 2014.

UNIÃO EUROPEIA. Comissão Europeia. Disponível em: <https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership>. Acessado em: 05 junho. 2018.

CRESWELL, John W. *Projeto de pesquisa: métodos qualitativo, quantitativo e misto*. Tradução: Magda Lopes. 3a ed. Porto Alegre: Artmed, 2010.

DECKER C.; WATTENHOFER R. Information propagation in the Bitcoin network. In P2P, Trento, Italy, 2013.

DISTRIBUTED LEDGER TECHNOLOGY: beyond blockchain. Technical report, 2016. UK Government Chief Scientific Adviser.

EYAL I. and et. al. Bitcoin-NG: A scalable blockchain protocol. In USENIX NSDI, Santa Clara, CA, 2016.

_____. Majority is not enough: Bitcoin mining is vulnerable. In FC, Christ Church, Barbados, 2014.

GIL, Antonio Carlos. *Como elaborar projetos de pesquisa*. 5a ed. São Paulo: Atlas, 2010.

GERVAIS A., G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Čapkun. On the security and performance of proof of work blockchains. In ACM CCS 2016), Vienna, Austria, 2016.

GORTON I., et al. Architecture knowledge for evaluating scalable databases. In WICSA, Montréal, Canada, 2015. [12] T. D. Joseph Poon. The Bitcoin lightning network: Scalable off-chain instant payments. 2016.

I. WEBER, et al. Untrusted business process monitoring and execution using blockchain. In BPM, Rio de Janeiro, Brazil, Sept. 2016.

MILLER A., A. Juels, E. Shi, B. Parno, and J. Katz. Permacoin: Repurposing Bitcoin work for data preservation. In IEEE S&P, San Jose, CA, 2014. [16] S. Nakamoto. Bitcoin: A Peer-to-Peer electronic cash system, 2008. [17] C. Natoli and V. Gramoli. The blockchain anomaly. In NCA'16. IEEE, Oct 2016.

M. Swan. Blockchain: Blueprint for a New Economy. O'Reilly, US, 2015.

M. VUKOLIĆ. The quest for scalable blockchain Fabric: Proof-of-Work vs. BFT replication. In iNetSec, Zurich, Switzerland, 2015.

MEHTA N. R., et al. Towards a taxonomy of software connectors. In ICSE, 2000.

MERKLE, Ralph Charles. Secrecy, Authentication, and Public Key Systems. Thesis from Stanford University – Department of Electrical Engineering, 1979. Disponível em: <http://www.merkle.com/papers/Thesis1979.pdf>. Acesso em: 26/06/2018.

OMOHUNDRO S. Cryptocurrencies, smart contracts, and artificial intelligence. AI Matters, 1(2):19–21, Dec. 2014.

WUILLE, P. Segregated witness and deploying it for Bitcoin, 12, 2015.

PAUTASSO, C. A Taxonomy of Blockchain-Based Systems for Architecture Design. IEEE, 2017.

PAUTASSO, X. Xu, C. et al. The blockchain as a software connector. In TSCHORSCH F., et al. Bitcoin and beyond: A technical survey on decentralized digital currencies. IEEE Communications Surveys & Tutorials, 18(3):464, 2016.

WOOD G. Ethereum: A secure decentralized generalised transaction ledger — homestead draft. Technical report, 2016.

ROWAN B., et al. Blindcoin: Blinded, accountable mixes for Bitcoin. In FC, San Juan, Puerto Rico, 2015.

SWANSON T. Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems. 2015.

SOUZA, Carlos Affonso Pereira de. Advogado. O progresso tecnológico e a tutela jurídica da privacidade. Direito, Estado e Sociedade, v. 9, n. 16, p. 6-39, jan./jul. 2000.

STALLINGS, W. Criptografia e Segurança de Redes: Princípios e Práticas – 6a edição. São Paulo: Pearson. 2015. ISBN 978-8543005898.

TANENBAUM, A. S.; WETHERALL, D. Redes de Computadores - 5a Edição. São Paulo: Pearson. 2011. ISBN 857605924X.

WEF REPORT. The future of financial infrastructure - an ambitious look at how blockchain can reshape financial services. Technical report, 2016.

BUTERIN, V. On public and private blockchains, 2015/08.

ZOHAR A. Accelerating Bitcoin's transaction processing - fast money grows on trees, not chains. Cryptology ePrint Archive, Report 2013/881, 2013.

_____. Inclusive block chain protocols. In FC, San Juan, Puerto Rico, 2015..