PONTIFÍCIA UNIVERSIDADE CATÓLICA DO PARANÁ

PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO

JOSÉLIO JORGE TEIDER

A REGULAMENTAÇÃO NO BRASIL DOS CONTRATOS INTELIGENTES IMPLEMENTADOS PELA TECNOLOGIA BLOCKCHAIN

CURITIBA

2019

JOSÉLIO JORGE TEIDER

A REGULAMENTAÇÃO NO BRASIL DOS CONTRATOS INTELIGENTES IMPLEMENTADOS PELA TECNOLOGIA BLOCKCHAIN

Dissertação apresentada ao Programa de Pós-Graduação em Direito da Pontifícia Universidade Católica do Paraná como requisito parcial à obtenção do título de Mestre em Direito.

Prof.ª Orientadora: Dr.ª Cinthia Obladen de Almendra Freitas

CURITIBA

2019

Dados da Catalogação na Publicação
Pontifícia Universidade Católica do Paraná
Sistema Integrado de Bibliotecas – SIBI/PUCPR
Biblioteca Central
Luci Eduarda Wielganczuk – CRB 9/1118

T262r
2019

Teider, Josélio Jorge
A regulamentação no Brasil dos contratos inteligentes implementados pela tecnologia Blockchain / Josélio Jorge Teider ; orientadora: Cinthia Obladen de Almendra Freitas. – 2019.
140 f. : il. ; 30 cm

Dissertação (mestrado) – Pontifícia Universidade Católica do Paraná, Curitiba, 2019
Bibliografia: 130-140

1. Contratos – Processamento de dados. 2. Tecnologia da informação. 3. Inovações tecnológicas. I. Freitas, Cinthia Obladen de Almendra. II. Pontifícia Universidade Católica do Paraná. Programa de Pós-Graduação em Direito. III. Título.

Dóris 4. ed. – 342.14429

JOSÉLIO JORGE TEIDER

A REGULAMENTAÇÃO NO BRASIL DOS CONTRATOS INTELIGENTES IMPLEMENTADOS PELA TECNOLOGIA BLOCKCHAIN

Dissertação apresentada ao Programa de Pós-Graduação em Direito da Pontifícia Universidade Católica do Paraná como requisito parcial à obtenção do título de Mestre em Direito.

Prof.ª Orientadora: Dr.ª Cinthia Obladen de Almendra Freitas

COMISSÃO EXAMINADORA

Prof.ª Dr.ª Cinthia Obladen de Almendra Freitas – Orientadora – PPGD/PUC-PR

Prof. Dr. Vinícius Borges Fortes – Convidado – IMED – Passo Fundo

---

Prof.ª Dra. Danielle Anne Pamplona – Membro – PPGD/PUC-PR

Curitiba, ____ de _____ de 2019.

AGRADECIMENTOS

Agradeço a Deus pelas bênção recebidas incessamentemente em minha vida. A primeira destas bênçãos foi a minha amabilíssima, sábia e abençoada mãe, Albina Teider, de saudosa memória, que sempre me proporcionou todo conforto material e espiritual, dedicou-se se forma exemplar e impecável em todos os aspectos de minha vida. Realizou tantos sacrifícios para que nada me faltasse, estando sempre presente de forma plenamente amorosa. Tenho saudades imensas e espero, do fundo do meu coração, estar honrando sua memória em cada momento de minha vida. Se hoje faço algo de bom nesse mundo, a fonte disso certamente tem origem no exemplo de minha mãe.

Agradeço também minha família. Meu filho, Lucas Teider que me inspira e motiva a cada passo. Foi do Lucas a ideia de eu fazer Mestrado e foi ele quem me apresentou a minha orientadora, Prof. Cinthia. Agradeço ao Lucas por todo companheirismo e toda a amizade, todo o carinho e todo o apoio! Também agradeço a Sofia que chegou a este mundo ao mesmo tempo que eu iniciava os estudos do Mestrado. Ela trouxe inspiração, motivação e mais uma razão para dedicação em busca de meus ideais. Agradeço à Patricia, minha esposa, que suportou o sacrifício das longas jornadas de estudo que me impediam de estar mais presente no cotidiano de nossa família.

Agradeço aos meus amigos, todos eles, desde aqueles da remota infância até os que estão próximos nos presentes dias. Seria impossível nominar estes amigos sem cometer a injustiça de algum esquecimento. Mas saibam todos, sem exceção, que eu tenho uma imensa gratidão por toda sua companhia e apoio. E dentro deste universo de amizades tão preciosas, agradeço também aos amigos que fiz aqui no PPGD da PUC-PR: colegas, professores, funcionários, colaboradores. Todos fazem parte desta história! Aprendi muito com vocês e me sinto muito feliz por tê-los conhecido e ter convivido com vocês. Espero que nossa amizade se perpetue e que possamos compartilhar mais momentos juntos!

Agradeço a PUC-PR por sua excelência em tudo o que se propõe a realizar em cada aspecto da educação. Agradeço aos Irmão Maristas que dedicam suas vidas para cumprir tão fielmente a missão que Deus lhes confiou. Todo o apoio que recebi nesta casa sempre será lembrado com muita gratidão e muito carinho.

E um agradecimento especial quero dedicar à Professora Cinthia Obladen de Almendra Freitas, minha orientadora. Possuidora de um currículo espetacular, um conhecimento impressionante e de uma simplicidade encantadora. Sempre paciente e elegante em atender com dedicação e carinho a todos. Seu trabalho na minha orientação foi impecável em todos os aspectos. Muito mais do que conhecimento, levo deste Mestrado, o exemplo de vida e paixão pela educação que emana da Professora Cinthia, a qual será sempre fonte de inspiração para mim por toda a vida.

RESUMO

Os exponenciais avanços das Tecnologias da Informação e Comunicação (TICs) promovem mudanças que impactam a sociedade de forma intensa, ubíqua e pervasiva. Torna-se impensável conceber a sociedade contemporânea realizando suas tarefas, das mais simples às mais complexas, sem os benefícios propiciados pelas TICs. Dentro do conjunto das inovações tecnológicas disruptivas destaca-se a tecnologia *Blockchain* que promete revolucionar as formas pelas quais as pessoas interagem entre si, estabelecendo relações de confiança por meio de sofisticados algoritmos criptográficos distribuídos em redes ponto-a-ponto descentralizadas, ao mesmo tempo que dispensa a necessidade de intermediários e promove a resiliência e a inviolabilidade dos dados, informações e transações. O objetivo geral do estudo foi verificar como o ordenamento brasileiro pode oferecer tutela em face aos impactos da tecnologia *Blockchain*, em particular na implementação de Contratos Inteligentes. O trabalho dissertativo foi desenvolvido a partir de técnicas de pesquisa bibliográfica e documental, pelo método de pesquisa dedutivo. Em que pese existirem muitos obstáculos a serem superados para que os Contratos Inteligentes se tornem uma realidade exequível na prática, é inexorável que seus benefícios os tornam uma tecnologia com potencial extraordinário para implementar relações contratuais mais eficientes e confiáveis. Conclui-se que os Contratos Inteligentes não são uma nova categoria contratual, tratando-se de nova forma de contratação e que o ordenamento jurídico brasileiro tem instrumentos para recepcioná-los. Porém, suas características de descentralização, imutabilidade e autoexecução suscitam desafios para a interpretação jurisdicional, gerando necessidade de capacitação dos operadores do Direito em conhecimentos tecnológicos e trabalhos em conjunto com peritos em tecnologia a fim de promover a implementação eficiente de fundamentos legais para uma boa implementação de Contratos Inteligentes.

Palavras-chave: novas tecnologias, inovação, sociedades, regulamentação, blockchain, contratos inteligentes

ABSTRACT

The exponential advances of Information and Communication Technologies (ICTs) promote changes that impact society in an intense, ubiquitous and pervasive way. It is unthinkable to conceive contemporary society performing its tasks, from the simplest to the most complex, without the benefits provided by the ICTs. Within the set of disruptive technological innovations, Blockchain technology stands out, which promises to revolutionize the ways in which people interact with each other, establishing trust relationships through sophisticated cryptographic algorithms distributed in decentralized point-to-point networks, at the same time as it dispenses the need for intermediaries and promotes the resilience and inviolability of data, information and transactions. The general objective of the study was to verify how the Brazilian legal system can offer tutelage in face of the impacts of the Blockchain technology, particularly in the implementation of Smart Contracts. The dissertation was developed based on bibliographic and documentary research techniques, using the deductive research method. While there are many hurdles to overcome in order for Smart Contracts to become a reality in practice, it is inexorable that their benefits make them a technology with extraordinary potential to implement more efficient and reliable contractual relationships. It is concluded that the Smart Contracts are not a new contractual category, being a new form of contracting and that the Brazilian legal system has instruments to receive them. However, its characteristics of decentralization, immutability and self-execution pose challenges for jurisdictional interpretation, generating a need for the training of law professionals in technological knowledge and working together with experts in technology in order to promote the efficient implementation of legal grounds for a good implementation of Smart Contracts.

Keywords: new technologies, innovation, societies, regulation, blockchain, smart contracts

LISTA DE FIGURAS

Figura 1 - Como funciona uma transação na *Blockchain*..... 22
Figura 2 - Criação de blocos em uma *Blockchain*..... 25
Figura 3 - Como funciona um Contrato Inteligente 50

LISTA ABREVIATURAS E SIGLAS

AML –	Anti Money Laundry
ASIC –	Application-Specific Integrated Circuit
B2B –	Business to Business
B2C –	Business to Consumer
BNDES –	Banco Nacional de Desenvolvimento Econômico e Social
BCH –	Bitcoin Cash
Baas –	Blockchain-as-a-Service
BTC –	Bitcoin
C2C –	Consumer to Consumer
DAO –	Decentralized Autonomous Organization
EDI –	Intercâmbio Eletrônico de Dados
ETC –	Ethereum Classic
ETH –	Ethereum
EVM –	Ethereum Virtual Machine
FSF –	Free Software Foundation
GDPR –	General Data Protection Regulation
GPL –	General Public License (Licença Pública Geral)
ICO –	Initial Coin Offering (Oferta Pública de Moedas)
ID –	Código de Identificação
ICP-Brasil –	Infraestrutura de Chaves Públicas Brasileira
IoT –	Internet of Things (Internet das coisas)
IPO –	Initial Public Offering (Oferta Pública de Ações)
KYC –	Know Your Customer
LGPD –	Lei Geral de Proteção de Dados
ONU –	Organização das Nações Unidas
P2P –	Peer-to-Peer (Ponto-a-ponto)
PoS –	Proof of Stake (prova de valor)
PoW –	Proof of Work (prova de trabalho)
TICs –	Tecnologias da Informação e Comunicação
UNCITRAL –	United Nations Commission on Internet Trade Law
WWW –	World Wide Web

SUMÁRIO

INTRODUÇÃO 11

1 A REVOLUÇÃO BASEADA NA TECNOLOGIA BLOCKCHAIN 15

1.1 AS ORIGENS DA TECNOLOGIA BLOCKCHAIN 17

1.2 BLOCKCHAIN COMO FONTE DE CONFIANÇA 20

1.3 O FUNCIONAMENTO DA TECNOLOGIA BLOCKCHAIN 22

1.3.1 Criação dos blocos 23

1.3.2 Obtenção de consenso 24

1.3.3 Replicação da cadeia de blocos 25

1.4 MODELOS DE CONSENSO 26

1.4.1 Prova de Trabalho (proof-of-work ou PoW) 27

1.4.2 Prova de participação (proof-of-stake ou PoS) 28

1.5 TIPOS DE *BLOCKCHAIN* 29

1.5.1 Redes Blockchain não permissionadas ou públicas 29

1.5.2 Redes Blockchain permissionadas ou privadas 30

1.6 APLICAÇÕES DA TECNOLOGIA *BLOCKCHAIN* 31

1.6.1 Criptomoedas 32

1.6.2 Proteção da propriedade intelectual 35

1.6.3 Transparência pública e privacidade do cidadão 36

1.6.4 Registro inteligente de propriedades 38

1.6.5 Contratos Inteligentes 39

1.7 ALGUMAS CONSIDERAÇÕES AO FINAL DO CAPÍTULO 1 41

2 OS CONTRATOS INTELIGENTES 42

2.1 BREVÍSSIMO HISTÓRICO 42

2.1 CONCEITO DE CONTRATO INTELIGENTE 45

2.2 CARACTERÍSTICAS DISTINTIVAS DOS CONTRATOS INTELIGENTES 46

2.2.1 Autoexecução 46

2.2.2 Imutabilidade 48

2.2.3 Descentralização 49

2.3 IMPLEMENTAÇÃO DOS CONTRATOS INTELIGENTES 49

2.3.1 Escolhendo uma plataforma Blockchain 52

2.3.2 Codificação dos Contratos Inteligentes 54

2.3.3 Executando o Contrato Inteligente na Blockchain 58

2.4 BENEFÍCIOS DA APLICAÇÃO DE CONTRATOS INTELIGENTES 59

2.4.1 Aumentar eficiência e diminuir custos nas relações contratuais *59*
2.4.2 Gerenciamento de propriedade inteligente *60*
2.4.3 Governança da Internet das Coisas *62*
2.4.4 Criação de Organizações Autônomas Descentralizadas *63*
2.5 DESAFIOS PARA IMPLANTAÇÃO DOS CONTRATOS INTELIGENTES 64
2.5.1 Riscos em face à confidencialidade *64*
2.5.2 Riscos em face à privacidade *65*
2.5.3 Problemas estruturais de tecnologia *67*
2.5.4 Falta de flexibilidade para formalização de obrigações *68*
2.5.5 Dificuldades dos operadores de Direito em face à interpretação jurisdicional *69*
2.5.6 Criação de uma plataforma em prol de atividades ilegais *70*
2.6 ALGUMAS CONSIDERAÇÕES AO FINAL DO CAPÍTULO 2 72

3 REGULAMENTAÇÃO DOS CONTRATOS INTELIGENTES 73
3.1 DEFINIÇÃO DA NATUREZA JURÍDICA DOS CONTRATOS INTELIGENTES 74
3.1.1 Em busca de uma classificação para os Contratos Inteligentes *75*
3.1.2 Equivalência funcional e jurídica dos Contratos Inteligentes *79*
3.1.3 Os Contratos Inteligentes em face à Tricotomia do Negócio Jurídico *81*
3.2 APRECIAÇÃO DAS ESPECIFICIDADES DOS CONTRATOS INTELIGENTES 88
3.2.1 Dos benefícios aos perigos da autoexecução *89*
3.2.2 As duas faces da imutabilidade *94*
3.2.3 Desconstruindo entes centralizadores e eliminando intermediários *99*
3.3 MECANISMOS DE REGULAÇÃO A PARTIR DO MODELO DE LAWRENCE LESSIG 103
3.3.1 Leis estabelecidas pelo Estado *104*
3.3.2 Normas sociais *108*
3.3.3 Forças de Mercado *111*
3.3.4 Arquitetura tecnológica *113*
3.4 CONTRATOS INTELIGENTES COMO INSTRUMENTO DE CONFIANÇA E TRANSPARÊNCIA 115
3.4.1 Promovendo a transparência na administração pública *118*
3.4.2 Construindo confiança no uso dos recursos públicos *120*
3.4.3 Riscos do uso de Contratos Inteligentes na aplicação das leis *122*
3.5 ALGUMAS CONSIDERAÇÕES AO FINAL DO CAPÍTULO 3 124

CONCLUSÃO 126
REFERÊNCIAS 130

INTRODUÇÃO

A evolução das Tecnologias da Informação e da Comunicação (TIC's), em particular o advento da Internet, viabilizou a comunicação instantânea sem barreiras geográficas, transformando profundamente as formas de interação social e possibilitando a criação de relações nunca antes imaginadas. Neste novo contexto tudo é acessível a partir um clique de *mouse* ou de um toque na tela de um *smartphone* provocando nas pessoas uma necessidade irrefreável de estarem sempre conectadas com seus equipamentos à mão. Comunicação, negócios, gestão pública e privada, educação, lazer e praticamente todos os segmentos da atividade humana dependem, em maior ou menor grau, de recursos das TIC's. A própria ONU reconhece oficialmente a importância da Internet em nossa sociedade (ONU, 2012, p. 2). Assim sendo, não é mais possível imaginar a sociedade atual sem os benefícios e os confortos propiciados por esta tecnologia.

Se de maneira geral a Internet possibilitou muitas mudanças positivas para aqueles que a ela têm acesso, não se pode desconsiderar uma série de limitações e problemas que emergem neste cenário. Em que pese a Internet ser uma excelente plataforma para colaboração e comunicação, é notoriamente imperfeita e insegura quando se trata de relações negociais:

> (...) toda atividade realizada por meio de computadores e da internet apresenta riscos, visto que pessoas não autorizadas podem acessar a informação que trafega em redes de computadores (seja essa rede uma intranet, seja a internet), sendo até mesmo possível caracterizar facilmente a transnacionalidade de eventuais condutas delituosas ocorridas nas redes computacionais pelo simples fato de estar a informação, na maioria das vezes, disponibilizada mundialmente, com acessos ou incursões que podem advir de qualquer parte do mundo (CAVEDON, FERREIRA, FREITAS, 2015, p. 211).

Em busca de uma solução que viabilize transações seguras e confiáveis, desponta a tecnologia *Blockchain*. Nesta plataforma a confiança é estabelecida por meio de colaboração coletiva funcionando independentemente de intermediários ou entidades centralizadoras e sendo regulada automaticamente por algoritmos autônomos implementados em linguagem de computador. Composta por uma imensa base de dados distribuída globalmente em um incontável número de dispositivos, nos qual não apenas dados e informações, mas qualquer objeto digital que represente valor, títulos, atos, identidades, até mesmo os votos podem ser armazenados, transmitidos e gerenciados de forma segura,

privada e fidedigna. A premissa da *Blockchain* é estar distribuída por meio da rede de computadores, sendo que as informações não estão sob controle de entes centralizadores (TAPSCOTT, 2016, p. 36).

A tecnologia *Blockchain* apresenta um grande potencial de aplicação, com destaque para o setor financeiro, mas não a ele limitado. Nesse sentido, uma das aplicações mais promissoras da tecnologia *Blockchain* são os Contratos Inteligentes que podem ser usados para implementar relações de negócios sem necessidade de um ente central para certificação da confiança entre as partes envolvidas. Esta tarefa fica por conta de algoritmos computacionais autoexecutáveis que garantem confiança e autenticidade à execução das condições previamente estabelecidas pelos contratantes, provendo transparência às operações, prevenindo eventuais manipulações ou tentativas de fraude, reduzindo os custos e aumentando a eficiência dos negócios (GUPTA, 2017).

Os Contratos Inteligentes promovem uma quebra de paradigma tão radical nas relações contratuais que se suscita um questionamento: estaria o ordenamento jurídico brasileiro apto a recepcionar e tutelar as transformações promovidas e amparar eventuais situações que necessitam de tutela jurisdicional? Nesta dissertação considera-se a hipótese de que os Contratos Inteligentes promovem tamanha transformação nos modelos contratuais que, por mais que a legislação se mantenha sempre em evolução, o ordenamento brasileiro, assim como todos os outros, terá dificuldade de acompanhar a evolução tecnológica e dar amparo jurisdicional a seus efeitos. Deste modo, o objetivo geral do projeto de pesquisa que resulta na presente dissertação foi analisar se o sistema normativo brasileiro possui instrumentos suficientes para recepcionar, tutelar e amparar adequadamente os efeitos produzidos no campo das relações jurídicas pela implementação dos Contratos Inteligentes construídos sobre a tecnologia *Blockchain*.

Dentro deste contexto, o Capítulo 1 apresenta uma síntese da evolução tecnológica que culminou no surgimento da tecnologia *Blockchain*. Composta por um conjunto de várias outras tecnologias que foram sendo aperfeiçoadas do longo das últimas décadas, a tecnologia *Blockchain* debutou por meio do manifesto que apresentou a criptomoeda Bitcoin ao mundo, de autoria de Satoshi Nakamoto, pseudônimo do desenvolvedor ou grupo de desenvolvedores que propôs e distribuiu livremente um modelo computacional no qual são especificados os primeiros moldes da tecnologia *Blockchain*

(NAKAMOTO, 2008, p. 8). Na sequência, são apresentadas as principais características da tecnologia *Blockchain*, uma síntese sobre o seu funcionamento, os principais tipos e os algoritmos pelos quais esta tecnologia gera confiança às transações de forma autônoma, sem intermediários. Por fim, são apresentadas as principais aplicações práticas da tecnologia *Blockchain*, dentre as quais destacam-se os Contratos Inteligentes, objeto do estudo desta dissertação.

Os Contratos Inteligentes, por seu turno, são estudados no Capítulo 2, no qual em primeiro plano é exposto um brevíssimo histórico da evolução dos contratos, passando pelos contratos eletrônicos até chegar aos Contratos Inteligentes implementados a partir da tecnologia *Blockchain*. Em seguida, apresenta-se a conceituação, o modo de funcionamento e as principais características (autoexecução, imutabilidade e descentralização) dos Contratos Inteligentes. Isto posto, é realizada uma reflexão sobre as oportunidades de aplicação de tais contratos e os desafios que surgem no tocante à sua implantação, com um enfoque especial no que tange às questões jurisdicionais.

No Capítulo 3 realiza-se uma reflexão sobre os Contratos Inteligentes com enfoque jurídico estudando, nesta perspectiva, sua natureza jurídica, seus efeitos dentro no contexto do Direito e as suas relações com outros componentes no plano normativo. Para contextualizar esta etapa do estudo foi realizada uma reflexão sobre a definição da natureza jurídica dos Contratos Inteligentes e sua classificação de acordo com o critério de automação dos contratos eletrônicos (SANTOS; ROSSI, 2000, p. 106). Em seguida, os Contratos Inteligentes foram analisados em busca de conferir sua validade e eficácia como negócios jurídicos para, em seguida, analisar-se o impacto da sua aplicação pela perspectiva do Direito e os desafios jurídicos tais como os perigos da autoexecução, conflito da imutabilidade das cláusulas dos Contratos Inteligentes em face à eventuais revisões contratuais, problemas de interpretação jurisdicional em relação à intrincada natureza da codificação em software das cláusulas contratuais, problemas de identificação da natureza jurídica das partes envolvidas e de determinação de um jurisdição diante da descentralização da execução dos Contratos Inteligentes. Diante deste cenário, foi realizada uma análise dos diferentes tipos de regulamentação propostos por Lawrence Lessig (2008, p. 106–129) em busca de um modelo equilibrado que propicie segurança jurídica à implementação dos Contratos Inteligentes ao mesmo tempo que não crie

obstáculos ao avanço da tecnologia. Ao final deste capítulo, são apresentadas oportunidades para aplicação dos Contratos Inteligentes em benefício da governança no setor público e no setor privado.

Ao longo deste estudo percebeu-se que o tema dos Contratos Inteligentes é desafiador, pois trata-se de um objeto multifacetado que envolve entrelaçamento de conhecimentos multidisciplinares para sua análise e implementação. Espera-se, por meio deste estudo, contribuir para o entendimento de qual poderá ser o melhor caminho para garantir a segurança jurídica na implementação de Contratos Inteligentes implementados sobre a tecnologia *Blockchain*.

1 A REVOLUÇÃO BASEADA NA TECNOLOGIA BLOCKCHAIN

O advento da tecnologia *Blockchain* representa profunda revolução nas relações realizadas pela Internet ao implementar uma inédita plataforma para descentralização de serviços tais como pagamentos, recebimentos e gastos, representação e transferência de ativos digitais, implementação e execução de negócios, entre outros. A principal funcionalidade desta tecnologia é possibilitar que qualquer transação entre indivíduos na Internet possa ser realizada diretamente, com segurança e confiabilidade, sem necessidade de um agente centralizador para autenticação da transação. A premissa da tecnologia *Blockchain* é estar distribuída por meio da rede de dispositivos interligados pela Internet, sendo que as informações não estão sob controle de entes centralizadores. Os serviços implementados com esta tecnologia funcionam independentemente de intermediários, independentemente de uma entidade centralizadora, sendo regulada automaticamente por protocolos implementados em linguagem de programação para computador. Deste modo, as pessoas não precisam se preocupar em confiar naqueles com quem se relacionam na Internet, mesmo que desconhecidos, pois a confiança está incorporada no próprio sistema (TAPSCOTT, 2016, p. 34).

A tecnologia *Blockchain* forma uma base de dados de transações distribuída globalmente em milhões de dispositivos e todo seu histórico pode ser acessado por qualquer pessoa sem a ingerência de um ente centralizador. Esta rede organiza qualquer tipo de informação, não se limitando a transações financeiras, podendo incluir valores, títulos, atos, identidades e até mesmo votos. As transações são armazenadas de forma segura, fidedigna e indelével. Esta tecnologia implementa uma revolucionária plataforma, formada por uma corrente de blocos, daí surge o nome *Blockchain*, encadeados por um algoritmo computacional, que contém as regras de funcionamento do seu protocolo. A principal característica desta plataforma é que seus registros podem ser publicamente verificáveis quanto à integridade sem necessidade de se comprometer a privacidade dos autores desses registros (GUPTA, 2017, p. 10).

Ao passo que preserva a identidade dos usuários, a tecnologia *Blockchain* valida e mantém um registro permanente de todas as transações, de tal forma que suas informações pessoais são privadas e seguras, enquanto toda atividade é transparente e

incorruptível. Todas as transações nesta plataforma são reconciliadas por colaboração coletiva e armazenadas em um repositório digital descentralizado que pode armazenar qualquer tipo de informação facilitando as transações entre os pares sem necessidade de intermediários como, por exemplo, um banco ou órgão governamental. Também se disponibiliza recursos para viabilizar transações seguras, mantendo preservada a identidade dos usuários sem que ela seja revelada a agentes não autorizados, pois as partes envolvidas não são identificadas por seus nomes próprios reais ou por identificadores, apenas por pseudônimos (NARAYANAN *et al.*, 2014).

Esta tecnologia pode resgatar parcialmente o espírito de liberdade e independência sonhado pelos pioneiros da Internet, quando a *World Wide Web* se tornou popular e propagou-se quase um consenso utópico sobre seu provável impacto social. Esperava-se que a Internet nivelasse as hierarquias sociais, distribuísse a informação de maneira personalizada e que novas formas de organização social e política surgissem de forma igualitária, acima de discussões econômica e políticas. Concebia-se um mundo com uma estrutura descentralizada para que os internautas pudessem organizar e governar seus próprios negócios, sem a interferência de autoridades centralizadas, conforme proclamado no manifesto “Uma Declaração da Independência do Ciberespaço” (BARLOW, 1996).

Este sonho aos poucos foi se desmantelando à medida em que a Internet foi evoluindo e, cada vez mais, foi se tornando mais concentrada e regulada. Foi esmaecendo a visão idealizada por Barlow de uma Internet em que o poder era descentralizado e havia liberdade de comunicação. A maioria dos serviços de Internet passou a apresentar grande concentração e passou a depender de poucos, mas poderosos e influentes, intermediários que controlam os mecanismos de pesquisa na Internet, redes sociais, serviços de pagamento, plataformas de computação em nuvem, entre outros. Esta concentração gera um considerável poder para que estes intermediários imponham suas próprias regras, possam controlar o conteúdo e até mesmo as escolhas das pessoas que acessam seus serviços. Também o surgimento de telefones celulares com seus ecossistemas de lojas de aplicativos gerou uma grande concentração do poder de controle da Internet. Atualmente há um punhado de corporações que controlam o fluxo de informações e as transações econômicas (BENKLER, 2011, p. 18).

Em busca do resgate destes ideais, desponta a tecnologia *Blockchain,* possibilitando o surgimento de novas formas de organizações, mais transparentes e menos hierárquicas, promovendo que grupos de indivíduos realizem transações mesmo sem se conhecer (DE FILIPPI; WRIGHT, 2018, p. 119-123).

1.1 AS ORIGENS DA TECNOLOGIA BLOCKCHAIN

A tecnologia *Blockchain* é o resultado de uma combinação de várias outras tecnologias da informação que foram amadurecendo ao longo de várias décadas. Os principais elementos que compõem esta tecnologia são a criptografia assimétrica com uso chaves público-privadas[1] e a comunicação por meio de redes ponto-a-ponto na Internet. Em busca de um melhor entendimento do desenvolvimento destas e de outras tecnologias que resultaram no atual modelo da tecnologia *Blockchain*, apresenta-se a seguir uma sinopse desta evolução.

Em 1988, durante o evento conhecido como CRYPTO'88 – 8ª Conferência Anual Internacional de Criptologia, Santa Bárbara, Califórnia, EUA, foi divulgado o Manifesto Criptográfico Anarquista, de autoria de Timothy C. May[2], que apregoava que a combinação dos modelos de criptografia de chave pública e inquebrável com a criação de comunidades em redes virtuais conectadas pela Internet iria produzir "mudanças interessantes e profundas na natureza dos sistemas econômicos e sociais" (MAY, 1988). Este manifesto não se furta em mencionar que os modelos criptográficos poderiam ser utilizados para atividades ilícitas, imorais e ilegais – o que é inevitável para qualquer tipo de tecnologia – porém ele prefere se concentrar em um viés otimista ao propor que este modelo pode transcender fronteiras e liberar as pessoas para fazer os arranjos econômicos que desejem fazer consensualmente.

[1] Criptografia assimétrica, também conhecida como de chave pública envolve um par de chaves conhecidas como uma chave pública e uma chave privada que estão associadas a uma entidade que precisa autenticar sua identidade eletronicamente, assinar ou criptografar dados. Cada chave pública é publicada e a chave privada correspondente é mantida em segredo. Os dados criptografados com a chave pública podem ser descriptografados somente com a chave privada correspondente.

[2] Devota-se neste ponto uma homenagem a Timothy C. May, mais conhecido como Tim May, um escritor técnico e político americano, engenheiro eletrônico e cientista sênior da Intel no início da história da empresa. Ele faleceu em 13 de dezembro de 2018.

Em meados da década de 1990 um movimento composto por criptógrafos e outros tecnólogos, autoproclamados “cypherpunks”, fascinados com os avanços na criptografia de chave público-privada, percebeu o poder das redes ponto-a-ponto e da criptografia, encarando ambas como ferramentas para neutralizar as erosões da liberdade e da liberdade pessoal. Em 1993 foi proclamado o “Manifesto Cypherpunk” que reclamava o direito das pessoas se comunicarem e realizarem transações na Internet revelando somente as informações estritamente necessárias para tal, deste modo preservando sua privacidade. Neste e em outros casos, os intermediários que prestam os serviços de infraestrutura e de aplicações para que a comunicação se estabeleça pela Internet não deveriam saber a identidade de quem está realizando as operações nem tampouco o conteúdo que está sendo transmitido. O manifesto expressamente declara que não se podia esperar que governos, corporações ou outras grandes organizações sem rosto concedessem, privacidade por sua benevolência, pois é de interesse destas organizações controlar a comunicação e saber o que cada um faz na Internet. A solução para mitigar esta ameaça repousa em softwares que implementam a troca de informações protegida por criptografia. Importante ressaltar que o movimento dos Cypherpunks continua ativo em sua missão de manter viva a necessidade alertar que a Internet em uma grande ferramenta em prol do totalitarismo (ASSANGE *et al*, 2013, p. 352).

O movimento de cypherpunks distribui os softwares que produz para serem acessados e usados livremente. Assim este software é disseminado e não pode ser destruído, pois “um sistema amplamente disperso não pode ser desligado” (HUGHES, 1993). Destaca-se, portanto, como fator fundamental para o desenvolvimento da tecnologia *Blockchain* um movimento importante de compartilhamento do desenvolvimento de softwares por colaboradores do mundo inteiro que utilizam a GPL – *General Public License* (Licença Pública Geral), designação da licença de software idealizada por Richard Stallman em 1989, no âmbito do projeto da *Free Software Foundation* (FSF), que permite o livre acesso, execução, distribuição, modificação e redistribuição de código de software, desde que este software seja distribuído na forma da GPL, ou seja, sempre se mantenha livre (FSF, 2007). Em entrevista recente, Stallman novamente alerta para falta absoluta de privacidade na era digital e sobre o controle maciço que os desenvolvedores de tecnologias, em particular celulares e redes sociais, têm sobre os dados pessoais – inclusive dados

sensíveis dos usuários, utilizados para o monitoramento dos usuários segundo ele prática inaceitável que afronta a liberdade das pessoas (EL PAIS, 2019).

A ideia de redes ponto-a-ponto resilientes e descentralizadas também inspirou o jurista e criptógrafo Nick Szabo que publicou um artigo em 1997 apresentando um projeto de protocolos para transações entre pessoas desconhecidas na Internet, cunhando o termo "contrato inteligente", em que apresenta um modelo teórico de como utilizar mecanismos de criptografia para proteger relacionamentos digitais contra violações, interceptação ou interferência maliciosa de terceiros, possibilitando segurança e inviolabilidade com aplicação em importantes áreas de contratação, incluindo crédito, gerenciamento de direitos de conteúdo, sistemas de pagamento e contratos. Szabo propõe que a combinação dos algoritmos criptográficos com a evolução do poder computacional e a capacidade de comunicação em redes públicas, como a Internet, descortinam um horizonte em que será possível formalizar e proteger novos tipos de relacionamento nesse ambiente, inclusive relações comercias e controles contábeis automatizados de forma segura, privada e íntegra (SZABO, 1997).

Dentro deste contexto evolutivo, o primeiro caso prático da tecnologia *Blockchain* foi a implementação da criptomoeda conhecida como Bitcoin, uma inovação monetária baseada em sofisticada estrutura tecnológica, essencialmente digital e descentralizada. Trata-se de um meio de pagamento eletrônico inovador, autopoliciada e autoregulamentada, instantâneo e de alcance global que independe de uma instituição que garanta o seu lastro, sendo uma inovação tecnológica sem precedentes na história da humanidade (EVANS *et al*, 2017). A formalização desta inovação aconteceu em 2008 por meio do manifesto intitulado "*Bitcoin: A Peer-to-Peer Electronic Cash System*" de autoria de Satoshi Nakamoto, pseudônimo do programador que desenvolveu e distribuiu livremente este modelo computacional (NAKAMOTO, 2008, p. 8).

Fruto de um notável avanço na ciência da computação, que se baseia em décadas de pesquisa sobre criptografia realizada por milhares de pesquisadores ao redor do mundo, a tecnologia *Blockchain* é capaz de armazenar informações de forma aberta, descentralizada e sincronizada entre repositórios por meio da Internet, com garantia de segurança, autenticidade e privacidade, portanto, promovendo confiabilidade dos dados armazenados e de suas transações (ANDREESSEN, 2014). Uma analogia bastante pertinente

remonta a ideia de um gigantesco cartório, aberto e gratuito, capaz de registrar e dar transparência perpétua para qualquer tipo de operação (LEMOS, 2016).

Porém, a tecnologia *Blockchain* não significa apenas uma evolução dos meios de transações financeiras, não se restringe ao suporte de criptomoedas ou somente à sistemas da área financeira. Esta tecnologia proporciona uma significativa mudança de paradigma na forma do registro das transações realizadas na Internet, garantindo integridade e confiança nas transações por meio do consenso automatizado de usuários conectados em rede, sem necessidade de uma autoridade central. Sua aplicação é extensível e pode ser muito importante em segmentos sociais, científicos, humanitários, políticos, etc. (SWAN, 2015, p. 24-40).

Sua capacidade de armazenar todo tipo de informação, tais como: registro de automóveis, certidões de casamentos, propriedades, comprovações de autoria e propriedade intelectual, documentos oficiais a exemplo de passaportes, registros médicos, informações logísticas, fluxo de produtos, registros de votações, registros de licitações, orçamentos participativos, entre outros. Sua arquitetura, distribuída e descentralizada, também pode ser aplicada para registrar ativos tangíveis como propriedades físicas, casas, carros ou ativos intangíveis como, por exemplo, votos, ideias, reputação, intenção, dados de saúde, informações, entre outros. Pode-se dizer, portanto, que qualquer lógica de negócios existente pode ser aperfeiçoada pela tecnologia *Blockchain* (KAAL; CALCATERRA, 2017).

1.2 BLOCKCHAIN COMO FONTE DE CONFIANÇA

A tecnologia *Blockchain* dispensa a confiança na outra parte com que se esteja fazendo transações, transferindo a certificação e a validação das transações para o seu próprio controle que é distribuído em rede e verificado constantemente por todo e qualquer participante da rede que se disponha a confirmar as transações. Isto aumenta o nível de confiança entre os participantes da rede, visto que as regras são conhecidas e é fácil verificar se estão sendo cumpridas. Considerando que todas as transações estão registradas em blocos concatenados de forma consistente, qualquer tentativa de adulteração é facilmente identificável pelo sistema, percebida e informada a todos e automaticamente rejeitada por consenso estabelecido automaticamente pelos algoritmos de software que

implementam aquele sistema. Esse autopoliciamento mitiga a necessidade de depender do nível atual de salvaguardas e sanções legais ou governamentais para monitorar e controlar o fluxo de transações comerciais. A comunidade de participantes faz isso. Os atributos de confiança construídos pela tecnologia *Blockchain* estão sustentados em 5 pilares (GUPTA, 2017, p. 10-11):

(i) **Sustentabilidade**: as informações registradas nos blocos da cadeia *Blockchain* são compartilhadas praticamente em tempo real e seu funcionamento não pressupõe a dependência em uma entidade centralizadora sujeitas a falhas e problemas de indisponibilidade;

(ii) **Imutabilidade**: as transações registradas são imutáveis e não podem ser adulteradas. Qualquer necessidade de correção de erros precisa ser realizada por meio de novas transações;

(iii) **Auditabilidade**: o sistema de permissões por meio de chaves criptográficas garante que os participantes sejam quem eles declaram ser. As transações possuem um pseudoanonimato, mascarando a identidade das partes, garantindo a privacidade dos participantes, porém as informações são registradas com data e hora e autenticadas no ato do seu registro na *Blockchain,* assim os participantes de determinada transação têm acesso aos mesmos registros, podem validar transações e verificar informações sem necessidade de intermediários ou terceiros;

(iv) **Consensualidade**: Os algoritmos de autenticação e validação das transações garantem que elas sejam legitimadas pela maioria dos participantes da rede, garantindo a concordância prévia da validade das informações. Cada estrutura *Blockchain* pode estabelecer as condições sob as quais uma transação ou troca de ativos pode ocorrer;

(v) **Flexibilidade**: os protocolos que implementam as plataformas *Blockchain* podem evoluir à medida que amadurecem para suportar processos de negócios em uma ampla variedade de atividades.

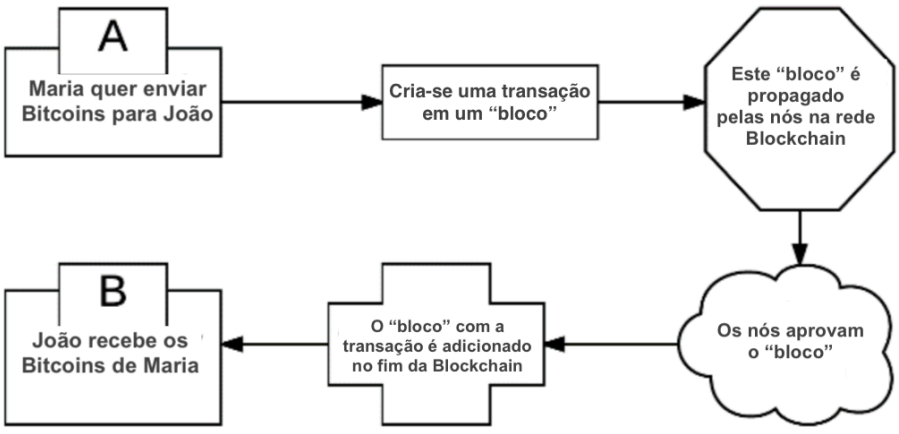
Relevante destacar que as características acima apresentadas são construídas por meio da implementação de sistemas com base na tecnologia *Blockchain*, os quais serão implementados de forma automática e autônoma, confirmando a premissa proposta por

Tapscott de que com o advento desta tecnologia as pessoas não precisam mais se preocupar em confiar umas das outras no sentido tradicional, porque a confiança é incorporada no próprio sistema (TAPSCOTT, 2016, p. 36). Em que pese o referido sistema implementado na plataforma *Blockchain* também dependa de vários participantes para sua implementação (mineradores, desenvolvedores dos algoritmos, participantes que replicam os nós com repositórios de informações, entre outros), toda a plataforma é construída em software aberto e perfeitamente auditável por qualquer parte que se importe conferir seu mecanismos. Para um melhor entendimento a plataforma Blockchain funciona, apresenta-se a seguir o funcionamento desta tecnologia.

1.3 O FUNCIONAMENTO DA TECNOLOGIA BLOCKCHAIN

A tecnologia *Blockchain* é uma arquitetura computacional capaz de armazenar informações de forma aberta, descentralizada e sincronizada entre nós distribuídos pela Internet, que funcionam como repositórios, oferecendo garantia de segurança, autenticidade e privacidade, deste modo, promovendo confiabilidade dos dados armazenados que contém informações dos participantes da rede, mesmo que desconhecidos, com interesses distintos e, por vezes, até mesmo potencialmente conflitantes em suas relações (Eze; Eziokwu; Okpara, 2017, p. 3).

Figura 1 - Como funciona uma transação na *Blockchain*



Fonte: Diagrama adaptado com tradução livre a partir do artigo publicado da Revista *Circulation in Computer Science – Special Issue* (Eze; Eziokwu; Okpara, 2017, p. 2).

Para um entendimento melhor da estrutura, pode-se considerar como exemplo a estrutura de *Blockchain* que atende a criptomoeda *Bitcoin*. A Figura 1 ilustra, de forma simplificada, como acontece uma transação desta criptomoeda. Neste caso prático, tem-se uma cadeia de blocos que registra todas as transações de *Bitcoin* que já foram executadas. Assim, a estrutura de funcionamento da plataforma *Blockchain* necessita das seguintes etapas: (i) Criação dos blocos; (ii) Obtenção de consenso e (iii) Replicação da cadeia de blocos.

1.3.1 Criação dos blocos

A plataforma *Blockchain* do *Bitcoin* têm informações completas sobre endereços e balanços das transações desde primeiro bloco, criado na primeira iteração do software que implementa a *Blockchain*, conhecido como bloco da gênese, até o bloco concluído mais recentemente. Cada vez que uma informação realizada é inserida em um bloco nesta cadeia, ela é criptografada, marcada temporalmente e inserida em um bloco que está encadeado ao bloco anterior, dando sequência a esta cadeia de blocos. Esta corrente é dinâmica em uma de suas pontas e pode crescer indefinidamente a partir do bloco gênese por meio de sucessivos blocos de informação interligados com autenticidade confirmada por meio da aplicação de criptografia assimétrica que usa pares de chaves pública e privada (DE FILIPPI; WRIGHT, 2015, p. 22).

Novos blocos são acrescentados ao fim desta cadeia em ordem cronológica, linear. Cada bloco contém um código único denominado *hash*, um identificador exclusivo criado por uma fórmula matemática de criptografia que funciona como uma espécie de impressão digital daquele registro, calculado com base nas informações do bloco em questão e praticamente impossível de ser revertido. O cálculo do *hash* do bloco atual utiliza o endereço *hash* do bloco imediatamente anterior, assim regressiva e continuamente os blocos são encadeados uns aos outros impedindo que qualquer bloco seja alterado ou que um bloco seja inserido indiscriminadamente entre dois blocos existentes. Desta forma, cada bloco subsequente fortalece a verificação do bloco anterior e, portanto, a cadeia de blocos inteira (GUPTA, 2017, p.14).

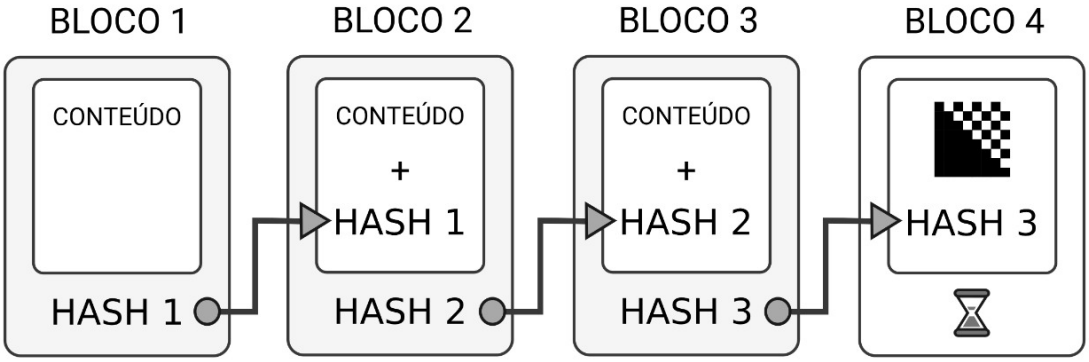
Deste modo, no exemplo do *Bitcoin*, a cadeia de blocos, está crescendo constantemente à medida que são adicionados novos blocos na ponta final desta cadeia. Estes blocos são criados por mineradores, membros da rede que criam novos blocos executando complexas tarefas de criptografia para codificar e encadear estes blocos, sendo são remunerados por meio de uma pequena taxa, paga em frações da criptomoeda *Bitcoin* e creditada nas respectivas carteiras dos mineradores. A mineração protege a plataforma *Blockchain* e permite o surgimento de consenso em toda a rede sem uma autoridade central (ANTONOPOULOS, 2017, p. 229).

Os blocos criados servem para registrar as informações das transações dos usuários que participam da rede *Blockchain* do Bitcoin. Ou seja, temos a figura dos usuários que utilizam a *Blockchain* do Bitcoin para registrar suas transações e temos a figura daqueles que constroem e mantem os blocos da rede *Blockchain*. É possível que um mesmo agente faça o papel das duas personagens nesta estrutura, mas isso não é necessariamente obrigatório, pois trata-se de figuras distintas.

1.3.2 Obtenção de consenso

Para que um bloco seja agregado no final da cadeia é necessário se obter o consenso da maioria dos participantes da rede. Há uma competição denominada prova de trabalho (*proof of work*) entre os mineradores e é realizada uma prova que consiste em resolver um problema matemático altamente complexo. Aquele minerador que conseguir resolver este problema, receberá uma recompensa calculada em *Bitcoins* e então poderá acrescentar um novo bloco. Ocorre que a conferência do cálculo resolvido com sucesso será conferida pelos outros nós da cadeia *Blockchain* sendo necessário um consenso da maioria dos participantes. Deste modo, a cadeia de blocos é permanentemente replicada e mantida sempre sincronizada em todos os computadores conectado à sua rede. Estes computadores têm instalado em si um cliente capaz de validar e retransmitir transações. Os blocos são adicionados e concatenados nesta cadeia formado uma espécie de livro-razão (*ledger*) público de todas as transações de Bitcoin que já foram executadas. Esta cadeia está constantemente sendo incrementada à medida que os mineradores adicionam novos blocos a ele, o que atualmente leva em torno de 10 minutos no caso do protocolo do *Bitcoin* (BTC) para registrar as transações mais recentes (ANTONOPOULOS, 2017, p. 231).

Figura 2 - Criação de blocos em uma *Blockchain*



Fonte: diagramação do próprio autor, 2019.

A figura 2 ilustra como os blocos em uma *Blockchain* são concatenados, destacando que o *hash* de um bloco é calculado a partir de uma combinação do conteúdo do bloco atual com o *hash* do bloco anterior.

1.3.3 Replicação da cadeia de blocos

A cadeia de blocos *Blockchain* é replicada em todos os computadores dos mineradores (nós) que compõem a sua rede, cada nó completo (isto é, cada computador conectado à rede *Bitcoin* usando um cliente que executa a tarefa de validar e retransmitir transações) tem uma cópia do *Blockchain* que é baixado automaticamente quando o minerador se junta à rede Bitcoin.

Como os repositórios são amplamente replicados, todos os dados armazenados em na *Blockchain* são altamente resilientes e tornam a estrutura de informações construída em uma *Blockchain* muito difícil de ser desativada. Uma *Blockchain* pode sobreviver mesmo se uma cópia estiver corrompida ou se um nó em uma rede falhar devido a um evento catastrófico, um ataque externo ou a tentativa de uma jurisdição local tentar encerrar a rede, pois as informações armazenadas em uma rede *Blockchain* podem ser recompostas e replicadas por meio de outros nós que contenham uma cópia (DE FILIPPI; WRIGHT, 2018, p. 427-431).

1.4 MODELOS DE CONSENSO

Em uma plataforma baseada em tecnologia *Blockchain* não há necessidade de se confiar em um terceiro ou em um intermediário que valide das transações entre os usuários, como um banco central, cartório ou uma instituição governamental. Na *Blockchain* as informações são armazenadas e distribuídas por computadores conectados em rede ponto-a-ponto pela Internet, sem obrigação da presença de um servidor central. Toda confiança é garantida por sofisticados algoritmos computacionais implementados por softwares instalados nos computadores que compõe a respectiva rede *Blockchain*. Estes algoritmos tem a capacidade de criar um consenso automático entre os usuários da rede para validar e confirmar a veracidade das transações na cadeia de blocos em que são registradas as informações. Este consenso é obtido por meio de um conjunto de regras rígidas com incentivos e estruturas de custos predefinidos, o que torna difícil e dispendioso para qualquer parte remover unilateralmente ou modificar dados armazenados em um *Blockchain* (DE FILIPPI; WRIGHT, 2018, p. *88-92*).

Os algoritmos do protocolo de uma rede *Blockchain* são desenvolvidos pela própria comunidade de cientistas, pesquisadores e empresas e são implementados de tal forma que a vinculação de um novo bloco depende do consenso da maioria dos outros participantes da rede, tornando a *Blockchain* muito segura, praticamente inviolável, pois adulterar um registro na cadeia de blocos seria necessário alterar todos os blocos anteriores até o bloco gênese para acomodar a informação falsificada, convencendo todos os outros nós da rede *Blockchain* a entrar em consenso com cada uma das interações de alteração. O paradoxo dos mecanismos de consenso é que, mesmo agindo em seu próprio interesse, os participantes da rede *Blockchain* estão servindo a rede ponto a ponto e, por sua vez, estão afetando sua reputação como membros do conjunto da economia (TAPSCOTT, 2016, p. 69).

Considerando que a criação de um novo bloco em uma plataforma *Blockchain* é alcançada por meio de uma prova realizada em uma competição entre os mantenedores dos nós, os mineradores que formam a rede que implementa aquela cadeia de blocos, apresentam-se os vários métodos de se obter esta prova, sendo os principais: (i) Prova de Trabalho (*proof-of-work*) e (ii) Prova de Participação (*proof-of-stake*).

1.4.1 Prova de Trabalho (*proof-of-work* ou PoW)

Trata-se do modelo de obtenção de consenso de muitas criptomoedas baseadas na tecnologia *Blockchain*, inclusive sendo o modelo proposto no manifesto publicado por Satoshi Nakamoto no qual se apresenta o conceito da criptomoeda *Bitcoin* (NAKAMOTO, 2008). Neste modelo de consenso a criação de um novo bloco acontece quando um minerador resolve um enigma matemático baseado em complexa criptografia, realizando uma prova de trabalho. Todos os mineradores de rede competem para ser o primeiro a encontrar uma solução para o problema matemático que diz respeito ao bloco candidato, um problema que não pode ser resolvido de outras formas um grande número de tentativas, requerendo uma grande capacidade de processamento, processo conhecido também como força bruta. Quando um minerador finalmente encontra a solução certa, ele o anuncia para toda a rede e outros nós, na rede, executam cálculos simples para conferir que o *hash* resultante atenda à especificação do protocolo Bitcoin. Ao final deste processo o minerador vencedor da competição recebe uma recompensa, um prêmio pago na criptomoeda implementada no protocolo da *Blockchain* em uso (ANTONOPOULOS, 2017, p. 229).

Este modelo é eficiente para que a rede *Blockchain* alcance consenso, pois todo bloco calculado é submetido à aprovação dos outros participantes e, se a maioria da rede concordar, este bloco é considerado válido e será inserido como próximo bloco na cadeia mais longa. Assim a participação dos mineradores confere se os membros estão agindo de acordo com as regras do protocolo, verificando transações e registrando novos blocos na cadeia (DE FILIPPI; WRIGHT, 2018, p. 477-481).

Apesar de sofisticado e engenhoso, o modelo de consenso por prova de trabalho vem sendo criticado por requerer um tremendo gasto de energia para dispor o poder computacional para a resolução dos complexos problemas criptográficos. Muitos consideram este gasto de energia um desperdício, visto que os problemas matemáticos não têm nenhuma utilidade prática em si, somente server como objeto da competição dos mineradores em busca de criar um novo bloco na *Blockchain* (WORSTALL, 2013). Por outro lado, há quem defenda que este gasto é um custo de operação e que é bem menor do que os gastos com a estrutura centralizada para se manter os registros das transações no modelo atual (SWAN, 2015, p. 1719-1726).

Apesar de muito seguro, o método de consenso por prova de trabalho não é infalível, a remota possibilidade quebra de *hashes* não significa que seja impossível a manipulação dos resultados na criação de blocos. O problema mais relevante do modelo de consenso por prova de trabalho é a vulnerabilidade conhecida como "ataque dos 51%". Trata-se da possibilidade de um grupo de mineradores controlarem mais da metade dos nós de uma rede *Blockchain* (não precisamente 51%, mas a maioria) e com isso conseguirem aprovar novos blocos adulterados, inclusive com a possibilidade de controlar do *Blockchain* e gastar repetidas vezes as mesmas moedas previamente transacionadas em sua própria conta. Segundo Antonopoulos, este tipo de ataque poderia beneficiar um fraudador que, após realizar um pagamento, pode editá-lo ou apagá-lo, modificando novos blocos na *Blockchain*, e com isso duplicando o uso de suas próprias criptomoedas, ou revertendo pagamentos já realizados e obtendo lucro com isso (ANTONOPOULOS, 2017, p. 271)

Nota-se que o problema do ataque de 51% deriva de uma desvirtuação da proposta inicial do modelo *Blockchain* que visa a descentralização e o empoderamento distribuído igualitário à comunidade de participantes. Se este ideal for desvirtuado pela concentração dos nós mineradores, este problema torna-se um risco real. A questão é a tendência de centralização na mineração em que a competição para registrar novos blocos de transação no *Blockchain* faz com que apenas alguns grandes grupos de mineração controlassem a maioria dos registros de transação (KIM et al, 2017).

1.4.2 Prova de participação (*proof-of-stake* ou PoS)

Prova de participação (PoS) é uma categoria de algoritmos de consenso para *Blockchain*s que dependem da participação econômica de um validador na rede. A prova de participação pode fornecer maior proteção contra um ataque mal-intencionado na rede, reduzindo incentivos para ataques e tornando muito dispendioso executar ataques. Este modelo de consenso foi proposto pela comunidade de mantenedores da *Blockchain* e foi cogitado para substituir o modelo de Prova de Trabalho na *Blockchain* da criptomoeda *Ethereum*[3] proposta por Vitalik Buterin em 2014. Seria uma solução para os principais

[3] *Ethereum* é uma plataforma que disponibiliza criptomoedas, similares ao *Bitcoin*, e ao mesmo tempo oferece funcionalidade de criação de pequenos programas em linguagem de computador que podem ser utilizados como base de programação de Contratos Inteligentes (ETHEREUM WIKI, 2018).

problemas do protocolo de consenso por prova de trabalho, originário do *Bitcoin,* tais como os altos custos de energia para a resolução das provas de trabalho e também o risco de dominação da rede por um grupo de atacantes que venha a controlar 51% ou mais dos nós da rede *Blockchain* (ETHEREUM WHITEPAPER, 2014).

Neste modelo, o processo de criar e concordar com novos blocos é realizado por meio de um algoritmo de consenso no qual todos os validadores atuais podem participar e são escolhidos de forma aleatória com base na quantidade de criptomoeda que detém e por quanto tempo a mantém. A aleatoriedade em um sistema de prova de participação impede a centralização, caso contrário, o indivíduo mais rico do sistema sempre criaria o próximo bloco e aumentaria consistentemente sua riqueza e, consequentemente, seu controle sobre o sistema. Este modelo desencoraja ataques pois, mesmo que um atacante se disponha comprar recursos para aumentar suas chances de ser escolhido para criar o próximo bloco, ele aumentaria o valor outros participantes que tem criptomoeda há mais tempo, dando a eles ainda mais chance de participar (ETHEREUM WIKI, 2018).

1.5 TIPOS DE *BLOCKCHAIN*

De um modo geral, os vários tipos de *Blockchain* podem ser classificados conforme o tipo de permissão de acesso, público ou privado.

1.5.1 Redes *Blockchain* não permissionadas ou públicas

É possível se criar uma cadeia de blocos específica para o projeto e convidar toda a comunidade da Internet para participar do projeto. Este modelo consiste em se criar uma *Blockchain* pública, regulada por regras programadas no algoritmo a ser seguido por todos os participantes. Por exemplo, *Bitcoin* e *Ethereum* são implementados sobre *Blockchain*s "sem permissão", abertas e acessíveis a todos que desejem participar. Qualquer pessoa com uma conexão à Internet pode baixar o software de código aberto que controla essas *Blockchain*s e participar da rede, sem revelar sua verdadeira identidade ou pedir permissão prévia (DE FILIPPI; WRIGHT, 2018, p. 620-622).

No caso da *Blockchain* do Bitcoin na qual estão registradas todas as transações desta criptomoeda, também é possível registrar outros tipos de ativos, na verdade, é possível registrar qualquer informação nesta cadeia de criptomoedas chamada Bitcoin

Blockchain. Para isso é necessário criar um bloco adicional no final desta cadeia, ou por meio de mineração, ou pagando para um minerador incluir esta informação em um bloco que será aprovado por meio de consenso fornecendo um *hash* daquela informação registrada na *Blockchain*. Deste modo é possível criar-se um novo projeto e utilizar uma cadeia de blocos *Blockchain* já existente, acatando as regras do modelo escolhido e pagando aos mineradores que criam os novos blocos as micro taxas de remuneração do modelo escolhido. Novos projetos baseados em *Blockchain* utilizam redes públicas já existentes como a *Blockchain* do Bitcoin e, em caso de desenvolvimento de Contratos Inteligentes, a *Blockchain* do Ethereum (DE FILIPPI; WRIGHT, 2018, p. 652-654).

1.5.2 Redes *Blockchain* permissionadas ou privadas

As *Blockchain*s permissionadas são também conhecidas como *Blockchain*s privadas, em que a participação depende de uma autorização de acordo com critérios previamente estabelecidos. O acesso às informações das transações contidas em uma *Blockchain* privada é controlado por meio de credenciais que permitem um acesso de acordo com uma hierarquia de privilégios estabelecidos conforme um acordo entre os participantes do consórcio que forma a rede de nós que compõem aquela *Blockchain*. Deste modo é possível limitar, conforme os direitos de acesso de determinado participante quais componentes ele poderá realizar leitura e se poderá ou não realizar inserções de blocos na corrente da *Blockchain*. Em uma cadeia de *Blockchain* privada, somente participantes autorizados podem realizar determinadas tarefas.

Como o número de membros é controlado e novos membros para serem admitidos têm que ser reconhecidos e aceitos pelo grupo inicial que criou a *Blockchain*, cada parte da rede é conhecida ou de alguma forma confiável. Frequentemente apenas um pequeno círculo de parceiros comerciais, alguns fornecedores, outras contrapartes e os reguladores têm acesso a uma *Blockchain* permissionada. Considerando que é menor o número de participantes em uma rede *Blockchain* privada, o consenso para se adicionar um bloco de informações na rede é menor, portanto, a rede torna-se mais rápida (TAPSCOTT, 2016, p. 103).

Este tipo de *Blockchain* é bem vista no setor financeiro no qual a assimetria de informações proporcionadas pelo maior *know-how* das instituições financeiras em face à

falta de transparência torna-se uma vantagem competitiva para as instituições financeiras. Quando mais poder informacional elas detêm, maior o controle que mantém sobre seus clientes. A ideia de uma tecnologia totalmente descentralizada pode se tornar uma ameaça a esta hegemonia (DE FILIPPI; WRIGHT, 2018, p. 619-634).

Há iniciativas de *Blockchain* privadas, tais como Hyperledger da Linux Foundation que formou um consórcio juntamente com grandes players do mercado corporativos tais como Accenture, ANZ Bank, Cisco, CLS, Credits, Deutsche Börse, Digital Asset Holdings, DTCC, Fujitsu Limited, IC3, IBM, Intel, J.P. Morgan, London Stock Exchange Group, Mitsubishi UFJ Financial Group (MUFG), R3, State Street, SWIFT, VMware and Wells Fargo. Trata-se de um projeto de código aberto com o objetivo de desenvolver a tecnologia *Blockchain* com enfoque voltado para negócios. Todavia, apesar do código-fonte do projeto ser disponibilizado para a comunidade como um todo por meio do site de compartilhamento de projetos GitHub, nota-se que muitos dos projetos desenvolvidos tem como foco a elaboração de *Blockchain*s privadas (LINUX FOUNDATION, 2015).

As redes *Blockchain* privadas não necessitam um complexo modelo de consenso, uma vez que as regras para criação de novos blocos podem ser acordadas entre os participantes sem necessidade da competição entre os mineradores por meio de prova de trabalho. Por outro lado, aumenta possibilidade de conluio entre os participantes, uma vez que conhecidos e determinados, podem existir uma combinação entre alguns em detrimento do interesse de outros. Não se pode desprezar que, no caso das redes privadas de *Blockchain,* a autonomia da rede é afetada frontalmente. Há eminente risco da comunidade se envolver no desenvolvimento da tecnologia *Blockchain* e este conhecimento ser apropriado por influentes corporações que irão criar novos jardins murados, cerceando o surgimento de um ecossistema comunitário livre e inviabilizando o desenvolvimento economias colaborativas (TAPSCOTT, 2016, p. 206).

1.6 APLICAÇÕES DA TECNOLOGIA *BLOCKCHAIN*

Os primeiros casos práticos da tecnologia *Blockchain* são oriundos do mercado financeiro, com destaque para a criação da primeira criptomoeda, *Bitcoin*. Porém o potencial de uma rede *Blockchain* não está restrito ao suporte de criptomoedas ou somente às plataformas de serviços relacionados com a área financeira. Sua aplicação é extensível

e pode ser muito importante em segmentos sociais, científicos, humanitários, políticos, etc. Sua arquitetura, distribuída e descentralizada, pode ser aplicada para registrar ativos tangíveis como propriedades físicas, casas, carros ou ativos intangíveis como, por exemplo, votos, ideias, reputação, intenção, dados de saúde, informações etc.

Alguns autores chegam ao ponto de afirmar que qualquer lógica de negócios existente pode ser aperfeiçoada pela tecnologia *Blockchain* (KAAL; CALCATERRA, 2017). Outros são mais ponderados e consideram que nem todas os negócios demandam um armazenamento de dados sequencial, público e distribuído. Nestes casos poderiam ser interessantes outros modelos computacionais ou até mesmo nem deveriam ser "monetizados" (SWAN, 2015, p. 2045-2052). De todo modo, a introdução do conceito de descentralização e resgate do empoderamento dos usuários no controle de suas próprias transações inspira uma nova consideração sobre a concepção de transferência, troca e relacionamento realizado no mundo digital, tornando válido um estudo dos principais usos da tecnologia *Blockchain*.

1.6.1 Criptomoedas

A tecnologia *Blockchain* pode ser utilizada como base de muitos tipos de operações financeira financeiras – ações, investimentos, títulos, fundos mútuos, derivativos, anuidades, pensões, vaquinhas virtuais (*crowdfunding*), promissórias, empréstimos, contratos, apostas, assinaturas, testamentos, fianças, garantias, entre outros (SWAN, 2015, p. 477). Neste segmento as criptomoedas foram o primeiro e talvez o principal exemplo até o momento. O *Bitcoin* foi a primeira criptomoeda implementada nesta tecnologia e tem como característica mais fascinante a sua natureza orgânica; não sendo emitida por nenhuma autoridade central, tornando-se teoricamente imune à interferência ou manipulação do governo ou de poderosos e influentes grupos econômicos (NARAYANAN *et al.*, 2016).

Uma criptomoeda é uma moeda virtual emitida eletronicamente por meio de um sistema computacional descentralizado que é transacionada entre nós conectados em rede deste sistema. Via de regra, novas unidades de criptomoedas são geradas e colocadas em circulação como forma de remuneração para aqueles, conhecidos como mineradores, que se dispõem a manter os nós que compõem a rede que sustenta a referida criptomoeda e

que fornecem capacidade de processamento computacional para resolver os complexos problemas que, por meio de avançada criptografia, protegem as operações dos participantes da rede, conferindo autenticidade às transações realizadas (EVANS *et al.*, 2017). Além da mineração, as criptomoedas podem ser negociadas e obtidas em troca de moeda fiduciária, produtos ou serviços. Há serviços de carteiras de criptomoedas que possibilitam transações virtuais com criptomoedas a partir de computadores pessoais e celulares (SWAN, 2015, p. 94-96).

Tem-se, então, que as criptomoedas funcionam em uma rede ponto-a-ponto (P2P) distribuída pela Internet e dispensam uma entidade central que concentre a administração do seu sistema, propiciando alta disponibilidade do sistema como um todo, visto que, mesmo que um ou vários dos nós que compõe a rede apresente problemas, a rede vai procurar automaticamente outros caminhos para funcionar. Este conceito é o mesmo que se aplica para o compartilhamento de arquivos por *torrents*[4] usado para distribuir, por exemplo, filmes, jogos e músicas pela Internet; sendo que neste sistema os usuários compartilham arquivos de seus próprios computadores com outros usuários sem necessidade de um servidor único que atue como repositório central e controlador das transferências. A tecnologia ponto-a-ponto serve muito bem para compartilhamento de arquivos comuns. Neste caso, ela não se importa com o controle da duplicação dos arquivos, uma vez que não há perda da informação para o usuário detentor do arquivo na origem, pois este fica intacto seja no seu computador em tempo que é transferido para o computador do usuário destino. Por exemplo, um arquivo digital pode ser copiado de um computador para outro deixando o arquivo original no emissor e criando uma cópia no destinatário. Este processo pode ser repetido infinitas vezes de tal forma que seriam criadas múltiplas cópias do arquivo original que por sua vez seriam réplicas digitais idênticas. Esta característica é altamente indesejável no caso de uma criptomoeda, visto que para a moeda ter valor é necessário que ela seja única e que, uma vez transferida, seu emissor não mais a possua nem possa gastá-la novamente. Disto resulta um dos problemas mais sérios enfrentados por uma criptomoeda, conhecido como "gasto duplo". Considerando que as criptomoedas são baseadas exclusivamente em unidades de informação digital e que estas, por sua vez,

[4] *Torrent* uma forma de compartilhar arquivos entre usuários por meio de um protocolo de rede que transfere as informações de um ponto a outro da rede, sem necessidade de passar por um servidor central. Trata-se de uma comunicação ponto-a-ponto, em inglês denominada *peer-to-peer* (P2P).

poderiam ser indefinidamente duplicadas (copiadas), também uma criptomoeda poderia ser duplicada e suas unidades gastas mais de uma vez em diferentes transações (DE FILIPPI; WRIGHT, 2018, p. 378-380).

Para resolver o problema do "gasto duplo", impedindo que o proprietário de uma criptomoeda transfira uma mesma criptomoeda para mais de um destinatário, desenvolveu-se uma tecnologia ponto-a-ponto, portanto também descentralizada, baseada em complexos algoritmo de criptografia que registra a transferência de uma criptomoeda desde sua origem até o seu destino. Deste modo, transferindo a propriedade do valor e registrando esta operação em cadeias de blocos criptografados – *Blockchain* (NAKAMOTO, 2008).

Desde o seu lançamento em 2009, o Bitcoin gerou um grupo de imitadores – moedas alternativas usando a mesma abordagem geral, mas com diferentes otimizações e ajustes (SWAN, 2015, p. 34-35). Esta intensa proliferação de comunidades virtuais que estão criando e distribuindo o seu próprio dinheiro digital, fenômeno desencadeado pelos desenvolvimentos tecnológicos e pelo aumento do uso da Internet, chamou a atenção dos bancos centrais. Em 2012, o Banco Central Europeu definiu moeda virtual como "um tipo de moeda digital não regulamentada, que é emitida e geralmente controlada por seus desenvolvedores, usada e aceita entre os membros de uma comunidade virtual específica" (ECB, 2012, p. 13).

A implementação de criptomoedas na tecnologia *Blockchain* sucede da possibilidade de se criar objetos digitais, conhecidos como *tokens,* para representar "uma unidade de valor que pode ser obtida e usada em um determinado sistema econômico", o que normalmente se denomina como "moeda" no jargão da Economia. Todavia esta nomenclatura não consegue abarcar todo o sentido de uma criptomoeda implementada na tecnologia *Blockchain*, visto que criptomoedas são diferentes das moedas fiduciárias tradicionais. As criptomoedas, ou melhor dizendo, os *tokens* possibilitam um intrincado e avançado mecanismo de operação que pode trazer benefícios para diferentes atividades (SWAN, 2015, p. 2115-2118).

Há sistemas baseados em tecnologia *Blockchain* que estão emitindo *tokens* para representar ativos financeiros ou participações em novos negócios. São os chamados

ICO's, expressão que significa, em inglês, "*Initial Coin Offering*" que, em português significa "Oferta Pública de Moedas", sendo que as moedas no caso em estudo seriam as criptomoedas. Trata-se de um acrônimo que procura parafrasear os tradicionais, conhecidos e regulados IPO's, em inglês, "*Initial Public Offering*" que, em português, quer dizer, "Oferta Pública de Ações". Por meio destes ICO's as empresas podem levantar fundos emitindo tokens, representando certificados digitais criptografados e registrados na *Blockchain*, que correspondem a algum valor ou serviço de uma empresa. Esses sistemas baseados em *Blockchain* geralmente ignoram barreiras legais que apoiam os mercados financeiros existentes e ignoram os regulamentos cuidadosamente construídos visando limitar a fraude e proteger os investidores (ESMA, 2017). O fato da tecnologia *Blockchain* possibilitar a criação de modelos negócio transnacionais e supralegais é uma característica que ao mesmo tempo que atrai o interesse da indústria financeira também gera intranquilidade. Nem todos os aplicativos e serviços baseados na tecnologia *Blockchain* cumprem estritamente as leis e regulamentações locais. Considerando-se que estes projetos normalmente estão disponíveis globalmente por meio da Internet, é quase que inevitável o conflito com algum jurisidição local (SWAN, 2015, p. 2505).

Manifesto exemplo é o caso das criptomoedas que operam transnacionalmente e ignoram as regulamentações existentes sobre transmissão de dinheiro e lavagem de dinheiro, bem como leis destinadas a combater fraudes e evitar a lavagem de dinheiro, financiamento do terrorismo ou outras atividades ilícitas (DE FILIPPI; WRIGHT, 2018, p. 128). Deste modo, há uma expectativa de como vai se desenrolar uma possível regulamentação governamental para se mitigar estes e outros riscos no desenvolvimento de uma indústria madura de serviços financeiros baseada em criptomoedas (SWAN, 2015, p. 2509).

1.6.2 Proteção da propriedade intelectual

Soluções baseadas na tecnologia *Blockchain* podem auxiliar os autores a proteger suas obras ao criar uma base de dados imutável com informações tais como as datas de registro, proveniência e informações de contato. Para proteger uma obra, digital ou algo no mundo físico, pode-se codificá-la em um arquivo digital e registrá-la em uma cadeia *Blockchain*, gerando o *hash* do respectivo arquivo e certificando que esta obra específica existia em determinada data e hora como uma forma de prova futura. Quando

o mesmo arquivo digital é apresentado novamente, o mesmo *hash* será criado e, portanto, fornecerá a verificação de que os arquivos são idênticos. Se, no entanto, o arquivo digital original tiver mudado de alguma forma, o novo *hash* não corresponderá ao marcador anterior (MORGAN, 2014).

Este registro é uma forma de evidenciar a existência da obra e de sua autoria e tem utilidade para eventuais disputas de direitos autorais. Trata-se de uma prova de existência que pode garantir confidencialidade do conteúdo, pois na *Blockchain* não é necessário armazenar cópia de qualquer documento original uma vez que o *hash* do documento digital que representa aquela obra é calculado na máquina do usuário e enviado para ser registrado em um bloco na *Blockchain* (TAPSCOTT, 2016, p. 78).

Também é possível utilizar esta tecnologia para registrar quem está consumindo, por exemplo, fazendo download deste trabalho e, por meio de Contratos Inteligentes, pode-se criar uma forma de remuneração para aqueles que estão registrados como autores. (SWAN, 2015, p. 491). Os autores podem estabelecer a paternidade de suas obras através do registro na *Blockchain*, garantindo sua originalidade, prevenindo-se contra o uso não autorizado de suas obras e definindo os termos de um contrato no qual as licenças concedidas serão estipuladas e executadas conforme são exercidas as condições acordadas.

Há várias iniciativas que utilizam a tecnologia *Blockchain* para registrar e proteger os direitos autorais como, por exemplo, KodakOne, Binded, Pixsy, TinEye, Ascribe, Mediachain e *Proof of Existence*, MyCelia; as quais usam *Blockchain* para rastrear o uso de obras autorais e gerenciar direitos e distribuição autorizada destas obras. São sites onde se pode registrar uma obra para garantir aos seus criadores os seus direitos sobre ela. Uma vez que os dados registrados em uma rede que é distribuída e descentralizada, a proteção não fica restrita a apenas ao mecanismo de registro. Ela vai ser distribuída pela rede *Blockchain* sendo, desta forma inalterável, duradoura e altamente confiável. Os benefícios são palpáveis: uma redução massiva nos custos de registro, graças a um procedimento mais econômico, menos burocrático e que pode eliminar disputas legais (HEAP, 2017).

1.6.3 Transparência pública e privacidade do cidadão

A tecnologia *Blockchain* e os Contratos Inteligentes nela implementados se propõem a revolucionar a forma como os membros da sociedade interagem entre si e em suas

relações com instituições públicas e privadas, e também propiciando um meio descentralizado e confiável para o armazenamento de informações e registros públicos. As informações dos órgãos governamentais – orçamentos, financiamento de campanhas eleitorais, licitações, portais da transparência – podem ser registradas e disponibilizadas em redes baseadas em *Blockchain*. Deste modo as informações ficam disponíveis de forma perene e distribuídas de forma decentralizada com segurança e confiabilidade. Estes dados na *Blockchain* podem ser acessados por sistemas do próprio governo e de entidades da sociedade civil e um moderno sistema composto de algoritmos que escrutinam uma *Blockchain* pública pode ser programado para combater fraudes, mau uso ou corrupção dos bens públicos. Podem ser implementadas plataformas governamentais que sirvam como repositório de documentos, registros e histórico de transações dos cidadãos com o poder público: um sistema universal de registros de uma sociedade (SWAN, 2015, p. 1474-1475).

Com a tecnologia *Blockchain* e o uso de chaves criptográficas público-privadas, é possível conferir ao cidadão o controle dos seus dados que o Estado detém, quem acessa estes dados, por qual motivo e o que é feito com estes dados conferindo o empoderamento necessário para a implementação de um modelo democrático digital. Exemplo encontra-se no modelo que está sendo desenvolvido na Estônia, um país aclamado mundialmente pelo pioneirismo em avançados serviços públicos baseados em tecnologia da informação. Em 2016, a *E-Health Foundation Estonian* lançou um projeto de desenvolvimento destinado a proteger registros de saúde do paciente usando a tecnologia *Blockchain* no arquivamento de registros de atividades relacionadas. Foi implementada uma plataforma em *Blockchain* para o gerenciamento das informações de saúde dos pacientes que garante a integridade e privacidade dos dados e o controle dos próprios pacientes (e-ESTONIA, 2016). Os registros ficam registrados de forma indelével em um banco de dados distribuído em servidores governamentais que garante a segurança e a integridade dos dados sem necessidade de um intermediário para garantir a autenticidade dos dados eletrônicos, pois esta pode ser comprovada matematicamente pelo assinaturas criptografadas. Isso significa que ninguém - nem hackers, nem administradores de sistemas, e nem mesmo o próprio governo - pode manipular os dados e se safar disso (e-ESTONIA, 2018).

Também o governo estoniano criou um novo serviço conhecido com *e-Residence* no qual qualquer pessoa do mundo pode se registrar como um cidadão estoniano e receber uma identidade digital, abrir empresas e fazer negócios de forma totalmente online. Trata-se de uma identidade transnacional que torna as fronteiras permeáveis e traz benefícios para a realização de negócios e transações internacionais, quebrando o atual paradigma dos atuais marcos regulatórios baseados em jurisdições locais centralizadas (TAPSCOTT, 2016, p. 251).

No Brasil há algumas iniciativas de utilização de soluções baseadas em *Blockchain.* Exemplo disso é o controle de empréstimos por meio de *tokens* registrados na cadeia de blocos do BNDES e controlados por meio de Contratos Inteligentes. Este caso será apresentado em detalhes mais adiante no tópico 3.4.2 deste trabalho, quando serão apresentados exemplos de Contratos Inteligentes.

1.6.4 Registro inteligente de propriedades

Com a tecnologia *Blockchain* é possível implementar um gerenciamento inteligente de propriedade de qualquer tipo de ativo, item ao qual pode ser atribuído algum tipo de valor, seja ele tangível (terras, imóveis, automóveis, objetos, etc.), seja intangível (votos, ideias, reputação, intenção, dados de saúde e informações). Um identificador único (*token*) pode ser codificado na *Blockchain* para cada ativo de forma que ele pode ser rastreado, controlado e trocado (comprado ou vendido). Também podem ser transacionados registros e transações destes ativos e dos direitos a eles inerentes, tendo sempre em mente a capacidade destas transações acontecerem em rede ponto-a-ponto, entre os envolvidos, sem necessidade de um ente certificador (SWAN, 2015, 591-592).

Torna-se possível codificar as propriedades por meio de um registro que possibilita o seu gerenciamento de forma inteligente, ativando e desativando o acesso e a utilização destes ativos de acordo com regras estipuladas e programadas em Contratos Inteligentes. E o potencial deste controle pormenorizado torna-se exponencial ao ser combinado com a colossal quantidade de sensores que estão sendo ligados a objetos como fechaduras, eletrodomésticos, automóveis, objetos pessoais, ferramentas, etc. Trata-se da Internet das Coisas, também muito conhecida pela expressão em inglês *Internet of Things* – IoT. A Internet das Coisas está crescendo de forma consistente e vertiginosa. Estima-se

que em 2020 serão mais de 25 bilhões de dispositivos nela conectados (GARTNER, 2013).

Os ativos que são representados originalmente em formato digital (documentos, músicas, vídeos, informações, etc.) podem ser representados diretamente em uma plataforma *Blockchain*. Porém há ativos que não tem representação digital nativa como, por exemplo, imóveis, veículos, máquinas. A utilização de dispositivos presentes na Internet das Coisas é a resposta para a questão da integração deste objetos não digitais para sua representação em uma plataforma Blockchain e seu gerenciamento por meio de Contratos Inteligentes. A estes objetos podem ser acoplados dispositivos eletrônicos para controle do seu uso, medidores e localizadores, que irão transmitir mensagens digitais que vai permitir o seu gerenciamento digital.

1.6.5 Contratos Inteligentes

Contratos Inteligentes, frequentemente referenciados pelo termo em inglês *Smart Contracts,* são implementações escritas em linguagem de computador dos contratos habituais do cotidiano para que sua automatização seja realizada assegurando o cumprimento contratual, incluindo tratados sociais (TAPSCOTT, 2016, p. 79). Desta forma os direitos e obrigações estabelecidos em um Contrato Inteligente são executados por um computador ou uma rede de computadores assim que as partes chegarem a um acordo ou que determinada condição programada seja satisfeita. A automação obtida pela implementação de um Contrato Inteligente repousa em três elementos principais (SWAN, 2015, 657-664):

(i) **Autonomia**: após sua implantação e do início de sua execução, um Contrato Inteligente opera de forma automática sem necessidade de consultar seu agente iniciador;

(ii) **Autossuficiência**: os Contratos Inteligentes podem ser autossuficientes em sua capacidade de mobilizar recursos - ou seja, arrecadar fundos fornecendo serviços ou emitindo patrimônio e gastando-os em recursos necessários, como poder de processamento ou armazenamento;

(iii) **Descentralização**: os Contratos Inteligentes são descentralizados, pois não subsistem em um único servidor centralizado; eles são distribuídos e auto executados nos nós da rede.

Os Contratos Inteligentes são capazes de processar lógica computacional básica IF-THEN-ELSE ("se isso, então aquilo, senão aquilo outro") e podem ser usados, por exemplo, para gerar e transferir *tokens* (associados a ativos físicos ou digitais), verificar assinaturas, registrar votos e implementar novos sistemas de governança baseados em *Blockchain* (ETHEREUM WHITEPAPER, 2018).

Sua implementação, de forma sintetizada ocorre quando um acordo é realizado quando as partes se comprometeram (de forma irrevogável) na execução do contrato, instalando o contrato em uma plataforma de hospedagem distribuída pela Internet na cadeia *Blockchain*. Uma vez que a execução do código do Contrato Inteligente define que se chegou em um ponto de cumprimento do contrato integralmente ou de alguma de suas cláusulas, significa uma acontecerá a execução proativa (*enforcement*) mediada por meios tecnológicos (SZABO, 1997, p. 2).

O objetivo de um Contrato Inteligente é executar os termos gerais de um contrato e limitar a quantidade de exceções e outros erros. Isso remove simultaneamente a necessidade de terceiros responsáveis por verificar a precisão do processo. Os Contratos Inteligentes implementam funcionalidades podem colaborar para diminuir o número de fraudes e outros fenômenos maliciosos, ao mesmo tempo em que reduzem os custos de transação à medida que os termos do contrato são implementados automaticamente (LAUSLAHTI *et al*, 2017). Uma das características dos Contratos Inteligentes derivada da tecnologia *Blockchain* é a eliminação da necessidade de um intermediário para conferir autenticidade aos contratos. Esta tarefa pode ser realizada por algoritmos computacionais utilizando a tecnologia *Blockchain*, garantindo confiança e autenticidade à execução de contratos entre partes que não se conhecem, provendo transparência às relações contratuais, prevenindo eventuais manipulações ou tentativas de fraude, reduzindo os custos e aumentando a eficiência e a velocidade das relações contratuais (GUPTA, 2017).

Em que pese haver muita expectativa a respeito do potencial disruptivo dos Contratos Inteligentes, sua aplicabilidade ampla e universal ainda suscita desafios.

Considerando que qualquer lógica comercial existente pode ser codificada em um Contrato Inteligente e registrada de forma segura e perene em uma plataforma *Blockchain*, torna-se crucial para a segurança jurídica dos negócios baseados em Contratos Inteligentes que existam meios jurisdicionais para a governança das transformações negociais em questão, para a eventual resolução de conflitos e para a proteção de todas as partes envolvidas, em particular aqueles que se encontram em posição hipossuficiente, como apenas consumidores desta nova tecnologia. (KAAL; CALCATERRA, 2017).

1.7 ALGUMAS CONSIDERAÇÕES AO FINAL DO CAPÍTULO 1

Toda tecnologia tem um poder de transformação impactante, porém algumas tecnologias vão além de simplesmente propiciar meios mais eficientes de realizar aquilo que já se fazia de forma convencional. São as ditas "inovações disruptivas" (CHRISTENSEN, 1997, p. 7) que geram uma reviravolta nos modelos tradicionalmente conhecidos. Neste contexto encaixa-se perfeitamente a tecnologia *Blockchain*. No Capítulo 1 foi apresentada a evolução desta tecnologia, suas principais características diferenciais e a radical transformação que ela pode catalisar em termos criar novos modelos de negócio que gerem confiança aos participantes de forma automática, por meio de algoritmos autônomos, sem necessidade de um ente intermediário certificador. Também foi apresentado o modo de funcionamento de uma rede *Blockchain*, seus tipos e aplicações, em um rol meramente exemplificativo, visto que o potencial de aplicação desta tecnologia é praticamente universal (KAAL; CALCATERRA, 2017, p. 3). Dentre as aplicações arroladas, destaca-se a construção de plataformas para implementação de Contratos Inteligentes, um conceito já proposto desde meados da década de 1990 que agora pode ser implementado na prática pela consolidação da tecnologia *Blockchain*. É sobre este novo modelo de se implementar relações contratuais que está dedicado o próximo capítulo desta dissertação.

2 OS CONTRATOS INTELIGENTES

É esplêndido o potencial da tecnologia *Blockchain* visto que, conforme apresentado no capítulo anterior, esta tecnologia tem amplo campo de aplicação nas mais diversas áreas de negócios, das mais simples realizadas no cotidiano das pessoas até as mais complexas realizadas em ambientes corporativos (REED, 2016, p. 40). Dentro destas possibilidades, destaca-se a aplicação desta tecnologia na construção de plataformas de contratos autoexecutáveis, sem necessidade de um ente central para certificação da confiança entre os contratantes. Trata-se da implementação, na prática, do conceito definido por Nick Szabo (1997) de *Smart Contracts* ou, em tradução literal que tem sido convencionada em português: Contratos Inteligentes, opção preferida nesta dissertação. De todo modo, para uma melhor compreensão dos potenciais impactos dos Contratos Inteligentes em nossa sociedade, em particular do ponto de vista jurídico, o presente capítulo dedica-se a um estudo de seu histórico e origens, características peculiares e oportunidades e desafios que se apresentam em face ao seu potencial de transformações das relações contratuais convencionais.

2.1 BREVÍSSIMO HISTÓRICO

Desde que os povos abriram mão da força bruta para a satisfação de suas necessidades, reconhecendo que o melhor caminho para a obtenção dos seus objetivos é o consenso entre as partes interessadas, as pessoas, consciente ou inconscientemente, estão interagindo por meio de relações negociais e, por conseguinte, estão assumindo obrigações contratuais. Deste modo, os contratos se tornaram o "o fenômeno mais frequente do cotidiano das pessoas, em todas as épocas" (LÔBO, 2017, p. 15).

A evolução das Tecnologias da Informação e da Comunicação (TIC's) também impactou de forma impressionante a vida das pessoas, substituindo inúmeras formas de interação humana, automatizando processos e facilitando a comunicação. Os exemplos das TIC's na sociedade são inúmeros e a celebração de contratos não é, de forma alguma, exceção (GOMES, 2018, p. 43).

As TIC's possibilitaram que contratos, tradicionalmente celebrados por meio de fala, palavras escritas ou ações, também pudessem ser praticados por meio de

computadores e que as etapas de celebração de um contrato fossem automatizadas. Há autores que afirmam que os precursores desta automação podem ser observados nas primitivas máquinas de venda automática, nas quais as transações são baseadas em automação mecânica: o equipamento aceita moedas, possibilita a escolha do produto desejado, confere se o valor depositado é suficiente, devolve o troco no caso de excesso de moedas e, finalmente, e entrega o produto selecionado. A máquina é construída mecanicamente para realizar a venda se as condições programadas forem cumpridas. (LAUSLAHTI *et al*., 2017, p. 12). Qualquer pessoa em posse de uma quantidade suficiente de moedas e com o desejo de comprar um item é capaz de se tornar uma parte contratante neste tipo de transação. Ao escolher o produto desejado que foi exposto na vitrine desta máquina (oferta) e ao inserir voluntariamente moedas para realizar a compra (aceitação), esta pessoa está satisfazendo uma operação sinalagmática com o vendedor, representado por sua máquina (SZABO, 1997).

No plano da informática, o primeiro modelo de tecnologia para automação de contratos foi a *Electronic Data Interchange* – EDI (Intercâmbio Eletrônico de Dados), criada por volta de 1948, no final da Segunda Guerra Mundial, como forma de integrar os sistemas dos que gerenciavam a logística de distribuição de toneladas de alimentos e suprimentos enviados pelos Estados Unidos e aliados para a Alemanha no contexto de pós-guerra. Funcionava como um padrão para exportação de lotes de transações de um sistema a serem transmitidos por telex, rádio ou telefone e depois importados no sistema destino. Na década de 1970 esta tecnologia tornou-se um padrão no mundo corporativo e atualmente, os sistemas de EDI obtiveram ampla adoção, particularmente no gerenciamento de cadeias de fornecimento complexas (DE FILIPPI; WRIGHT, 2018, p. 1428).

Embora muito sendo muito úteis para as organizações comunicarem transações comerciais entre si de forma padronizada, permitindo ao receptor executar a transação pretendida, os contratos de EDI não são muito mais do que meras reiterações de termos e condições existentes, “com apenas algumas expectativas de automação realizadas em ambiente eletrônico” de forma assíncrona e “pouco fazem para mudar a forma como as partes entram e cumprem as obrigações comerciais” (SZABO, 1997).

Notável inovação disruptiva ocorreu com o advento da globalização da Internet na década de 1990 quando também ocorreu uma impressionante evolução do poder

computacional dos equipamentos de informática. Conjugados estes fatores, resulta o surgimento e a proliferação de contratos eletrônicos*,* "assim chamados os que utilizam a rede mundial de computadores, para aquisição ou utilização de produtos ou serviços, ofertados no meio virtual" (LÔBO, 2017, p. 33).

Em que pese, nos primórdios, estes contratos eletrônicos eram apenas reproduções dos contratos tradicionais que foram convertidos em formulários digitais, há considerável evolução proporcionada por este novo modelo, pois agora as partes podem colocar os termos e condições do contrato em um formato capaz de ser processado por um sistema computacional e sua execução pode se dar de forma remota, síncrona e praticamente em tempo real. De todo modo, os contratos eletrônicos continuam limitados a reafirmar termos e condições existentes em formato eletrônico e, em termos jurídicos, estes contratos operam da mesma forma que os contratos tradicionais, apenas com a particularidade de se poder tratar de contratos de adesão, contratação à distância ou de contratos de consumo (GOMES, 2018, p. 43).

Já no final da década de 1990, o cientista da computação e também jurista Nick Szabo, percebeu o vasto potencial da evolução da tecnologia de criptografia de dados no campo dos contratos eletrônicos e publicou o conceito dos Contratos Inteligentes em um artigo de uma revista científica, definindo-os como trechos de software que se auto executam quando os termos do acordo são cumpridos e, devido à sua estrutura descentralizada, também são resilientes e invioláveis (SZABO, 1997). Este modelo descreve como os protocolos criptográficos podem ser utilizados para escrever em software as cláusulas contratuais e vincular as partes reduzindo a possibilidade de um deles descumprir suas obrigações (DE FILIPPI; WRIGHT, 2018, p. 1439).

A teoria de Szabo também assevera que os Contratos Inteligentes diminuem o número de fraudes e outros comportamentos maliciosos ao mesmo tempo em que se reduz os custos de transação à medida que os termos do contrato são automaticamente implementados (LAUSLAHTI *et al*., 2017, p. 12).

O conceito de Contratos Inteligentes pode ser considerado uma ideia a frente do seu tempo. À época, as ferramentas de tecnologia da informação ainda não estavam suficientemente amadurecidas para a implementação de Contratos Inteligentes em larga

escala. O advento da tecnologia *Blockchain* e das arquiteturas de consenso decentralizadas, como visto no capítulo anterior, viabilizariam mais recentemente implementação dos Contratos Inteligentes (LAUSLAHTI *et al.*, 2017, p. 3).

Os Contratos Inteligentes podem ser considerados o uso mais importante da tecnologia *Blockchain*. Em que pese no momento a mais notável aplicação da arquitetura *Blockchain* é a implementação das criptomoedas, servindo além de representação digital de um meio de troca ou de reserva de valor (ULRICH, 2014, p. 93), outros tipos de aplicações também podem ser programadas para disponibilizar uma ampla gama de logísticas de modelos de negócios e não demorará muito para que os Contratos Inteligentes comecem a aumentar e transformar os procedimentos tradicionais do cotidiano, possibilitando uma ampla variedade de novas estruturas de negócios e, a longo prazo, substituindo os controles tradicionais (BBVA *Research*, 2015, p. 4).

Levando em conta todo o potencial da tecnologia dos Contratos Inteligentes, é relevante realizar um estudo de como eles são implementados na prática, definindo seus contornos e transformações no campo jurídico.

2.1 CONCEITO DE CONTRATO INTELIGENTE

A objetiva exposição apresentada por Nick Szabo em seu manifesto, define os Contratos Inteligentes como a combinação de protocolos[5] com interfaces de usuário para formalizar e proteger relacionamentos em redes de computadores, "facilitando e ao mesmo tempo protegendo as etapas de busca, negociação, comprometimento, desempenho e adjudicação constituem o domínio dos Contratos Inteligentes" (SZABO, 1997).

Ao tratar de protocolos, Szabo faz referência à criptografia e outros mecanismos de segurança tecnológica, que formam a base de Contratos Inteligentes. A criptografia e o modelo de chaves de segurança pública e privada são fundamentais para a construção de um modelo de contrato que seja seguro e, portanto, confiável para ambas as partes que ensejam realizar um contrato e, ao mesmo tempo, seja fácil de operacionalizar e tenha a

[5] Um protocolo é um conjunto de regras convencionadas implementadas no hardware, software ou por uma combinação de ambos, que possibilita a conexão, comunicação, transferência de dados entre dois sistemas computacionais.

praticidade de ser implementado com segurança em uma rede pública e descentralizada de computadores, como a Internet.

As obrigações em um Contrato Inteligente já estão programadas em código de uma linguagem de programação formal e estrita e distribuída nos incontáveis nós da rede *Blockchain*, o que viabiliza sua execução automática, de forma segura e confiável, quando determinadas condições pré-negociadas são satisfeitas, uma vez que a natureza descentralizada da rede *Blockchain* é capaz de impedir mudanças não autorizadas de sua lógica interna como resultado de sua natureza descentralizada (BBVA *Research*, 2015, p. 4).

2.2 CARACTERÍSTICAS DISTINTIVAS DOS CONTRATOS INTELIGENTES

O conceito dos Contratos Inteligentes demonstra que qualquer lógica contratual pode ser codificada em uma rede *Blockchain* que possui um protocolo que permite programação computacionalmente universal, dando-lhe uma aplicabilidade extremamente ampla em quase todas as indústrias e áreas de assunto (KAAL; CALCATERRA, 2016, p. 3). Esta programação possibilita que os Contratos Inteligentes transcendam os recursos dos contratos tradicionais, oferecendo três distintas características.

2.2.1 Autoexecução

Os Contratos Inteligentes são executados por agentes autônomos que estão replicados e distribuídos ao longo da rede *Blockchain*. Agentes autônomos são *scripts* que contém instruções de computador codificadas para que se multipliquem e se distribuam entre os nós que compõem a cadeia de blocos da *Blockchain* sem nenhuma intervenção manual. São robôs digitais implementados por software. Um exemplo popularmente conhecido de agente autônomo é o vírus de computador implementado por software pois "uma vez criado e lançado na rede, ele sobrevive replicando-se de uma máquina para outra sem a necessidade de intervenção humana deliberada" (TASPSCOTT, 2016, p. 162).

Como nenhuma parte controla a rede *Blockchain*, um Contrato Inteligente não pode ser interrompido depois de acionado pelas partes que o propuseram, a não ser que tenha sido previamente programada uma cláusula dentro da lógica daquele Contrato

Inteligente para interromper a execução do programa, a qual seria disparada sob determinada condição (DE FILIPPI; WRIGHT, 2018, p. 1463).

Esta característica diferencia os Contratos Inteligentes dos demais tipos de contratos tecnologicamente automatizados. Mesmo os contratos eletrônicos muito disseminados na Internet na onda do *e-commerce* são implementados de forma que sua execução pode ser interrompida pela intervenção humana em qualquer momento. No caso dos Contratos Inteligentes, a execução completa do contrato, incluindo a transferência de valores e bens ocorre de forma automática e imutável (GOMES, 2018, p. 46).

A questão da autoexecução proporcionada pelos Contratos Inteligentes tem demonstração admissível quando os objetos de execução são ativos[6] virtuais como, por exemplo, criptomoedas ou outros ativos digitais, os quais têm seu controle e administração em uma estrutura de *Blockchain*. Porém quando se trata de ativos do "mundo real", os Contratos Inteligentes ainda têm pouco alcance. Os Contratos Inteligentes funcionam muito bem com ativos oriundos do mundo digital, aqueles que foram implementados por meio de *tokens* que representam o seu valor no mundo real. Um Contrato Inteligente com ativos tradicionais, sem representação no mundo digital, ainda necessita de muito arranjos para ser de fato efetivado (BBVA *RESEARCH*, 2015, p. 5). Uma solução para este dilema é a combinação da tecnologia *Blockchain* com a tecnologia da Internet das Coisas, conforme previamente apresentado no item 1.6.6 deste trabalho.

Todavia, o próprio Nick Szabo já previa em seu manifesto há algumas décadas que a evolução da tecnologia da informação avançaria a tal ponto que os objetos físicos seriam controlados por autômatos digitais. Neste mesmo artigo, Szabo apresentou um exemplo de um Contrato Inteligente de locação de um veículo propondo que, se o contratante deixasse de pagar o aluguél do carro, inadimplindo uma regra programada, neste momento um gatilho seria disparado e seria executado o bloqueio do veículo, impedindo o acesso ao carro e devolvendo as "chaves virtuais" para o banco (SZABO, 1997). Pode-se dizer que esta profecia está se tornando realidade pois qualquer ativo pode ser registrado no *Blockchain* e, portanto, sua propriedade pode ser controlada por quem tiver a chave privada. O proprietário pode vender o ativo transferindo a chave privada para outra

[6] Ativo é um termo contábil que serve para referenciar determinado objeto que representa um valor.

parte. “Propriedade inteligente, então, é aquela controlada via *Blockchain*, usando contratos sujeitos à lei existente” (SWAN, 2015, p. 603-606). Considerando o conceito de propriedade inteligente, tem-se que a autoexecução dos Contratos Inteligentes torna-se próxima da realidade.

2.2.2 Imutabilidade

A imutabilidade dos Contratos Inteligentes deriva da inviolabilidade das informações da arquitetura *Blockchain* e da sua estrutura de armazenamento baseada em forte criptografia (LAUSLAHTI *et al*., 2017, p. 7). Uma vez que um Contrato Inteligente, suas cláusulas e transações são enviadas para a *Blockchain*, estas informações são submetidas consenso dos nós participantes e quando aprovadas são eternizadas em um bloco da cadeia daquela *Blockchain* não sendo mais possível alterar ou apagar o seu conteúdo. Caso seja necessária alguma retificação, é necessário executar o ciclo novamente inserindo as informações retificadas em um novo bloco, novamente replicando as informações em toda aquela *Blockchain*.

A segurança dos Contratos Inteligentes é reforçada pela implementação de um sistema de assinaturas digitais[7] composto por um par de chaves assimétricas para codificar e decodificar as informações. Deste modo, cada parte envolvida em uma relação contratual em um Contrato Inteligente possui duas chaves conjugadas em um par: uma chave pública e uma chave privada. A chave pública é divulgada e pode ser conhecida pelos outros participantes da relação. A chave privada, por sua vez, é secreta e somente o seu proprietário deve ter acesso a ela e mantê-la em sigilo e segurança pois, se alguém tiver acesso indevido a ela, poderá decodificar todas suas informações. Quando uma parte deseja enviar uma mensagem para outra, o remetente codifica a mensagem com sua assinatura privada. Assim quando esta mensagem chegar ao destinatário ele poderá decodificar esta mensagem com a chave pública do remetente obtendo, assim, uma certificação que a mensagem é realmente daquele remetente e que seu conteúdo não foi alterado (MODI, 2018, p. 7).

[7] Uma “assinatura digital”, neste contexto, não se trata de uma assinatura biométrica e sim de uma assinatura baseada em uma chave privada (código secreto armazenado em um arquivo de computador) usada pelo seu proprietário para decodificar mensagens a ele destinadas.

Os Contratos Inteligentes também podem exigir múltiplas assinaturas digitais para que determinada transação seja executada, ou seja, duas ou mais partes são notificadas quando determinada condição foi satisfeita e para executar determinada ação, como por exemplo, liberar pagamentos, as partes são notificadas e é solicitada sua aprovação, o que é muito útil para contas corporativas, contas de poupança seguras e algumas situações de depósito e transferência de ativos (ETHEREUM WHITEPAPER, 2015).

2.2.3 Descentralização

Esta característica mitiga a dependência imposta pelas arquiteturas centralizadoras nas quais as informações são custodiadas por um número restritos de servidores, normalmente mantidos por uma ou escassas entidades, que trazem para si toda a responsabilidade de prover a estrutura para o funcionamento dos sistemas e, ao mesmo tempo, sendo pontos únicos de falhas operacionais e brechas de segurança. Os Contratos Inteligentes, por sua vez, utilizam todo o potencial de segurança proporcionado pela plataforma *Blockchain* sendo armazenados, distribuídos e executados nos nós descentralizados (SWAN, 2015, p. 662-665).

A descentralização da estrutura que mantém os Contratos Inteligentes também contribui para a eliminação da necessidade da centralização em entidades para autenticação, conferência e endossamento das transações. A confiança nas informações advém do próprio sistema de informações e é obtida por meio do consenso entre os participantes da rede que validam os blocos por meio dos protocolos de verificação e constantemente replicam todo a base de dados entre os participantes da rede. Assim, os Contratos Inteligentes "são conferidos por todos os nós da rede. Isso significa que todo nó deve executar cada contrato em um *Blockchain*, portanto, o código do contrato é executado por cada nó na rede" (WALL; MALM, 2016, p. 40).

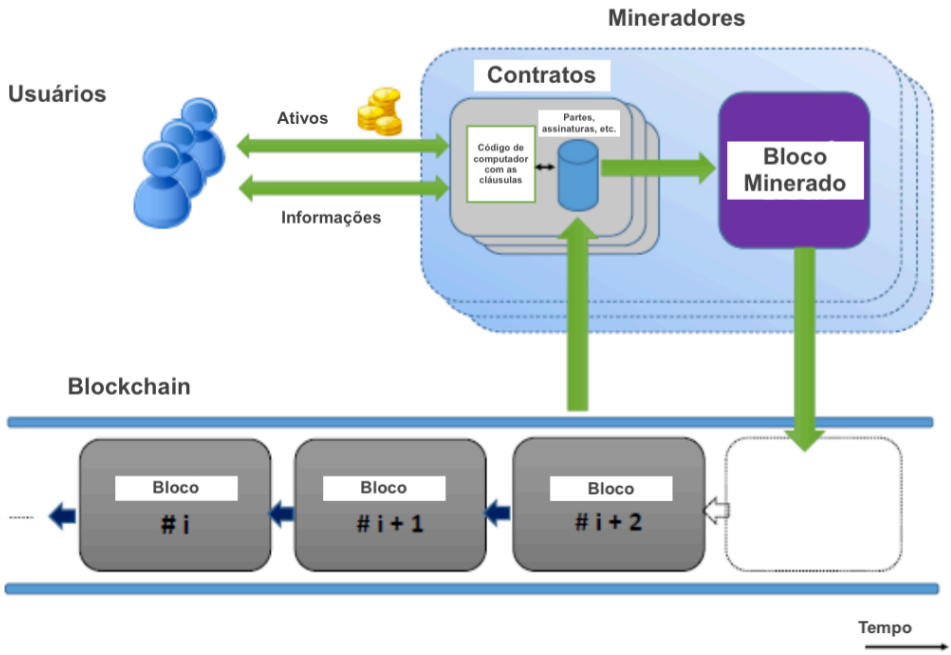
2.3 IMPLEMENTAÇÃO DOS CONTRATOS INTELIGENTES

Os Contratos Inteligentes são o resultado da combinação de protocolos de informática, interfaces com usuários e promessas expressas por meio dessas interfaces, para "formalizar, proteger e executar relações contratuais em redes públicas" (SZABO, 1997), com é o caso da Internet. Por meio de sua implementação é possível aperfeiçoar a prática

dos contratos convencionais e, mais do que isso, é possível motivar novas maneiras de formalizar as relações contratuais.

Em um primeiro plano, os Contratos Inteligentes podem ser implementados seguindo a lógica dos contratos tradicionais, positivada pelo mundo jurídico em linguagem humanamente compreensível, realizando uma tradução[8] para linguagem de computador. Uma vez que as partes negociaram os termos de sua relação contratual, fase que Szabo denomina de "encontro de mentes" (SZABO, 1997), estes termos escritos em linguagem natural devem ser transcritos em código de software por meio de uma linguagem de programação estrita e formal para "ser executado de maneira distribuída por todos os nós que suportam a rede subjacente baseada em *Blockchain*, sem necessariamente depender de qualquer operador intermediário" (DE FILIPPI; WRIGHT, 2018, p. 1461). Deste modo, na Figura 3 apresenta-se um diagrama que ilustra os componentes dos Contratos Inteligentes e suas interações com uma cadeia de blocos da *Blockchain.*

Figura 3 - Como funciona um Contrato Inteligente



Fonte: Diagrama adaptado com tradução livre a partir do artigo publicado da Revista *Circulation in Computer Science – Special Issue* (Eze; Eziokwu; Okpara, 2017, p. 3).

[8] Já há projetos de que esta tradução seja realizada automaticamente por meio de Inteligência Artificial, o que não é objeto deste estudo, mas pode se tornar um projeto futuro de pesquisa.

Atentando que um contrato tradicional típico contém relevante dose de complexidade, uma abordagem intuitiva mais producente para simplificar o procedimento de conversão de um contrato convencional para um Contrato Inteligente seria gerar um código de software específico para cada cláusula, de forma que a execução fosse "modularizada em pequenos trechos"[9] contendo testes de condições e respectivas ações ou sanções a serem executadas por meio de gatilhos quando aquelas condições fossem, respectivamente, satisfeitas ou não satisfeitas.

Esta abordagem modularizada também é proveitosa para tratar de disposições contratuais presentes nos contratos convencionais que são abertas, imprecisas e muito subjetivas, não sendo diretamente traduzíveis em lógica computacional, a qual tem natureza organizada de forma binária e muito estrita. Muitas vezes a ambiguidade dos contratos é necessária para resultar em contratos mais eficientes e flexíveis. Também é importante ponderar que nem sempre é possível prever todas as condições e eventos futuros durante a fase de negociação dos contratos. Nesse caso, manter contratos abertos pode ser uma forma de reduzir o tempo e o custo da negociação. Deste modo, com a abordagem modular é possível construir contratos híbridos no quais outras partes muito subjetivas podem ser construídas de forma convencional, enquanto partes objetivas do contrato pode ser implementadas como Contratos Inteligentes e depois integradas às primeiras (DE FILIPPI; WRIGHT, 2018, p. 1502).

Para efetivar a codificação propriamente dita em linguagem de programação, há plataformas de software que agrupam as ferramentas necessárias para a codificação de um Contrato Inteligente. Também há interfaces gráficas amigáveis e intuitivas para auxiliar na sua programação. De todo modo, seria muito pretensioso afirmar que qualquer usuário pode realizar a programação de um Contrato Inteligente sem uma boa noção dos elementos computacionais envolvidos no seu desenvolvimento. E, sem o devido conhecimento jurídico, também seria temerário que um usuário final ou até mesmo que um analista de sistemas ou um programador, se aventurassem por conta própria a desenvolver e programar um Contrato Inteligente. Trata-se de uma missão de muita responsabilidade. Tentar transcrever os negócios jurídicos diretamente para a linguagem de computador

[9] Metodologia de ciência da computação conhecida como "Dividir e conquistar". https://pt.khanacademy.org/computing/computer-science/algorithms/merge-sort/a/divide-and-conquer-algorithms. Acesso em 22 fev. 2019.

sem o crivo de um especialista jurídico pode trazer consequências arrepiantes. E a situação se agrava considerando-se que a natureza de autoexecução dos contratos inteligentes (*auto enforcement*). No estágio atual do ecossistema de tecnologias que compõem a estrutura de desenvolvimento dos Contratos Inteligentes, pode-se dizer que se trata de uma empreitada multidisciplinar.

Outro ponto a ser considerado com a máxima atenção é a questão das falhas de software. Assim como todo software, um Contrato Inteligente precisa ser testado exaustivamente antes de ser colocado em produção. Nenhum software é imune a conter *bugs*[10] em seu código. Avaliando que a execução de um software pode combinar um grande número de variáveis, gerando um número exponencial de combinações entre elas, a margem de possibilidade de erro, por menor que seja, é consideravelmente significativa. Em se tratando de relações contratuais, um erro em um software que gerencia um contrato coloca em severos riscos as partes envolvidas. Este risco torna-se potencializado ao extremo quando se sopesa que um Contrato Inteligente é indelével, autônomo e potencialmente difícil de ser encerrado depois de implantado (DE FILIPPI; WRIGHT, 2018, p. 99-101).

Deste modo, os próximos tópicos se propõem a apresentar um panorama geral das etapas de implementação de um Contrato Inteligente na arquitetura *Blockchain*. Mesmo sem entrar em minúcias técnicas, se faz deveras importante o entendimento dos componentes que compõem o Contrato Inteligente e suas interrelações para que se possa projetar suas possibilidades e limitações de forma consciente e responsável.

2.3.1 Escolhendo uma plataforma *Blockchain*

Qualquer lógica de negócios existente pode ser codificada no *Blockchain*, dando-lhe uma aplicabilidade extremamente ampla em quase todas as indústrias e áreas de assunto. No caso dos Contratos Inteligentes não é diferente, eles podem ser implementados, armazenados e executados em uma plataforma *Blockchain*. Porém nem todas as plataformas *Blockchain* são iguais. Como uma *Blockchain* possui código aberto, é possível novos projetos estabeleçam modificações em seus protocolos com o objetivo de

[10] Um bug de software é um erro ou falha em um programa de computador que faz com que ele produza um resultado incorreto ou se comporte de maneira não intencional.

fornecer novas capacidades para determinados modelos de negócios (KAAL; CALCATERRA, 2016, p. 3). Por exemplo, a *Blockchain* mais conhecida e mais utilizada no momento é aquela que atende a criptomoeda Bitcoin. Contudo, esta cadeia de blocos que atende o Bitcoin tem um conjunto de instruções computacionais limitado para atender transações financeiras pois ainda lhe faltam algumas funções necessárias para a implementação de um Contrato Inteligente como, por exemplo, uma função para repetição (*loops*) de blocos de código e também lhe falta a capacidade de controlar estados intermediários de uma transação. A ausência destas funções não afeta o desempenho das transações em Bitcoin, pelo contrário, tornam o protocolo mais específico e mais performático. Todavia, para programação de Contratos Inteligentes na *Blockchain* do Bitcoin seria necessário improvisar arranjos técnicos para implementar as funções computacionais ausentes (ETHEREUM WHITEPAPER, 2015, p. 1).

A efervescência e o entusiasmo da comunidade de desenvolvedores em torno da tecnologia *Blockchain* foi muito fecunda. Diversos projetos floresceram e alguns deles tornaram-se modelos de referência tanto no universo acadêmico quanto no corporativo. Um dos mais notáveis exemplos trata-se da plataforma Ethereum, proposta em 2013 pelo jovem russo, radicado no Canadá, Vitalik Buterin (ANTONOPOULOS; WOOD, 2018, p. 653-654). "Ethereum é uma tecnologia *Blockchain* de segunda geração que foi projetada especificamente como uma plataforma de Contratos Inteligentes descentralizada" (WALL; MALM, 2016, p. 40).

Esta plataforma implementa um computador virtualmente distribuído pelos nós de uma *Blockchain*. Como um computador genérico, o Ethereum pode carregar o código em sua máquina virtual e executar esse código, armazenando as mudanças de estado resultantes em seu *Blockchain*. As duas maiores diferenças do Ethereum para um computador convencional e que esta plataforma funciona na base do consenso e o estado de suas informações é distribuído globalmente (ANTONOPOULOS; WOOD, 2018, p. 720-727).

O Ethereum pode ser considerado uma plataforma modular para programadores escreverem Contratos Inteligentes. A plataforma Ethereum fornece uma plataforma denominada Máquina Virtual Ethereum – *Ethereum Virtual Machine (EVM)* – que reproduz uma estrutura computacional completa conformando-se plenamente em uma máquina de

Turing[11] que pode ser utilizada para programar Contratos Inteligentes com facilidade de desenvolvimento em um ambiente econômico e seguro (REED, 2016, p. 22).

Os Contratos Inteligentes programados na plataforma Ethereum são muito mais do que apenas formulários a serem preenchidos. Trata-se de agentes autônomos que "vivem" dentro da plataforma da *Blockchain* sempre prontos para executar uma parte específica do seu código quando for disparado determinado "gatilho" por uma mensagem ou transação, tendo controle direto sobre recursos próprios para sua autoexecução (ETHEREUM WHITEPAPER, 2015).

A evolução das soluções baseadas em tecnologia *Blockchain* proporciona também uma evolução e um amadurecimento significativo da plataforma Ethereum encontram um ambiente que dispõe de uma oportunidade real para o desempenho descentralizado de programas dentro do *Blockchain*, viabilizando a programação de Contratos Inteligentes (LAUSLAHTI *et al.*, 2017, p. 12).

Uma vez vencida a etapa da escolha de qual *Blockchain* será utilizada para a implementação dos Contratos Inteligentes, avança-se para o passo seguinte que vai tratar da codificação dos mesmos.

2.3.2 Codificação dos Contratos Inteligentes

Para que as semânticas contratuais possam ser "computáveis" e transcritas em um Contrato Inteligente é necessário que elas possam ser expressadas por meio de uma série de instruções seguindo uma lógica em uma linguagem de programação de computadores. O conjunto destas instruções codificadas em linguagem de programação vai determinar que um computador "possa processar e que todas as informações necessárias para o processamento do contrato se encontrem disponíveis e acessíveis pelo computador em formato digital" (GOMES, 2018, p. 44).

[11] O conceito de máquina de Turing propõe um dispositivo teórico conhecido como máquina universal, que foi concebido pelo matemático britânico Alan Turing (1912-1954), muitos anos antes de existirem os modernos computadores digitais. Em 1936, ele criou um modelo matemático de um computador que consiste em uma máquina de estado que manipula símbolos, lendo-os e gravando-os em memória sequencial, semelhante a uma fita de papel de comprimento infinito. Em uma máquina de Turing é possível emular qualquer computador digital (ANTONOPOULOS; WOOD, 2018, p. 774-777).

A escolha da linguagem de programação utilizada para codificar um software está intimamente ligada com a plataforma em que este software será implementado e executado. Considerando que, no momento a plataforma mais propícia para o desenvolvimento de Contratos Inteligentes seria a *Blockchain* do Ethereum, torna-se necessário realizar a sua codificação de acordo com as especificações do grande computador virtual e distribuído desta plataforma.

No caso da plataforma do Ethereum, os Contratos Inteligentes precisam ser codificados para funcionar na Máquina Virtual Ethereum (EVM). Neste ambiente computacional há possibilidade de se utilizar algumas linguagens de programação, entre as quais destacam-se Solidity[12], Serpent[13], LLL[14] e Vyper[15]. Há importantes diferenças entre estas linguagens. A linguagem de programação Solidity é uma linguagem de alto nível, o que significa, em termos de ciência da computação, que ela é similar a uma linguagem humana natural como o inglês. Esta linguagem é a que tem maior similaridade com linguagens de programação muito conhecidas e difundidas como C++, Python e JavaScript e possui uma estrutura orientada a objetos, bastante popular entre a comunidade de programadores. As linguagens Serpent e LLL são minimalistas, muito rápidas, porém implementas como linguagens de baixo nível, ou seja, uma linguagem programação de que se aproxima mais dos códigos de máquina (computador), sendo quase ininteligível para interpretação direta de pessoas e, portanto, recomendadas apenas para programadores muito experientes. A linguagem Vyper, por sua vez, é uma linguagem mais simples e mais inteligível mesmo para programadores intermediários, entretanto ainda está em estado experimental. Deste modo a melhor escolha, no momento, seria codificar o Contrato Inteligente na linguagem Solidity.

Mesmo sendo a linguagem de programação Solidity uma linguagem de alto nível, com comandos e funções escritos em uma forma mais próxima de uma linguagem natural, a lógica de programação e as metodologias de desenvolvimento de software não

---

[12] **Solidity homepage**. Disponível em https://solidity.readthedocs.io/en/latest/index.html. Acesso em 16 jan. 2019.
[13] **Serpent language introduction**. Disponível em: https://github.com/ethereum/serpent. Acesso em 16 jan. 2019.
[14] **Lisp Like Language**. Disponível em: https://lll-docs.readthedocs.io/en/latest/lll_introduction.html. Acesso em 16 jan. 2019.
[15] **Vyper, a contract-oriented, pythonic programming language**. Disponível em: https://vyper.readthedocs.io/en/v0.1.0-beta.6/. Acesso em 16 jan. 2019.

são fáceis e óbvias para qualquer usuário, por mais avançado que seja, codificar um software tal qual um Contrato Inteligente. Via de regra, softwares são criados por desenvolvedores e programadores de computador, "pois exigem uma compreensão profunda de como funcionam os códigos binários" (REED, 2016, p. 38). Talvez uma interface amigável poderia ser útil, como por exemplo a plataforma que oferece ferramentas visuais para todo o processo de implementação de um Contrato Inteligente. Mas mesmo assim seria necessário um conhecimento mais técnico do usuário ou, o mais recomendável, uma assessoria de pessoal perito em desenvolvimento de sistemas.

Para exemplificar, apresenta-se um trecho de código de software de um Contrato Inteligente que exibe uma função que verifica se há crédito na conta de origem, para depois fazer transferência de fundos, debitando da conta origem `[msg.sender]` ao mesmo tempo que credita na conta destino `[to]` (TRUFFLE, 2019).

```
pragma solidity ^0.4.18;
contract Token
{
     mapping (address => uint) balance;

     function transfer(address to, uint amount )
     {
           require(balance[msg.sender] >= amount);
           balance[msg.sender] -= amount;
           balance[to] += amount;
     }
     …
}
```

Independentemente da linguagem de programação escolhida, uma tarefa imprescindível ao se codificar um Contrato Inteligente é a parametrização das informações que precisam ser armazenadas e também especificar as condições que serão testadas durante os eventos que se sucedem na consecução da relação contratual e que funcionarão como gatilhos disparando ações programadas, sempre lembrando que um Contrato Inteligente tem o conceito de ser autossuficiente e autoexecutável, ou seja, para uma ativação sem erros, o seu código precisa conter as ligações (*links*) para obter os valores das variáveis definidas, bem como a localização dos ativos digitais (*tokens*[16]) que são objetos de sua autoexecução do Contrato Inteligente e que também serão utilizados para o

[16] *Tokens* são unidade de representação digital de um item que tem valor em si (econômico, incentivo, reputacional, etc.) Os sistemas de *token* são surpreendentemente fáceis de implementar no Ethereum (ETHEREUM WHITEPAPER, 2015).

micropagamento dos nós que sustentam a *Blockchain* na qual está sendo armazenado, implementado e será executado o Contrato Inteligente (REED, 2016, p. 25).

Cabe aqui uma ressalva relevante sobre os repositórios de informações que serão acessadas pelo Contrato Inteligente, pois nem todas as informações necessárias para teste das condições estarão disponíveis na *Blockchain* na qual aquele Contrato Inteligente é executado. Para se obter informações externas à *Blockchain* (por exemplo; informações do mundo real como preços, cotações, reputações, etc.), os Contratos Inteligentes implementados em Ethereum se valem de entidades conhecidas como oráculos. Os oráculos funcionam como portais de passagem (*gateways*) para repositórios de informações externas à *Blockchain* que podem ser consultados por um Contrato Inteligente para obtenção de determinada informação para validar e dar continuidade à sua execução.

Os oráculos precisam ser muito bem definidos pelas partes, pois pode facilmente se tornar um ponto de vulnerabilidade em um Contrato Inteligente, além do mais, o uso de oráculo fere frontalmente o princípio da descentralização, pois esta fonte de dados seria controlada por uma única entidade que poderia manipular as respostas, pois se um oráculo não for uma fonte confiável ou isenta, pode ser utilizado por pelas partes para inserção manual direta de informações manipuladas e tendenciosas. Em tese, um oráculo poderia ser uma fonte oficial de informações de terceiros como, por exemplo, a Bolsa de Valores ou sites de índices de instituições comprovadamente fidedignas. Todavia será necessário que o Contrato Inteligente dependa de uma única fonte de informação ao adquirir dados de fontes externas, o que suscita uma fragilidade. Uma ideia para se mitigar este risco seria consultar várias fontes de dados, filtrando respostas anormais e calculando um valor médio dos restantes. O nível de risco em tal caso pode ser considerado tolerável em certos sistemas (WALL; MALM, 2016, pp. 41-43).

Após a etapa da definição das variáveis, dos repositórios de informações e da reserva dos ativos digitais para transação entre as partes e para os micropagamentos da estrutura da *Blockchain*, serão definidas as tarefas específicas que o Contrato Inteligente vai executar e quais são os seus respectivos acionadores, em outras palavras, as partes do contrato. Estas partes são aquelas que possuem contas com ID's pessoais que as representam e que possuem respectivas chaves privadas para acessar e assinar suas transações. O código do Contrato Inteligente possui várias seções nas quais são codificadas as

cláusulas que definem a relação contratual tornando-se um agente autônomo que possui um código identificador único (conta do contrato) e também vinculando-se à chave privada do agente que o inseriu na *Blockchain* e às chaves privadas das partes nele participantes (REED, 2016, pp. 25-28).

2.3.3 Executando o Contrato Inteligente na *Blockchain*

Uma vez que gerado o código fonte do Contrato Inteligente em linguagem de alto nível, no caso Solidity, ele precisa ser compilado, ou seja, traduzido para uma linguagem de pré-processamento de máquina, gerando o código objeto ou, em termo técnico *bytecode*. É este código intermediário será transferido para a *Blockchain* na qual será finalmente executado pela Máquina Virtual do Ethereum (EVM). Neste momento de transferência do código do Contrato Inteligente, será necessário assinar o Contrato Inteligente com a chave privada que o implementou para se obter o endereço único na *Blockchain* na qual aquele Contrato Inteligente está localizado (REED, 2016, p. 28).

O código do Contrato Inteligente tem sua execução distribuída pelo imenso computador virtual estruturado e distribuído na *Blockchain*, ou seja, o código é executado de maneira distribuída por todos os nós que suportam a rede baseada em *Blockchain* subjacente, sem necessariamente depender de qualquer operador intermediário ou entidade certificadora (DE FILIPPI; WRIGHT, 2018, p. 1462).

A concepção de execução virtualizada e distribuída é uma característica de tal modo inovadora que se faz necessário um esforço de abstração para assimilar tal conceito. O processo de execução do código do Contrato Inteligente é parte do algoritmo de validação de um bloco na cadeia *Blockchain* da plataforma Ethereum, assim, se uma transação foi adicionada em determinado bloco, o código do contrato será executado no momento de sua inserção do bloco e será validada e reconhecida por toda a rede por meio do protocolo de consenso e a execução do código gerada por essa transação será executado por todos os nós, agora e no futuro, que baixam e validam aquele bloco (WALL; MALM, 2016, p. 40). Mesmo que um contrato seja removido pela função de “autodestruição” implementada em seu código, isso não significa que ele vai ser excluído assim como se apaga um arquivo em um disco rígido em um computador tradicional. No caso de um

Contrato Inteligente, o rastro de suas transações continuará armazenado na cadeia de blocos na qual ele foi executado.

Os Contratos Inteligentes concretizam, portanto, o corolário proposto pela arquitetura *Blockchain* de descentralização e imutabilidade, gerando confiança sem necessidade de intermediários, o que descortina um mundo de oportunidades para sua aplicação na prática.

2.4 BENEFÍCIOS DA APLICAÇÃO DE CONTRATOS INTELIGENTES

É muito grande o potencial dos benefícios que os Contratos Inteligentes podem proporcionar às mais variadas atividades humanas. Praticamente todas as áreas de negócio e até mesmo as relações mais usuais do cotidiano das pessoas podem ser otimizadas por meio de automação inteligente, de forma transparente e prática. (KAAL; CALCATERRA, 2017). Alguns dos benefícios, porém, merecem ainda maior destaque.

2.4.1 Aumentar eficiência e diminuir custos nas relações contratuais

As qualidades da plataforma *Blockchain*, quando implementadas na forma de Contratos Inteligentes, propiciam a criação de eficiência através da remoção de intermediários e dos custos que eles trazem para as transações. Este efeito já foi preconizado por Nick Szabo quando da sua definição do modelo conceitual de um Contrato Inteligente: “Os contratos inteligentes reduzem os custos de transação mental e computacional impostos por intermediários, terceiros ou suas ferramentas” (SZABO, 1997). Removendo a necessidade de um intermediário, há uma economia direta de custos de autenticação e certificação das transações e consequentemente redução dos custos operacionais de contratação. A eficiência inerente e a segurança da tecnologia *Blockchain* aplicada em Contratos Inteligentes é o motivo pelo qual os grandes instituições financeiras e governos estão recorrendo a eles para soluções inovadoras para eliminar processos burocráticos e com grande utilização de processos manuais. A integração dos numerosos sistemas que compõem o ecossistema financeiro utilizando tecnologias convencionais é complexa, dispendiosa e muito lenta, levando vários dias para a se efetivar a liquidação de títulos financeiros. Análises recentes indicam que os custos de infraestrutura da indústria

poderiam ser reduzidos de 15 a 20 bilhões de dólares por ano apenas no setor bancário, ao alavancar a tecnologia *Blockchain* (WALL; MALM, 2016, p. 31-32).

Também é relevante a economia indireta proporcionada pela redução dos custos de monitoramento para prevenir falhas humanas na execução manual de um contrato tradicional ou até mesmo de um eventual comportamento oportunista mal-intencionado das partes. Os contratos em suas formas tradicionais são redigidos de modo seus termos resultam em muita imprecisão. Com o uso dos Contratos Inteligentes isso pode ser melhorado em muitos casos, reduzida a necessidade de interpretação daquelas ambiguidades. Esse tipo de aplicação dos Contratos Inteligentes pode levar a reduções significativas nos custos causados pela elaboração de contratos e pela supervisão de sua execução (LAUSLAHTI, 2017, p. 13).

Por padrão, os Contratos Inteligentes possuem natureza determinística em sua autoexecução que garante que os termos do acordo serão executados exatamente como previstos no código subjacente, dispensando controles de cada parte e eliminando a necessidade de se verificar e monitorar repetidamente as obrigações incorporadas em um contrato (DE FILIPPI; WRIGHT, 2018, p. 1581).

Também são diminuídos os custos com a inadimplência dos Contratos Inteligentes, uma vez que cláusulas contratuais são incorporadas em software de forma que torne a quebra contratual mais onerosa, em alguns casos, quase que impossível, para a parte que descumprir, intencional ou acidentalmente um termo avençado. Os ganhos econômicos associados incluem a diminuição de prejuízos por fraude, custos com litigância e execução coerciva e outro tipo de custos relacionados com as transações (SZABO, 1997).

2.4.2 Gerenciamento de propriedade inteligente

A sociedade está repleta contratos que funcionam como mecanismos com o propósito de proteger a propriedade (SZABO, 1997). Muitos destes mecanismos são fracos e ineficientes. Para uma melhor eficiência de sua segurança é necessária a criação de estruturas adicionais de controle que, via de regra, são complexas e dispendiosas e continuam apresentando vulnerabilidades. Cria-se um ciclo vicioso sem fim.

Com o uso combinado de diversas tecnologias já existentes é possível desenvolver uma solução para o gerenciamento inteligente de propriedade. Todo objeto – seja um ativo originalmente em formato digital (documentos, músicas, vídeos, informações, dados de saúde, votos, ideias, etc.), seja um objeto tangível (imóveis, veículos, computadores, máquinas, etc.) – que necessite de proteção de propriedade, pode ser registrado em uma *Blockchain* ao passo que recebe um identificador único, denominado *token* (SWAN, 2015, p. 56). Este identificador único permite que sejam registradas de forma persistente na *Blockchain* as transações realizadas com aquele objeto, permitindo o seu controle, rastreamento, negociação (compra, venda, aluguel, empréstimo, etc.).

O gerenciamento das transações realizadas com estes objetos pode ser automatizado com o uso de termos e condições codificadas em um Contrato Inteligente. Os objetos podem ter "fechaduras inteligentes" que controlam o acesso conforme as regras estabelecidas contratualmente. Firmado o Contrato Inteligente, automaticamente será verificada se cada parte tem a capacidade que declara para realizar as transações com que se compromete, se os ativos em questão existem e estão disponíveis para contratação, evitando fraudes como, por exemplo, a venda de um mesmo ativo para vários compradores. O acompanhamento da execução contratual também se dará automaticamente quando da satisfação das condições combinadas no Contrato Inteligente. Havendo o inadimplemento de qualquer condição pré-estabelecida, o acesso àquele objeto fica bloqueado até que a questão se resolva.

O controle do uso também se torna muito mais eficiente. É possível criar controles extremamente minuciosos e precisos que geram micropagamentos conforme o uso daquele ativo, racionalizando o seu uso e possibilitando uma contração mais justa para ambas as partes. A possibilidade de registrar todas as transações na *Blockchain* e gerenciá-las por meio de Contratos Inteligentes, também elimina a necessidade de um ente centralizador para certificar e dar confiança àquela relação contratual.

O conceito de propriedade inteligente já é uma realidade, a tecnologia subjacente à sua implementação está disponível e já existem soluções sendo criadas e oferecidas em vários segmentos (ULRICH, 2014, p. 27).

2.4.3 Governança da Internet das Coisas

A Internet das Coisas (em inglês, *Internet of Things* ou *IoT*) é uma das mais promissoras tecnologias de informação e comunicação (TIC's) (ZHENG *et al.*, 2018, p.364). Trata-se da interconexão pela Internet de bilhões de dispositivos digitais que, por meio de sensores, estão silenciosamente coletando informações de forma massiva e ininterrupta. Um banco de dado convencional, centralizado não teria escalabilidade eficiente para transacionar tamanho volume informacional, por maior que seja sua capacidade de processamento e armazenamento. Também haveriam problemas de latência, mesmo que este sistema centralizado dispusesse das mais rápidas conexões de acesso com a Internet.

A implementação da base de dados para a Internet das Coisas se beneficiaria das características presentes na plataforma *Blockchain*, tornando mais eficiente o sistema de armazenamento e processamento por meio da uma plataforma descentralizada. Também a questão de conexões de acesso pode ser otimizada por meio da utilização da quantidade de nós distribuídos em uma rede *Blockchain* (FOTIOU; POLYZOS, 2017, p. 75-78).

Além do mais, o desafio não se limita à coleta, transmissão e armazenamento desta extraordinária massa de informações. Os dispositivos conectados na Internet das Coisas vão estabelecer entre si intensa comunicação *machine-to-machine* (HANADA; HSIAO; LEVIS, 2019, p. 1) e vão realizar microtransações para prestar serviços e informações úteis para seus usuários. Este intenso volume de transações precisa ser executado de forma confiável, segura, transparente e auditável. No caso da necessidade de monetizar os serviços prestados pelo dispositivo, um Contrato Inteligente pode cobrar microtaxas dos usuários para remunerar os prestadores dos serviços. Todas estas e outras funcionalidades são prestadas de forma determinística, transparente e garantida, controlando por meio de chaves privadas as devidas autorizações para acesso dos dispositivos entre si, conferindo autenticidade aos entes e aos dados coletados, estabelecendo relações de faturamento por meio do sistema de *tokens*, inclusive comunicando-se com outros Contratos Inteligentes dos mais diversos dispositivos conectados por meio da Internet das Coisas. Uma ressalva se faz importante a respeito do armazenamento em *Blockchain* públicas de informações sensíveis e informações sigilosas coletadas pelos dispositivos conectados à Internet das Coisas. Considerando o caráter público e transparente dos registros, a

implementação de um Contrato Inteligente deve levar isso em conta para não expor os usuários a riscos à sua privacidade (FOTIOU; POLYZOS, 2018, p. 3-4).

De todo modo, toda tecnologia apresenta vicissitudes em seus estágios iniciais, as quais são superadas por ondas aperfeiçoamento. Não será uma exceção o caso da junção dos Contratos Inteligentes aplicados no campo dos serviços prestados pela Internet das Coisas, ainda em um estágio embrionário, mas com grande potencial de transformação das relações contratuais em relações inteligentes.

2.4.4 Criação de Organizações Autônomas Decentralizadas

Os Contratos Inteligentes habitam na *Blockchain* e são executados na grande máquina virtual formada pelos nós que a compõem. Quando é acionada uma das condições que "desperta" o seu código, são executados por um dos nós, que por meio de consenso, valida as transações e executa automaticamente os termos previamente avençados em software. Neste modelo, ao invés de uma estrutura centralizada e com controle hierárquico, as pessoas interagem entre si de acordo com um protocolo especificado em software e executado na *Blockchain*, compondo uma organização descentralizada.

Este modelo decentralizado de organização pode ser estruturado de forma com que os Contratos Inteligentes possam ser interconectados uns aos outros para criar uma DAO – *Decentralized Autonomous Organization* – Organização Autônoma Decentralizada (SWAN, 2015, p. 903-904) que opera independentemente de seus desenvolvedores e que tem o condão de executar as mesmas funções que as estruturas tradicionais de organização convencional. A DAO é uma estrutura complexa inteiramente controlada por software, executado de forma autônoma e autossuficiente, pois o próprio código dos Contratos Inteligentes gerencia *tokens* com o intuito de realizar micropagamentos para remunerar e sustentar a *Blockchain* em que reside. Nenhuma pessoa ou entidade detém o poder de decisão, tudo é projetado para funcionar de forma autônoma em uma *Blockchain* (BUTERIN, 2014).

Trata-se de uma importante mudança de paradigma na qual a atividade decisória passa a ser delegada a algoritmos. A primeira vantagem suscitada é que este tipo de organização autônoma decentralizada por resolver problemas de corrupção, oportunismo e falta de transparência na organização. Por outro lado, erros acidentais ou intencionais na

programação dos Contratos Inteligentes que compõem a DAO podem ser muito prejudiciais e perigosos (DE FILIPPI; WRIGHT, 2015, p. 16-17).

Exemplos históricos de DAO's são as criptomoedas (Bitcoin, Ethereum, etc.) que operam em *Blockchain* públicas. Estas criptomoedas não são controladas por nenhuma entidade e depois que foram implementadas são autossuficientes. As regras que operam a rede são definidas por protocolos que gerenciam as operações e remuneram os nós que executam os algoritmos de consenso que validam as transações, incentivando aqueles que mais contribuem para manter a rede em funcionamento (DE FILIPPI; WRIGHT, 2018, p. 2941).

Mesmo considerando o grande potencial de automação e de independência, na prática, as DAO's ainda não são plenamente autônomas, pois dependem de pessoas que realizam a criação dos softwares que as implementam e também dependem de pessoais que mantém os nós que compõem a rede *Blockchain* incluindo os mineradores responsáveis pelos protocolos de consenso. Sem sombra de dúvida é uma tecnologia muito promissora que já apresenta frutos interessantes como no caso das criptomoedas, mas ainda é necessário superar muitos desafios para atingir sua consolidação.

2.5 DESAFIOS PARA IMPLANTAÇÃO DOS CONTRATOS INTELIGENTES

É notável o cenário auspicioso promovido pelas possibilidades imediatas e futuras proporcionadas pelos Contratos Inteligentes. Todavia, seria de certa forma ingênuo acreditar que tudo o que é digital é melhor e que funciona perfeitamente. É necessário fazer uma crítica sincera e objetiva, no sentido de enfrentar com consciência as vicissitudes desta tecnologia inovadora para que seja possível superar os obstáculos e dela tirar o melhor proveito. Se pequenas arestas podem ser aparadas para a plena implementação dos Contratos Inteligentes, alguns desafios são significativos e ensejam maior ponderação.

2.5.1 Riscos em face à confidencialidade

Os Contratos Inteligentes não são uma panaceia, pois apresentam riscos e ameaças que podem, inadvertidamente, expor informações críticas se não foram tomadas as devidas precauções (FOTIOU; POLYZOS, 2018, p. 5). Considerando-se que um Contrato

Inteligente tem sua estrutura baseada na estrutura transparente e distribuída de uma *Blockchain* e que todas as suas transações, bem como o código do contrato, são propagadas pela rede ponto-a-ponto, tornando-os publicamente visíveis aos nós da rede, este código publicado pelo autor pode ser acessado pelos participantes da rede em torno da *Blockchain* utilizada (DE FILIPPI; WRIGHT, 2018, p. 1640). Este elevado grau de transparência pode ser indesejável para as partes contratantes, que invariavelmente tem necessidade de manter sigilo dos elementos contratuais envolvidos e isto suscita uma pertinente preocupação com possível risco de perda de confidencialidade. Por mais sedutoras que sejam as outras vantagens dos Contratos Inteligentes, nem as empresas nem os indivíduos estariam particularmente interessados em publicar todas as suas informações em um banco de dados público que possa ser lido arbitrariamente sem restrições por parte do próprio governo, governos estrangeiros, membros da família, colegas de trabalho e empresas concorrentes.

Para mitigar este tipo de problema há diversas técnicas computacionais que se dispõem a proteger o código dos Contratos Inteligentes, por exemplo, considerando que um Contrato Inteligente tem as cláusulas em linguagem humanamente compreensível codificadas e compiladas em linguagem de computador, as partes do código de um Contrato Inteligente que precisa ser protegido de divulgação pública podem ser "ofuscadas" por ferramentas de criptografia gerando uma espécie de "caixa-preta" em que são gravados estes códigos sigilosos. A máquina virtual que executa os códigos dentro dos nós da cadeia *Blockchain* vai conseguir executar o as cláusulas contratuais propostas nestes trechos de códigos, porém o "significado" subjacente da informação é completamente ofuscado. A lógica interna do Contrato Inteligente é preservada, mas torna-se inviável determinar quaisquer outros detalhes sobre o conteúdo a ser preservado (BUTERIN, 2016).

2.5.2 Riscos em face à privacidade

Se a proteção do conteúdo das cláusulas contratuais se faz necessário, também é relevante considerar a privacidade das partes envolvidas. A identificação das partes envolvidas em uma relação contratual inteligente implementada em uma *Blockchain* se dá por meio de contas que vinculam estas partes entre si e aos respectivos contratos implementados em software. Para a implementação de um Contrato Inteligente são utilizados dois tipos de contas: contas de propriedade externa, controladas por chaves privadas e

atribuídas às partes contratantes e contas de contrato, controladas pelo código de contrato (ETHEREUM WHITEPAPER, 2015).

A natureza destas contas não é puramente anônima. Trata-se de contas pseudônimas, ou seja, a parte realiza o seu cadastro para entrar na rede na *Blockchain* e recebe um ID de identificação. Este ID está vinculado à identidade real daquela parte que fica oculta. Todas as transações realizadas com aquele ID ficam a ele atreladas e, como isso, é possível por meio de técnicas de rastreamento, com certa dose de sucesso, determinar estas transações por meio de cruzamento de informações que estão públicas na *Blockchain* na qual o Contrato Inteligente foi programado. Depois que a identidade de uma parte for identificada, todas as operações realizadas com a mesma conta poderão ser associadas à mesma identidade (DE FILIPPI; WRIGHT, 2018, p. 1645).

Em ordem para mitigar o problema da privacidade em Contratos Inteligentes e também o problema de confidencialidade apresentado no item anterior, os pesquisadores da Universidade de Maryland e da Cornell University propuseram uma sofisticada plataforma para desenvolvimento de Contratos Inteligentes descentralizados que não armazena as transações financeiras à vista no *Blockchain*, mantendo assim a privacidade transacional da visão do público (KOSBA *et. al*, 2016). Este sistema, denominado Hawk, possibilita que um programador, com conhecimentos moderados de linguagem de computador possa implementar um contrato utilizando todos os notáveis recursos de transparência e descentralização da arquitetura *Blockchain* ao mesmo tempo que mantendo a confidencialidade do contrato e a privacidade das partes contratantes. O compilador do Hawk decompõe o Contrato Inteligente original em dois subcontratos vinculados entre si. O primeiro deles contém as informações sigilosas que se pretende manter preservadas das vistas do público, tais como identidades e valores, e as encapsula em uma camada criptografada adicional antes de enviá-las para um bloco na cadeia da *Blockchain*. O segundo subcontrato, que contém as regras de negócio que pode se tornar públicas sem prejuízo, é separado para ser enviado diretamente para ser processado na *Blockchain*. (JUELS *et al*, 2016, p. 1).

De todo modo, para se preservar a privacidade de um Contrato Inteligente na arquitetura *Blockchain* é certo que haverá algum prejuízo à transparência e também "custos" em face às camadas de processamento adicionais para implementar soluções parciais,

heurísticas e mecanismos criados para levar a privacidade a classes específicas de aplicativos (BUTERIN, 2016).

2.5.3 Problemas estruturais de tecnologia

A dependência dos Contratos Inteligentes à tecnologia *Blockchain* resulta em profundo relacionamento entre estas tecnologias. Todos pontos fracos presentes na tecnologia *Blockchain* suscitam ameaças diretas os Contratos Inteligentes. Além da vulnerabilidade do ataque de 51% descrita no capítulo 1 deste trabalho, existem outros riscos estruturais que estão se desenvolvendo ao longo da adoção destas tecnologias.

Originalmente o conceito proposto por Satoshi Nakamoto no manifesto que propôs a criação do Bitcoin, primeira aplicação prática da tecnologia *Blockchain*, carregava o ideal de que a *Blockchain* seria mantida por uma comunidade descentralizada que se autorregularia por meio de consenso obtido de forma igualitária e democrática, cada qual contribuindo com sua capacidade computacional (NAKAMOTO, 2008, p. 8). Porém, na prática nota-se há uma tendência de concentração dos nós mineradores que produzem o consenso para validar novos blocos na cadeia *Blockchain*. Ao invés de cada um dos participantes de uma *Blockchain* participarem com seus próprios computadores para se obter o consenso necessário para validação de um bloco, a maioria dos deles não realiza a validação de blocos localmente; em vez disso, eles contam com um centro de mineração centralizado (*pool*) para fornecer os cabeçalhos de bloco. Estes centros de mineração possuem equipamentos especializados chamados ASIC (*Application-Specific Integrated Circuit* – Circuito Integrado de Aplicação Específica) foram projetados com a função única de minerar blocos na *Blockchain* obtendo expressivos lucros quando vencem a competição com outros mineradores e recebem as taxas por seus serviços. Isso significa que a mineração não é mais uma atividade altamente descentralizada e igualitária, pois exige significativo investimento para se participar de forma efetiva. Esta concorrência é insuportável para os usuários finais com seus computadores pessoais, mesmo que equipados com sofisticados e caros processadores de última geração. Disso tudo resulta que a concentração dos nós em uma *Blockchain* fica comprometida (ETHEREUM WHITEPAPER, 2015).

Outra preocupação que concerne com a estrutura *Blockchain* que sustenta os Contratos Inteligentes é a centralização dos fornecedores que oferecem infraestrutura para aquela plataforma. O ideal revolucionário de se criar uma rede independente de governos e corporações na qual as pessoas encontrassem liberdade para se relacionar livremente e de forma consensual (MAY, 1988) pode estar em risco em face à concentração da estrutura sob domínio de grande corporações como Amazon, Microsoft e IBM que estão oferecendo serviços completos para a implementação de estruturas *Blockchain-as-a-Service* (Baas) na nuvem e também oferecendo plataformas proprietárias para construção de Contratos Inteligentes (ZHENG *et al.*, 2018, p.363).

A crescente adoção de Contratos Inteligentes para as mais variadas formas de negócios está gerando um efeito colateral: o crescimento exponencial da do tamanho das *Blockchain*s. Este crescimento do tamanho da cadeia de blocos causa um expressivo risco de que participantes com capacidade computacional muito modesta e conexões à Internet mais lentas, não consigam copiar, em tempo hábil, a *Blockchain* inteira da Internet para seus computadores pessoais. Este cenário provável ocasionaria que apenas um número muito pequeno de grandes empresas executaria nós completos. Os desenvolvedores da plataforma Ethereum, prevendo este panorama, projetaram uma funcionalidade é possível copiar da Internet somente uma porção com últimos blocos da *Blockchain* para processando e validação (ETHEREUM WHITEPAPER, 2015).

2.5.4 Falta de flexibilidade para formalização de obrigações

Os Contratos Inteligentes são implementados em uma lógica formal muito estrita utilizando linguagem de computador com condicionais do tipo IF-THEN-ELSE (“se isso, então aquilo... senão, aquilo outro”). Esta característica inerente da lógica de programação é muito útil em situações objetivas e determinísticas nas quais o fluxo decisório é minimamente previsível, o que não necessariamente ocorre em todos os casos das relações contratuais, frequentemente permeado por situações em que as cláusulas são vagas ou abertas. Muitas vezes, as partes não têm tempo disponível nem recursos para discernir todas as possibilidades de eventos futuros, outras tantas vezes nem é possível fazer esta previsão no momento da celebração de um contrato. Para uma maior aderência da tecnologia dos Contratos Inteligentes à realidade contratual do mundo real será necessário que seja possível programar decisões substantivas sobre o significado, o conteúdo e a

aplicabilidade dos acordos das partes contratantes. Os desenvolvedores não teriam condições de resolver, somente com técnicas de programação, julgamentos subjetivos, interpretações e decisões substantivas sobre eventos futuros potencialmente incertos ao redigir o código do Contrato Inteligente (DE FILIPPI; WRIGHT, 2018, p. 1658).

Quiçá a utilização de sistemas dotados com Inteligência Artificial possa ser uma alternativa para implementar soluções neste contexto. Porém, em seu estágio atual, os Contratos Inteligentes, ao contrário do que seu nome pode sugerir, não estão sendo desenvolvido com utilização de inteligência artificial. Todavia, não se pode desprezar a contribuição da Inteligência Artificial combinada com a lógica dos Contratos Inteligentes em um futuro muito próximo, considerando a extraordinária velocidade da evolução tecnológica. Pode-se presumir, então, que os computadores dotados de algoritmos com inteligência artificial preditiva que possam pensar e decidir venham revolucionar novamente o modelo de contratos, trazendo mais flexibilidade e previsibilidade de cláusulas que humanamente não se podem predizer (LAUSLAHTI *et al*., 2017, p. 3).

2.5.5 Dificuldades dos operadores de Direito em face à interpretação jurisdicional

Na medida em que os Contratos Inteligentes forem ganhando escala de utilização, mesmo que sejam aperfeiçoadas as interfaces de utilização pelas pessoas, a premissa básica por trás desta tecnologia continua sendo enfatizada na automação por meio de linguagem de programação e não na interação humana. A codificação dos Contratos Inteligentes não é destinada para ser inteligível por um observador humano. Ela é destinada à interpretação por computadores em uma rede de nós que compõem a *Blockchain*. Neste contexto, o significado e o raciocínio lógico da linguagem codificada é substancialmente diferente da linguagem humana. Esta característica intrínseca dos Contratos Inteligentes pode resultar em dificuldades jurisdicionais e “os tribunais podem não ser capazes de levantar a hipótese de uma interpretação razoável de um Contrato Inteligente”. (KAAL; CALCATERRA, 2016, p. 8).

A granularidade dos agentes autônomos em uma rede *Blockchain* que operam por meio de transações criptografada cria obstáculos praticamente intransponíveis para a atuação das jurisdições convencionais. Em caso de problemas na execução do código que implementa um Contrato Inteligente, pode ser imperioso determinar a responsabilidade e

eventual reparação de danos. A determinação da responsabilidade tornar-se-ia uma tarefa hercúlea em face a natureza distribuída e decentralizada e a complexidade das ferramentas utilizadas para implementação dos Contratos Inteligentes. Considerando que estes são implementados em uma tecnologia globalmente distribuída e, por essência, decentralizada, torna-se impraticável a determinação de limites para a contratação de partes localizadas em diferentes jurisdições. Também os ativos transacionados podem estar distribuídos em qualquer localização (LAUSLAHTI et al., 2017, p. 6).

A natureza autônoma dos Contratos Inteligentes e a capacidade das partes operarem de forma pseudônomica, praticamente anônima, também cria complicações para a interpretação jurisdicional e a atribuição de responsabilidades legais. Uma parte, ao celebrar um Contrato Inteligente pode estar contratando com outra parte sem conhecer sua identidade real, sem respaldo de uma entidade oficialmente conhecida e que pode estar fora de sua jurisdição (WALL; MALM, 2016, p. 38). Até mesmo para ingressar com uma ação judicial, a parte lesada por ter grandes dificuldades para saber a identidade da parte contrária para atender aos requisitos de serviço. Neste contexto, um julgamento padrão teria efeito prático limitado, a menos que a identidade da outra parte em um Contrato Inteligente pudesse de alguma forma ser estabelecida (DE FILIPPI; WRIGHT, 2018, p. 1690). No entanto, para implementar esse tipo de controle, o protocolo da tecnologia *Blockchain* deve facilitar a identificação das partes, o que resulta em um desvio de seu ideal precípuo (WALL; MALM, 2016, p. 38).

Além das questões tradicionais de interpretação da intenção das partes em um eventual litígio contratual, os operadores do Direito irão se deparar com imbricadas questões envolvendo complexas tecnologias o que demanda a necessidade de habilidades técnicas e capacidade de analisar o caráter legal e ao mesmo tempo tecnológico dos Contratos Inteligentes (LAUSLAHTI et al., 2017, p. 2). Decididamente, os operadores do Direito vão necessitar de apoio de peritos em computação para interpretar a linguagem codificada de um Contrato Inteligente em questão em um determinado caso.

2.5.6 Criação de uma plataforma em prol de atividades ilegais

Os benefícios proporcionados pelos Contratos Inteligentes e as tecnologias subjacentes que os implementam podem ser ter aplicação desvirtuada e podem contribuir

para atividades imorais, ilícitas e até mesmo criminosas. Assim como as criptomoedas já foram utilizadas para sustentar atividades ilegais (GDPO, 2013, p. 2), também os Contratos Inteligentes podem ser utilizados para implementar arranjos econômicos ilegais apoiados em criptografia e na natureza decentralizada e sem intermediários oficiais da *Blockchain*, procurando funcionar de forma invisível aos olhos da jurisdição tradicional, evadindo-se intencionalmente da aplicação das leis e regulamentações existentes.

São muitos os exemplos de atividades ilegais que podem se beneficiar da tecnologia que implementa os Contratos Inteligentes. Poderia ser criado um sistema que permitisse a negociação de mercadorias proibidas em uma determinada jurisdição ou poderia ser criado sistemas para apoias apostas não autorizadas ou jogos de azar em jurisdições nas quais não são permitidos, sem depender de entes centralizados que poderiam ser encontrados e interditados. Por não haver um intermediário centralizado encarregado de manter o sistema, nenhuma parte pode encerrar o serviço (DE FILIPPI; WRIGHT, 2018, p. 1733).

Pesquisadores da Universidade de Cornell e da Universidade de Maryland descreveram em um artigo como a tecnologia da *Blockchain* e dos Contratos Inteligentes poderia ser usada para facilitar também crimes mais complexos, como o assassinato, tráfico de drogas e terrorismo. Em seu artigo, apresentaram um exemplo hipotético de como um Contrato Inteligente poderia se utilizar para contratar um assassino e combinar os detalhes da encomenda, transferindo o pagamento do "serviço" para uma conta de alguma criptomoeda na qual o valor combinado ficaria bloqueado até que um "oráculo" confiável do mundo real (um jornal de grande circulação, por exemplo) confirmasse a notícia da morte da vítima. Quando esta condição fosse satisfeita, o pagamento seria liberado na conta do criminoso. Com o Contrato Inteligente gerenciando todas as etapas deste hediondo negócio, nenhuma das partes precisaria se identificar, os envolvidos no apoio e execução do crime não precisariam se comunicar uns com os outros para se realizar a prática criminosa e o pagamento seria realizado de forma segura mediante confirmação do assassinato de acordo com as condições pré-definidas (JUELS *et. al.* 2016, p. 283).

Toda e qualquer tecnologia pode ser utilizada para fins impróprios. Os Contratos Inteligentes não seriam uma exceção. Porém, esta generalização não pode ser ignorada

em face ao grande potencial de alcance e exponencialização dos resultados desta tecnologia, seja para o bem, seja para o mal.

2.6 ALGUMAS CONSIDERAÇÕES AO FINAL DO CAPÍTULO 2

Os Contratos Inteligentes são uma realidade já disponível para aperfeiçoar as relações contratuais oferecendo uma importante gama de serviços de descentralização, confiança e autoexecução, inclusive com a possibilidade de substituir, de certo modo, a atividade decisória humana (GOMES, 2018, p. 54). Todavia resta evidente a necessidade de várias adequações técnicas e estruturais para que os Contratos Inteligentes se tornem uma realidade a ser adotada universalmente. Considerando que a Tecnologia da Informação e da Comunicação avança sempre a passos rápidos e que há intensa pesquisa acadêmica e científica desenvolvendo e aperfeiçoando os protocolos existentes e, ao mesmo passo, constantemente criando inovações tecnológicas, pode-se prognosticar que é uma questão de tempo para que os problemas técnicos sejam ultrapassados.

Por outro lado, as questões jurisdicionais necessitam de especial atenção e dedicação para serem superadas, visto que é imprescindível a devida segurança jurídica para abarcar os impactos causados pelos Contratos Sociais na sociedade (KAAL; CALCATERRA, 2016, p. 13). Não basta acenar com promessas redução de gastos, mais eficiência ou novos serviços, para que os Contratos Inteligentes ganhem maior adesão e se popularizem de forma consistente é necessário que se assegure às partes que celebrarem um Contrato Inteligente a garantia de que nenhum dos seus direitos legais será sacrificado e que seus negócios estejam a salvo de riscos como exposição indevida, instabilidade tecnológica, falta de clareza e ausência de mecanismos de governança e resolução de conflitos para resolver eventuais lides.

É necessário, portanto, que existam e estejam disponíveis meios jurisdicionais para resolução de conflitos que sejam aplicáveis às transações criptográficas da *Blockchain* e que possam lidar com as características da autoexecução, imutabilidade e descentralização dos Contratos Inteligentes. Sem estes meios, por mais sedutora que seja a tecnologia, a confiança nela estaria minada e sua expansão estaria comprometida. O próximo capítulo tem o objetivo de ponderar sobre estes tópicos, apresentando possíveis soluções para tais desafios.

3 REGULAMENTAÇÃO DOS CONTRATOS INTELIGENTES

Os contratos, de acordo com Szabo (1997, p. 3), são o alicerce básico da economia constituindo-se na principal forma de formalizar as relações entre duas ou mais pessoas, momento por ele denominado de “encontro entre mentes”. Em sua forma tradicional, os contratos geram efeitos na sociedade, os quais precisam de tutela do Direito para que ocorram com segurança jurídica, um dos pilares para o desenvolvimento da sociedade. Com os Contratos Inteligentes não é diferente. Sem segurança jurídica que confirme sua validade, não há nem de se cogitar sua utilidade prática. “Embora possa haver muitas barreiras à adoção de contratos inteligentes, a incerteza jurídica não precisa ser uma delas” (RASKIN, 2017, p. 340).

Os Contratos Inteligentes codificam as relações existentes no plano dos negócios por meio de algoritmos implementados na cadeia de blocos *Blockchain*, utilizando avançadas tecnologias de comunicação por meio de redes ponto-a-ponto (P2P) levando a completa desnecessidade de um agente centralizador, ao mesmo tempo que promovem confiança, mesmo entre partes desconhecidas, por meio de avançados algoritmos de criptografia implementados em complexos protocolos computacionais, aperfeiçoando as relações contratuais, promovendo eficiência, economia e confiança e proporcionando funcionalidades inéditas, tais como: descentralização, imutabilidade e autoexecução.

Este fenômeno resulta na possibilidade de uma significativa mudança na forma pela qual as pessoas interagem entre si, realizando negócios e, enfim, estabelecendo relações jurídicas, em particular celebrando contratos. Torna-se relevante, portanto, avaliar se o presente arcabouço jurídico do ordenamento brasileiro tutela o fenômeno dos Contratos Inteligentes ou se é necessário instituir novas construções jurídicas para tal propósito. Deste modo, este capítulo apresenta um estudo dos Contratos Inteligentes definindo sua natureza legal, seus efeitos dentro no plano do Direito e suas relações com outros componentes no plano normativo.

Em um primeiro momento importa esclarecer se os Contratos Inteligentes constituem uma nova forma de negócio jurídico ou se é possível abarcar sua tutela dentro das formas existentes, sendo eles tão-somente uma nova forma de se estabelecer relações contratuais. A finalidade da definição conceitual dos Contratos Inteligentes tem notável

relevância para que seja possível enquadrar suas semelhanças e diferenças com os contratos convencionais, facilitando o seu estudo teórico e, também, abordando suas consequências jurídicas na prática (VIANA, 2008, p. 47). Um segundo passo proposto no presente estudo jurídico dos Contratos Inteligentes é o trabalho de classificação dentro das possíveis espécies de contratação. Partindo da definição conceitual obtida na etapa anterior, foi utilizada a classificação estabelecida por Manoel Joaquim Pereira dos Santos e Mariza Delapieve Rossi, na qual os autores relacionam o emprego das TIC's na formação e execução de contratos (SANTOS, ROSSI, 2000). Por fim, foi realizada uma análise da interface dos Contratos Inteligentes com as normas jurídicas com enfoque no ordenamento brasileiro, buscando apenas quando necessário alguns institutos de outros ordenamentos para efeito de comparação. Nesta fase da pesquisa foram utilizados alguns exemplos emblemáticos da utilização dos Contratos Inteligentes com o intuito de dar mais concretude ao seu estudo em relação aos componentes do plano normativo.

A partir do estabelecimento deste caminho, foi possível buscar conhecimento sobre como os Contratos Inteligentes são recepcionados pela estrutura jurídica posta pelo sistema jurídico brasileiro.

3.1 DEFINIÇÃO DA NATUREZA JURÍDICA DOS CONTRATOS INTELIGENTES

No ordenamento brasileiro, as discussões sobre contratos formados por meio de aparatos tecnológicos já estavam presentes no Código Civil de 1916 o qual considerava, de forma expressa em seu artigo 1.081, inciso I, que os contratos também poderiam ser celebrados por meio de telefone, sendo que, mesmo nesse caso, tratar-se-ia de contrato firmado entre presentes (BRASIL, 1916). Com o avanço da tecnologia da informação, já na década de 70, os computadores passaram a desempenhar papel fundamental no mundo empresarial. Todavia, foi com a disseminação da Internet que as relações negociais tiveram um exuberante crescimento por meio do comércio eletrônico atingindo todos os públicos, desde as relações entre empresas (B2B – *Business to Business*) até mesmo as relações entre empresas e seus clientes (B2C – *Business to Consumer*) e, ainda, as relações diretas entre consumidores (C2C – *Consumer to Consumer*). Consequência disso, a formação de contratos percebeu notável transformação por meio dos contratos celebrados em *sites* das empresas com seus clientes na Internet.

Também os doutrinadores começaram a expandir discussões acerca do uso de tecnologia em prol das relações contratuais. É interessante destacar algumas das várias denominações que foram sendo empregadas conforme o contexto do estudo aplicado, tais como: contratos virtuais, contratos telemáticos, contratos pela Internet, contratos via Internet, contratação na Internet, contratos eletrônicos. Esta última denominação foi aquela que ganhou maior relevância nos usos e costumes internacionais e também sendo a designação mais frequente recepcionada pelos projetos de lei brasileiros sobre comércio eletrônico em vigência ou em trâmite no Congresso Nacional.

Uma das premissas para um contrato ser considerado contrato eletrônico é que o consentimento que se conclui com a aceitação da proposta ocorra por meio eletrônico, como, por exemplo, por computador, equipamento similar ou simplesmente pelo "ACEITO" ou "CONCORDO" via telefone; e que podem ser firmados por senha ou por meio de assinatura eletrônica (REBOUÇAS, 2015, p. 279). É o caso dos Contratos Inteligentes que implementam uma nova forma de realizar as tradicionais relações negociais por meio da *Blockchain*, nos quais são celebrados por meio eletrônico no momento em que acontece a manifestação da vontade dos contraentes quando da celebração do contrato e firmados por meio de sua assinatura eletrônica quando do uso das chaves público e privadas, assim sendo, os Contratos Inteligentes podem ser considerados uma variedade de contrato eletrônico.

De tal modo, em que pese os Contratos Inteligentes possibilitem recursos extraordinários tais como autoexecução, descentralização e inviolabilidade, não são necessariamente uma nova categoria contratual. Por fim, pode-se inferir que os Contratos Inteligentes se encontram sob o mesmo entendimento e podem ser analisados como uma nova forma de contratar que herda todas as propriedades dos contratos eletrônicos.

3.1.1 Em busca de uma classificação para os Contratos Inteligentes

A Tecnologia da Informação e da Comunicação (TIC) possibilita um número sem limites de formas de se estabelecer relações contratuais. E a cada momento surgem novas formas, frutos da criatividade humana em estabelecer arranjos aplicando combinações entre novas invenções e novos modos do uso destas tecnologias, que resultam em múltiplos tipos de contratos implementados por meio de aparatos tecnológicos. Neste

cenário, em constante evolução, torna-se útil estabelecer uma classificação que facilite a interpretação e a compreensão dos contratos e suas relações com a tecnologia para promover um estudo dos efeitos e implicações jurídicas nestes contextos.

Uma das formas de classificação frequentemente utilizada é aquela que leva em conta o grau de interação entre as partes contratantes e os meios eletrônicos e, a partir de uma análise ampla, classifica os contratos em três categorias: interpessoais, interativos e intersistêmicos (SANTOS; ROSSI, 2000, p. 106). Ao passo que se considera que os Contratos Inteligentes podem ser classificados como uma forma avançada de contratos eletrônicos, é perfeitamente possível buscar dentro da classificação apresentada, em que categoria eles podem ser qualificados.

3.1.1.1 Contratos Interpessoais

As contratações eletrônicas interpessoais são aquelas que requerem uma maior intervenção humana com os meios eletrônicos para a realização da manifestação da vontade contratual tanto no momento da proposta quanto no momento da aceitação, cada qual a seu turno – simultaneamente ou não, e também na execução do contrato. Exemplo típico é a realização da comunicação dos atos de contratação por meio de tecnologias como o serviço de e-mail e outras ferramentas similares, tais como salas de conferência na Internet, comunicadores instantâneos, etc. Também os serviços de comunicação mais contemporâneos oferecidos pelas redes sociais podem ser considerados ferramentas disponíveis para a formação de contratos eletrônicos interpessoais.

A natureza informal das relações interpessoais, mesmo quando realizadas por meio eletrônico, torna este tipo de contratação mais rápida e de maior acesso a qualquer pessoa que tenha acesso a equipamentos como, por exemplo, computadores e *smartphones*. Por outro lado, a mesma informalidade que facilita o acesso também proporciona fragilidade para comprovação das obrigações assumidas mutuamente pelos contratantes, sendo que é necessário todo o cuidado com a documentação das trocas de mensagens e, em casos de litígios, para que as provas tenham valor processual, é necessário recorrer às atas notariais para atestar a veracidade dos fatos promovidos.

3.1.1.2 Contratos Interativos

As contratações interativas são aquelas nas quais um contratante, pessoa natural, interage com um software, por meio de uma interface interativa, que disponibiliza uma aplicação para que aquela pessoa possa, por exemplo, escolher itens de compra desejados, preencher formulários de dados pessoais, e, especialmente, indicar sua aceitação aos termos de fornecimento e escolher e autorizar formas de pagamento. Em termos jurídicos, no momento em que esta interface disponibiliza uma "vitrine *online*" exibindo produtos, informações comerciais, preços, forma de pagamento e outras informações comerciais, conforme o artigo 429 do Código Civil (BRASIL, 2002), caracteriza-se uma oferta em termos contratuais. O momento em que o ofertante manifesta sua vontade é aquele em se realiza a disponibilização da "vitrine *online*" em um *site* da Internet, por exemplo, sustentado por toda a infraestrutura tecnológica subjacente. Por seu turno, a manifestação da vontade do adquirente se consuma no momento em que este toma ciência de todos os detalhes exibidos da proposta visível no *site* de Internet, preenche os formulários formalizando suas escolhas e utiliza o meio eletrônico disponível para indicar sua aceitação, como por exemplo clicando com o *mouse* ou tocando em uma tela para preencher em um campo específico para tal fim. Neste momento consuma-se a celebração do contrato.

Os contratos eletrônicos interativos são muito utilizados no comércio eletrônico (*e-commerce*) realizado por meios de *sites* na Internet. A natureza da relação de comunicação estabelecida entre o internauta, usuário que navega pelas páginas da Internet, e os sites de lojas virtuais resulta em uma relação muito prática, porém sem muita flexibilidade para o contratante que deseja adquirir um produto ou serviço. Normalmente, não há negociação com alguma pessoa natural representante do ofertante, visto que a interação acontece por meio da interface que já contém as regras de negócio previamente programadas e cláusulas unilateralmente preestabelecidas pela parte ofertante sem a possibilidade de discussão ou alteração pela parte adquirente. Esses contratos equiparam-se aos contratos por adesão, pois, se o adquirente não concorda com as cláusulas impostas, não há como negocia-las no sentido de serem adequadas às suas necessidades (LAWAND, 2003, p. 103).

3.1.1.3 Contratos Intersistêmicos

Nas relações estabelecidas por meio de contratos eletrônicos intersistêmicos é ausente a interação humana. As cláusulas contratuais são previamente acordadas entre as partes e depois codificadas em linguagem de máquina criando componentes de software que serão executados nos sistemas computacionais interconectados pelas redes das partes envolvidas. Via de regra, a estrutura tecnológica envolvida é mais sofisticada e envolve o intercâmbio de informações entre sistemas empresariais.

Destacam-se como exemplos de contratos eletrônicos intersistêmicos os padrões de envio e recebimento de informações eletrônicas padronizadas conhecido como *Electronic Data Interchange* – EDI, em tradução livre, Intercâmbio Eletrônico de Dados. Por meio destes padrões, definidos em conjunto por entidades privadas, governamentais e não governamentais, em nível internacional, pode-se criar formatos compreensíveis por sistemas distintos para troca de informações tais como pedidos de cotação, tabelas de preços, ordens de fornecimento, faturas, ordens de pagamento, de transporte e outros. A troca destas informações possibilita que módulos de software possam acessar determinados dados e testar condições para ativar gatilhos programados que irã executar ações previamente acordadas. Os contratos intersistêmicos no início eram restritos a corporações que podiam arcar com os custos de infraestrutura própria de comunicação. Com o advento da Internet no Brasil, em meados dos anos 1990, este tipo de contratação passou a ser oferecida também para empresas de médio e pequeno porte, popularizando este recurso que agiliza a contratação e reduz os custos operacionais.

Um exemplo clássico são os sistemas de empresas que são controlados por softwares de gestão que se integram com os estoques dos fornecedores e, quando o nível de estoque de determinado componente atingir um número mínimo em estoque, o sistema desta empresa automaticamente envia um pedido para o sistema do fornecedor, gerando uma fatura que será enviada para cobrança na empresa origem do pedido. Todos estes e outros passos da cadeia de fornecimento são automatizados e são executados conforme são satisfeitas as condições pré-programadas, sem a interação humana (LEAL, 2004, p. 82).

Enfim, realizadas as considerações sobre os tipos de contratos eletrônicos interpessoais, interativos e intersistêmicos, resta ponderar sobre em qual destas categorias

pode-se albergar os Contratos Inteligentes. Levando em conta que os Contratos Inteligentes são programados para serem executados automaticamente na *Blockchain* quando as condições programadas forem satisfeitas, não resta dúvida de que eles se encaixam na categoria dos contratos eletrônicos intersistêmicos com a notável diferença de que agora podem ser implementados não somente por empresas, mas por qualquer pessoa, física ou jurídica, que possa criar uma conta em uma *Blockchain* e se proponha a implementá-los. Por tal importância deste fato, neste trabalho serão pormenorizados, mais adiante, os efeitos da autoexecução dos Contratos Inteligentes e seus impactos jurídicos.

3.1.2 Equivalência funcional e jurídica dos Contratos Inteligentes

A importância da convicção de que os Contratos Inteligentes podem ser tratados como contratos, uma espécie do gênero dos negócios jurídicos, sem necessidade de criação de uma nova categoria faz entender que toda a base principiológica que cabe aos contratos em geral, também se aplica aos Contratos Inteligentes.

A análise de todas as teorias e princípios aplicáveis ao direito contratual seria repetitiva e extrapolaria o objeto do presente trabalho. Porém, o princípio da equivalência funcional dos contratos tem grande relevância, merece ser destacado e analisado com especial atenção devido à sua importância para a aceitação dos contratos eletrônicos e, por conseguinte, dos Contratos Inteligentes.

O princípio da equivalência funcional dos contratos dispõe sobre a garantia de que os contratos realizados em meio eletrônico devem ter os mesmos efeitos jurídicos dos contratos estabelecidos por verbalmente ou por meio escrito (LEAL, 2004, p. 83). Da mesma forma corrobora Fábio Ulhôa Coelho (2007, p. 39) ao explicar que “registro em meio magnético cumpre as mesmas funções do papel. Assim as certezas e incertezas que podem exsurgir do contrato e não são diferentes das do contrato”.

A história da origem deste princípio remonta a impressionante expansão do comércio eletrônico pela Internet em meados de 1990. Este fenômeno tornou-se tão relevante que em 1996 surgiu a Lei Modelo sobre Comércio Eletrônico da UNCITRAL (*United Nations Commission on Internet Trade Law*) (UNCITRAL, 1996). Esta lei apresenta em seu artigo 11 preceito importante sobre a formação e a validade dos contratos que dispõe que na formação de um contrato, tanto a oferta quanto a aceitação, podem ser

expressas por mensagens eletrônicas, salvo exista disposição em contrário. O mesmo artigo também assevera que não serão negadas nem validade nem eficácia a um contrato pela simples razão de utilização de mensagens eletrônicas para sua formação.

Este preceito legal fortalece a validade das relações contratuais estabelecidas quando o meio eletrônico é utilizando. Desde a celebração do contrato por meio da aceitação da proposto até os atos realizados pelas partes no cumprimento de suas obrigações contratuais, há um pleno reconhecimento e equiparação funcional dos contratos eletrônicos aos que são celebrados por outros meios não vedados pela lei.

Mesmo considerando que esta Lei Modelo da UNCITRAL (1996) não pretenda invadir o espaço legislativo soberano de cada país, ela traz notável inspiração para que legislações locais que regulam as relações eletrônicas no âmbito comercial e tem levado muitos países, entre eles o Brasil, a iniciar uma atividade legislativa especificamente direcionada a normatizar as novas situações e circunstâncias jurídicas decorrentes do uso dos meios eletrônicos (GARCIA, 2004).

Em que pese no Brasil não há uma regulamentação específica sobre contratos eletrônicos, a promulgação do Decreto n.º 7962/2013 pela presidente Dilma Rousseff, regulamentou o Código de Defesa do Consumidor no que tange ao comércio eletrônico (BRASIL, 2013), trazendo alusões expressas sobre a contratação por meio de sítios eletrônicos, ou seja, sites da Internet, com o objetivo de assegurar a proteção ao consumidor. Estas referências indicam de maneira clara que os contratos eletrônicos são reconhecidamente uma forma válida e legalmente admitida de se estabelecer relações contratuais.

Mesmo considerando que este decreto se refere à esfera consumerista, já é possível considerar que no ordenamento brasileiro, pelo princípio da equivalência funcional, não há nada que obste que os contratos eletrônicos sejam reconhecido como forma válida de contratação, pois se assim não fosse, não poderiam ser regulamentos tampouco para as relações contratuais entre fornecedores e consumidores pela Internet. No mesmo sentido, não se encontra no ordenamento brasileiro norma que venha a coibir a realização de contratos por meio eletrônico, sendo a única exceção quando a legislação prevê outras formas solenes para que o ato jurídico venha a se revestir de efeitos jurídico pertinentes. Também corroborando esta afirmação, Maria Helena Diniz destaca que não há no Código

Civil vedação legal à formação de contratos eletrônicos, salvo nas hipóteses legais em que se requer forma solene para validade e eficácia negocial (DINIZ, 2002, p. 656).

Finalmente, levando em conta que se os contratos eletrônicos são recepcionados como forma válida de contratação no ordenamento brasileiro, também o seriam os Contratos Inteligentes, pois estes são uma evolução tecnológica daqueles. Entretanto, para evitar conclusões antecipadas, torna-se valioso realizar uma meticulosa análise dos Contratos Inteligentes à luz de importante doutrina que trata dos pressupostos fáticos dos planos da existência, validade e eficácia do Negócio Jurídico, também conhecida como Tricotomia do Negócio Jurídico ou ainda como "Escada Ponteana" em homenagem à Pontes de Miranda, notável jurista brasileiro.

3.1.3 Os Contratos Inteligentes em face à Tricotomia do Negócio Jurídico

Em essência, um Contrato Inteligente é "um conjunto de promessas, especificadas em formato digital, incluindo protocolos dentro dos quais as partes realizam essas promessas" (SZABO, 1997). Destacando-se a primeira parte, referente ao contrato em si, à luz do ensinamento de Maria Helena Diniz que afirma que o contrato "constitui uma espécie de negócio jurídico de natureza bilateral ou plurilateral, dependendo, para a sua formação, do encontro da vontade das partes" (DINIZ, 2008, p. 13) é possível determinar que o Contrato Inteligente pode ser visto como uma forma de contrato juridicamente constituída e, por sua vez, também trata-se de um negócio jurídico, em sentido estrito, bilateral ou plurilateral.

O que sucede é que, no caso particular dos Contratos Inteligentes, é que o negócio jurídico em questão será realizado por meio da codificação de suas cláusulas em linguagem de computador a ser executada em determinada estrutura *Blockchain* que, por sua natureza, proporciona recursos extraordinários como, por exemplo, rastreamento dos objetos envolvidos no contrato, bloqueio dos mesmos até que determinada condição seja satisfeita, garantia dos atos das partes por meio de autenticação criptográfica, eliminação de intermediários e muitos outros tantos benefícios. Sob outra perspectiva, para o melhor aproveitamento dos benefícios dos Contratos Inteligentes, torna-se imprescindível assegurar a segurança jurídica em todo o contexto de sua implementação, ao mesmo que é importante demonstrar se esta nova forma de contratação está em conformidade com o

ordenamento jurídico brasileiro. Neste intuito, propõe-se uma apreciação que examine se os Contratos Inteligentes estão em concordância com o estudo da Tricotomia do Negócio Jurídico, teoria presente dentro do estudo dos negócios jurídicos (AZEVEDO, 2002, p. 23). Também conhecida como "Escada Ponteana" em homenagem ao ilustre jurista Pontes de Miranda, esta teoria propõe uma análise em três planos distintos, a saber, plano da existência, plano da validade e plano da eficácia. Nestes planos verificar-se-á se os negócios jurídicos em questão apresentam os requisitos jurídicos mínimos de existência, possuem aptidão legal para produzir efeitos jurídicos válidos e eficazes.

3.1.3.1 Plano da Existência

Antes de se cogitar a validade ou a eficácia de um negócio jurídico, é necessário confirmar a sua existência, verificando se há presença de todos os elementos que a comprovam. Neste plano verifica-se a presença dos pressupostos fáticos para um negócio jurídico, seus elementos mínimos e essenciais: agente, vontade, objeto e forma (TARTUCE, 2018, p. 13). No plano da existência não se cogita da invalidade ou eficácia do fato jurídico, importa, apenas, a realidade da existência. Tudo, aqui, fica circunscrito a saber se o suporte fático suficiente se compôs, dando ensejo à incidência. A caracterização da existência do negócio jurídico também não depende dos questionamentos sobre sua validade ou eficácia, são apenas analisados os componentes fáticos de realidade da existência do fato jurídico (REBOUÇAS, 2015, p. 1235).

A presença do elemento agente apresenta certa obviedade e um relacionamento íntimo com a expressão da vontade. Pela definição de negócio jurídico, este só existe quando houver a presença de um agente, pessoa física ou jurídica, que venha a realizar um ato jurídico que gere efeitos em que se expresse sua vontade. Para a manifestação de uma vontade, é necessária a existência de um agente, por conseguinte, não há de se falar de vontade sem se falar de agente, que manifesta essa vontade. De outro lado, a presença de um agente inerte que não expressa sua vontade, deixa ausente este segundo elemento e não traz à existência o negócio jurídico.

Nos Contratos Inteligentes também é indispensável que se comprove a existência do sujeito e sua vontade. Mesmo considerando que alguns Contratos Inteligentes podem ser implementados "robôs" que existem de forma autônoma por software, estes autômatos seriam instrumentos das partes que os programaram, pessoalmente ou por encomenda, e

neste ato já manifestam sua vontade de contratar. Além do mais, a relação dos atos jurídicos com seus autores sempre pode vir a ser comprovada por meio das assinaturas com chaves privadas realizada pelo agente que realiza aquela transação, sendo possível associá-la com a existência seu autor. Mesmo que sua identidade deste autor esteja vinculada a uma conta na *Blockchain* identificada apenas por um pseudônimo digital, presume-se a existência deste autor que figura como o agente necessário no plano da existência.

Em relação ao objeto no plano da existência este é necessário para que as partes possam ter algo para negociar os seus interesses. Sem um objeto não haveria de se falar em negócio jurídico. Não haveria como haver uma relação negocial entre as partes, ora se o objeto for de absoluta impossibilidade, o negócio jurídico não chega a se formar, configurando caso de inexistência por falta de objeto (AZEVEDO, 2002, p. 34). No caso dos Contratos Inteligentes, a presença de um objeto para ser alvo da negociação entre as partes torna-se também um elemento evidente e de fácil comprovação.

Por seu turno, a forma é o meio pelo qual se exterioriza a vontade do agente que intenta realizar o negócio jurídico na celebração de um contrato. Ressalta-se que o ordenamento brasileiro utiliza o princípio da liberalidade das formas em que a manifestação de vontade pode ser expressa em qualquer meio, desde que não haja proibição legal. Deste modo não há óbice para que a forma seja implementada por meio de Contratos Inteligentes, no qual se a declaração da vontade se confirma pelo acesso do agente à interface que permite a codificação do Contrato Inteligente e se manifesta por meio de códigos de criptografia que possuem condições embutidas para serem realizados.

3.1.3.2 Plano da Validade

Uma vez presentes os elementos que comprovam a existência do negócio jurídico, é possível fazer sua qualificação dentro do plano da validade. Neste plano será analisado se cada elemento possui os requisitos dispostos no artigo 104 do Código Civil: agente capaz; objeto lícito, possível, determinado ou determinável e forma prescrita e não defesa em lei (BRASIL, 2002). Mesmo não estando expressa neste artigo, também a questão da vontade é analisada neste plano da validade, seja na capacidade e legitimidade do agente, seja na licitude do objeto do negócio (TARTUCE, 2018, P. 14).

Quanto ao agente é preciso que ele apresente capacidade e legitimidade em sentido jurídico. A capacidade corresponde a uma qualidade jurídica do sujeito que corresponde a um estado pessoal relacionado ao poder de, pessoalmente, exercer os direitos e praticar os atos da vida civil. A falta de capacidade torna o negócio jurídico nulo ou anulável. Serão nulos os negócios jurídicos firmados por absolutamente incapazes, conforme o artigo 166, I do Código Civil, enquanto que os realizados por relativamente incapazes são apenas anuláveis por força do artigo 171, I do mesmo código (BRASIL, 2002). Ainda se ressalta que os negócios jurídicos nulos são irremediáveis conforme prevê o art. 169, do CÓDIGO CIVIL, enquanto que os anuláveis admitem confirmação e se convalidam com o passar do tempo, caso a parte interessada não intente ação própria no prazo de quatro anos conforme artigos 172 e 178, III, do Código Civil (BRASIL, 2002). Por seu turno, a legitimidade consiste em uma posição do sujeito relativamente ao objeto do direito, que se traduz, em geral, na titularidade do direito, posição esta que tem como conteúdo o poder de disposição, tal qual o poder de aquisição (REBOUÇAS, 2015, p. 1425). A legitimidade é direta quando o próprio sujeito capaz é quem atua dispondo de seus direitos e contraindo obrigação. Quando o negócio jurídico é realizado por representante investido dos direitos para representar o aquele sujeito, diz-se que a legitimidade é indireta.

As partes em um Contrato Inteligente podem operar por meio de contas registradas na *Blockchain* em que aquele contrato será instalado e posto em funcionamento. Estas contas podem conter apenas pseudônimos dos reais sujeitos que as criam. Esta característica dos negócios jurídicos, em sentido estrito, implementados na forma de Contratos Inteligentes pode suscitar problemas de identificação da capacidade e da legitimidade dos sujeitos, ora partes do contrato. Neste sentido a boa-fé objetiva torna-se ainda mais importante em prol de conclamar a idoneidade das partes contratantes. Porém, em caso de um litígio, pode-se tornar inviável esclarecer se a parte que contraiu negocia sabia ou não e eventual incapacidade, absoluta ou relativa, ou ainda ilegitimidade do agente com que contraiu negócio. Este tipo de problema pode ser superado se as partes foram compelidas a usar sua identificação real quando de seu cadastro na *Blockchain*. Este tipo de imposição até pode ser compreensível no caso das redes *Blockchain* compostas por membros associados, fechadas e permissionadas, porém é opera frontalmente em sentido contrário às *Blockchains* abertas ou não permissionadas que possuem caráter libertário.

A vontade está intimamente relacionada com a questão do agente, pois não basta que este seja capaz e possua legitimidade para ser parte do negócio jurídico, é imperioso que a sua declaração da vontade seja livre e não esteja eivada de vícios ou defeitos jurídicos conforme disposto nos artigos 138 a 165 do Código Civil (BRASIL, 2002). Em outras palavras, a declaração de vontade, tomada como um todo, dever ser: a) resultante de um processo volitivo; b) querida com plena consciência de realidade; c) escolhida com liberdade; d) deliberada sem má fé (REBOUÇAS, 2015, p. 1368).

Nos Contratos Inteligentes, a expressão da vontade pode ser observada em dois momentos: no primeiro momento a parte proponente programa seu interesse que será codificado em um bloco da cadeia *Blockchain* para depois ser aceito pela parte contraente em outra transação a ser também codificada na mesma cadeia de blocos. Ambas as transações são autenticadas pelos outros membros da mesma cadeia de blocos, tornando as transações registradas de forma imutável na *Blockchain*. Apesar da execução dos Contratos Inteligentes ser automática, a mesma não dispensa a manifestação da vontade das partes para se tornar efetiva, o que ocorre a quando da celebração do contrato (GOMES, 2018, p. 48). Em paralelo com todo o aparato tecnológico envolvido, a tecnologia não tem muito a oferecer em termos de garantia da validade da expressão da vontade, visto que a forma de transações registradas de forma voluntária em na *Blockchain* não consegue garantir que não aconteceram problemas como simulação ou reserva mental, ou seja, aquilo que o declarante manifesta não é exatamente aquilo que o deseja, tentando manipular o negócio para prejudicar um terceiro.

A respeito da qualificação do objeto em um negócio jurídico, este deve ser lícito, possível, determinado ou determinável, conforme expresso no artigo 104, II do Código Civil (BRASIL, 2002). Também na doutrina se afirma que além dos requisitos legais dispostos, é indispensável observar os bons costumes, evitar o abuso do direito, não violar a ordem econômica, preservar a boa-fé objetiva e a função social do contrato (GOMES, 2009, p. 382).

A responsabilidade pela determinação de um objeto válido nos Contratos Inteligentes cabe inteiramente às partes que realizam aquele negócio jurídico. A cadeia *Blockchain* é neutra e, mesmo composta por um grande número de agentes autenticadores das transações, não é validado o objeto em si, visto que a referida validação da transação

confere autenticidade comprovada que ela realmente existiu e que as foram as partes contratantes que a realizaram por meio de suas assinaturas por meio de chave privada. Não se entra no mérito de interpretar o objeto, nem no mundo dos fatos, tampouco em acepção jurídica. Por exemplo, se as informações sobre o objeto negociado em um Contrato Inteligente forem derivadas de um registro de um documento físico, sua inserção na *Blockchain ex postfacto* depende do grau em que os dados originais são precisos, corretos, confiáveis, etc. Mesmo que seja utilizado um sistema de multiassinatura no qual cada parte contratante precisa conferir e assinar o documento antes de submetê-lo a registro na *Blockchain*, esta abordagem apenas asseguraria que "os documentos foram transcritos com acurácia a partir do registro original para o sistema baseado em *Blockchain*, não que os documentos fossem acurados desde o início" (LEMIEUX *et. al*, 2018, p. 20).

Talvez, em um futuro não tão distante, possam ser implementados algoritmos dotados de Inteligência Artificial que realizem uma análise em sentido legal da validade dos objetos, porém, neste cenário serão suscitados outros tipos de questionamento como a liberdade e autonomia das partes contratarem em face à uma vigilância autoritária. O presente trabalho não tem a ousadia de contemplar este tipo de pressuposição.

Por fim, o plano da validade contempla a forma do negócio jurídico, meio pelo qual se institui a manifestação da vontade das partes contratantes. Esta forma deve ser forma prescrita ou não defesa em lei, o que é consubstanciado por força legal no artigo 104, III do Código Civil (BRASIL, 2002).

A primeira parte desta normativa, ao declarar a expressão forma prescrita se refere a casos particulares quando a lei expressamente exigir forma específica para celebração daquele negócio jurídico, deverá o operador do Direito atentar-se como deve ser implementado o Contrato Inteligente em questão. É o que acontece quando a lei exige das partes, para a própria garantia dos negócios, forma especial, por exemplo, na compra e venda de imóveis de valor superior a um mínimo legal de trinta vezes o salário mínimo vigente no País, conforme artigo 108 do Código Civil, dos pactos antenupciais e das adoções, em que requer a escritura pública disposto no artigo 1657 do Código Civil e artigos 167, I, 12 e 178, V da Lei de Registros Públicos (BRASIL, 1973). A seu turno, a segunda parte do referido inciso manifesta que é possível se utilizar da forma preferida pelas partes para a formação de negócios jurídicos. Nesse sentido também corrobora o expresso no

artigo 107 do Código Civil, ao se dispensar forma especial para a manifestação da vontade das partes, salvo quando a lei expressamente o exigir (BRASIL, 2002).

Esta preleção confirma que os Contratos Inteligentes podem, de forma geral, serem utilizados para implementar a maioria dos contratos em um panorama geral de aplicação, porém ficando dependente os casos previstos em lei que exigem confirmação legal através de escritura pública, de documento autêntico ou de documento particular autenticidade (GOMES, 2018, p. 48). Sem o cumprimento desta formalidade prevista em lei, os negócios jurídicos seriam nulos e estaria em risco a segurança jurídica de Contratos Inteligentes nestes casos específicos.

3.1.3.3 Plano da Eficácia

No plano da eficácia são tratados as consequências e os efeitos que o negócio jurídico produz em relação às partes e a terceiros, ou seja, "não basta que o negócio jurídico exista e seja válido, pois, necessário se faz que ele esteja apto a emanar efeitos, em suma, ser eficaz" (JORGE JUNIOR, 2004, p. 23). Podemos elencar neste plano a presença da condição, de termo e do encargo, institutos jurídicos regrados no Código Civil pelos artigos 121 a 137 (BRASIL, 2002) e também de casos como as regras relacionadas com o inadimplemento, dos juros, da multa ou cláusula penal, das perdas e danos, da resolução, da resilição, do registro imobiliário e da tradição de bens reais (TARTUCE, 2018, p. 15). Em outros termos pode-se afirmar que alguns efeitos dos negócios jurídicos somente são ineficazes até que alguma situação seja testada se foi satisfeita conforme estabelecido previamente. Um exemplo prático pode ser obtido no caso de uma contratação com condição suspensiva de vinculação ao pagamento, ou seja, a compra e venda existe e é válida, porém está pendente de confirmação do pagamento ou da liberação de determinado crédito (REBOUÇAS, 2015, p. 1456).

Os Contratos Inteligentes tornam-se uma ferramenta de grande valia para se operar os elementos do plano da eficácia dos negócios jurídicos, pois trazem ao controle da execução das cláusulas recursos computacionais que podem testar as situações combinadas e, conforme o resultado do teste, dar continuidade ou não à execução do contrato, inclusive suspendendo direitos e obrigações até o momento em que forem satisfeitas as condições previamente combinadas. Porém, no caso de bens reais, este recurso tem algumas limitações de ordem prática, visto que pode ser necessário, conforme a legislação

pertinente, confirmar a tradição ou ainda realizar registro público para que seja concretizada a eficácia do negócio jurídico perante terceiros. Nestes casos, fica parcialmente comprometida a funcionalidade de autoexecução daquele Contrato Inteligente. Solução possível para este impasse seria fornecer ao Contrato Inteligente acesso a algum oráculo para que possa se comunicar com o mundo externo à *Blockchain* para verificar se aquele evento de fato ocorreu.

Até o momento em que se realiza a presente pesquisa ainda é tímida a oferta de serviços que implementem tal comunicação entre os Contratos Inteligentes implementados em *Blockchain* com os órgãos de registros públicos. Há um projeto piloto acontecendo na cidade de Pelotas no Rio Grande do Sul onde o Cartório de Registro de Imóveis vai registrar informações detalhadas como endereço de propriedade, proprietário, número de parcela e classificação de zoneamento em *Blockchain* (LEMIEUX *et al.*, 2018). Neste caso, as propriedades podem se tornar efetivas propriedades inteligentes e os Contratos Inteligentes podem ser utilizados com suas plenas funcionalidades.

3.2 APRECIAÇÃO DAS ESPECIFICIDADES DOS CONTRATOS INTELIGENTES

Partindo do ponto que os Contratos Inteligentes podem ser definidos como contratos eletrônicos intersistêmicos e podem ser concebidos como negócios jurídicos em sentido estrito, válidos e eficazes à luz da teoria da "Escada Ponteana", passa-se a um estudo mais minucioso a respeito da interpretação jurídica específica dos Contratos Inteligentes. O foco no estudo destas características peculiares dos Contratos Inteligentes é uma forma de otimizar a abordagem desta pesquisa, pois considera-se que, de modo geral, os Contratos Inteligentes não são muito diferentes do que as outras formas de contratos existentes (DE FILIPPI; WRIGHT, 2018, p. 1447).

Tomando como base que, via de regra, os Contratos Inteligentes são tutelados pelo mesmo arcabouço jurídico dos contratos convencionais, é possível focalizar as especificidades de tutela jurídica de modo mais diligenciado, ponderando como estas podem colaborar para a formação de contratos com segurança jurídica e também quais são os desafios a serem superados.

Muitas das barreiras a serem superadas na implementação dos Contratos Inteligentes são oriundas do desconforto da mudança para algo novo e desconhecido e pela incerteza ocasionada pelo impacto desta mudança. O enfrentamento destes obstáculos pode ser melhor realizado traçando paralelos entre os pontos de críticos em que se melhor percebe a definição da mudança e a realidade já conhecida (RASKIN, 2017, p. 340). A partir deste entendimento, serão analisados os efeitos dos Contratos Inteligentes no ordenamento jurídico brasileiro a partir dos planos de maior impacto promovidos por sua inovação tecnológica em suas dimensões peculiares, a saber, descentralização, imutabilidade e autoexecução.

3.2.1 Dos benefícios aos perigos da autoexecução

O apelo que se faz em torno dos Contratos Inteligentes é que sua autoexecução vai trazer maior confiança para as partes e que a remoção dos intermediários vai reduzir custos e vai aumentar a eficiência das transações (DE FILIPPI; WRIGHT, 2018, p. 1410). Esta proposição é muito sedutora, porém é imprescindível considerar que na prática os contratos serão celebrados e operados em um mundo não determinista, cheio de incertezas e ambiguidades. Deste modo é importante ponderar a respeito um modelo para se projetar Contratos Inteligentes que possam operar de forma eficaz e com segurança jurídica.

O arcabouço legal em que se assenta a base jurídica que sustenta um contrato transforma uma obrigação moral em um conjunto de obrigações reconhecidas pela sociedade e juridicamente exigíveis e também pode tornar um contrato nulo ou anulável, por exemplo, quando houver alguma ilegalidade que suscite a invalidade do negócio jurídico em questão. As sanções em face ao inadimplemento de uma cláusula contratual incentivam o cumprimento do contrato, fornecendo parte do mecanismo de execução – um contrato também pode conter elementos de um mecanismo pelo qual as obrigações contratuais podem ser executadas. Assim, é possível encerrar um mecanismo no contrato que cria uma expectativa de cumprimento apoiada pelo quadro legal externo, dando origem a uma "norma de execução". A perspectiva de execução legal que se liga a um contrato, em oposição a uma obrigação moral, aumenta a confiança de que a obrigação será cumprida, tornando-a mais comprometedora do que apenas aquela obrigação moral (LIM, 2016).

No contrato tradicional, o conjunto de definições de obrigações entre as partes é expresso em uma linguagem que, em tese, as partes conseguem entender. Porém, a flexibilidade de se escrever os contratos utilizando a linguagem natural gera um certo grau de ambiguidade em face à imprevisibilidade dos acontecimentos futuros do contexto em que o contrato vai ser operado, visto que nem sempre é possível transcrever suas relações contratuais abertas e, muitas vezes, ambíguas, em uma linguagem determinística. Talvez isso nem seja possível sem perder a flexibilidade inerente à expressiva linguagem humana. Deste modo, há casos em que é necessário examinar se realmente as partes tinham aquela intenção expressa naquele contrato, sendo necessário, por vezes, recorrer ao Judiciário para solucionar algum conflito.

Os Contratos Inteligentes, por sua vez, possuem uma lógica booleana[17] que é determinística, formal e rígida. Todas as condições a serem cumpridas devem ser previstas no início de sua programação, pois os Contratos Inteligentes não deixam alternativas às partes senão a autoexecução automática e irreversível do que foi programado em suas cláusulas. Nos contratos tradicionais, as partes muitas vezes descumprem, por eventual necessidade, um termo pactuado, mesmo cientes das sanções e consequências decorrentes deste inadimplemento. Em tese, um negócio autoexecutado por Contratos Inteligentes teria menor ocorrência de litígios por inadimplência e consequentemente uma redução de acionamento do judiciário para resolução daqueles litígios, porque a execução já estava predefinida nas regras programadas no código de computador do respectivo Contrato Inteligente. Infringir a lei seria o mesmo que inadimplir um Contrato Inteligente, o que necessitaria de adulterar o código de software – inviável para quase que a totalidade das pessoas. (DE FILIPPI; WRIGHT, 2015, p. 26).

Uma vez programado o Contrato Inteligente e posto em funcionamento na *Blockchain*, sua execução é automática. Se o objeto do contrato for composto por ativos inteligentes, aqueles que originalmente tem natureza digital e podem ser alcançados por comandos da *Blockchain*, no momento da satisfação das condições estabelecidas, aqueles ativos inteligentes serão transacionados de forma automática. Isso já é uma realidade no

[17] Em Ciência da Computação, lógica booleana é um conjunto de operações algébricas que possui dois valores, que podem ser considerados como 0 ou 1, falso ou verdadeiro. A denominação booleana é uma homenagem a George Boole, que definiu um sistema de lógica algébrica pela primeira vez na metade do século XIX.

tempo em que se realiza esta pesquisa. Porém, mesmo que o objeto do contrato não esteja vinculado a um ativo inteligente, ainda assim é possível fazer sua integração com sistemas que controlam estes objetos por meio de dispositivos inteligentes a eles atrelados. Como exemplo pode-se citar um carro que tem um software instalado para evitar ignição se os termos de um contrato de financiamento não forem cumpridos (RASKIN, 2018, p. 310).

Outro exemplo clássico trata-se de um mecanismo de depósito, muito comum em negociações de fusões e aquisições. Uma das partes tem um bem que quer negociar e a outra parte tem o dinheiro para a compra daquele bem. Há um "encontro de mentes" (SZABO, 1997). A convergência este proposta e aceitação está consumada. Porém aquele que detém o bem não quer entrega-lo sem o devido pagamento, pois tem receio de entregar o bem e a outra parte não entregar o pagamento. E aquele que possui o dinheiro pra a aquisição, não quer realizar o pagamento antes que a outra parte lhe entregue o bem, pois teme pagar e nada receber. Deste modo há um impasse e a solução atual é contratar um terceiro certificado que vai registrar a transferência do bem ao mesmo tempo que realiza o pagamento. Este terceiro, por óbvio, tem seus custos, demoras, etc. O Contrato Inteligente pode implementar um mecanismo de "depósito". Uma câmara de garantia que recebe os dois ativos, o bem e o dinheiro, e somente finaliza a liberação de ambos para as outras partes quando se certifica que que está tudo certo. Qualquer inconformidade automaticamente aciona comandos no Contrato Inteligente para desfazer a relação contratual e devolver os respectivos ativos para seus proprietários originais (CICCONI, STABILE, 2018, p. 6).

O encanto promovido pela funcionalidade de autoexecução garantida dos Contratos Inteligentes tem alguns percalços a serem superados, pois nem sempre o contrato e é estabelecido de forma hermética dentro de uma *Blockchain*, perfeitamente isolado e previsível. Ele vai, necessariamente, influenciar e ser influenciado pelo mundo dos fatos e vai sofrer as dores que historicamente os contratos tradicionais sofrem, tais como: equívocos sobre a interpretação da intenção das partes, manipulação da intenção de uma das partes, falta de capacidade para uma parte realizar aquele contrato, entre outros defeitos que acometem os negócios jurídicos, listados de forma exemplar, mas não exaustiva, nos artigos 166 e seguintes do Código Civil (BRASIL, 2002).

Em um contrato tradicional, alguns destes vícios podem ser passíveis de retificação quando não se adequarem às exigências da lei ou quanto não refletirem as obrigações acordadas pelas partes contratantes. Em um Contrato Inteligentes, as instruções são irrevogáveis e serão executadas independentemente de situações supervenientes. (JUELS *et al.*, 2016, p. 2).

Outra implicação resultante da autoexecução é em relação ao princípio da boa-fé objetiva está previsto no art. 422 do Código Civil (BRASIL, 2002), o qual aduz que na execução e na conclusão as partes devem sempre prezar pela probidade e pela boa-fé. Nos casos dos Contratos Inteligentes, a boa-fé objetiva só pode ser observada no momento da codificação das cláusulas, visto que depois não há de se falar de autonomia da vontade, pois a autoexecução se dará de forma automática e ininterrupta.

A programação dos contratos em linguagem computacional também resulta na necessidade de redigir o código do contrato de forma assertiva e sem erros de programação. Ambas premissas são muito difíceis de serem implementadas. A linguagem natural, como visto, é aberta e, em oposição à linguagem de computador tende a incluir termos abertos que descrevem as obrigações contratuais. O caso da boa fé apresentado é um exemplo clássico. Uma parte pode se comprometer a dispor dos melhores esforços para cumprir suas obrigações, porque a maneira mais econômica ou eficiente de desempenho talvez ainda não seja previsível. Muitas vezes há valor em manter contratos abertos ou ambíguos, porque proporciona flexibilidade às partes, ao mesmo tempo em que reduz o tempo e o custo da negociação. Em muitos casos, a imprecisão pode, de fato, resultar em contratos mais eficientes (DE FILIPPI, WRITGH, 2018, p. 1506). Se para uma pessoa natural isso é perfeitamente compreensível, para programar esta condição em um software seria necessário definir todos os sentidos de uma expressão de forma determinística, em um exercício de previsão para se testar todas as condições possíveis.

A questão de erros na programação dos softwares que implementam os Contratos Inteligentes também é digna de apreensão. O desenvolvimento de software é estruturalmente propenso a falhas, apesar dos esforços significativos para remediá-las, eliminar bugs completamente é simplesmente impossível. Por mais que se esforce para produzir sem falhas as linhas de software do Contrato Inteligente, erros podem ser descobertos somente no momento da execução das cláusulas (DE FILIPPI, WRITGH, 2018, p. 694).

E como não será possível interromper a execução daquele software, visto que ele está funcionando em nodos da *Blockchain*, executando comandos fora do alcance das partes e realizando operações indesejadas que precisarão ser revertidas, pode-se gerar custos insuportáveis ou, em cenários mais extremos, danos irreversíveis.

Uma solução que pode mitigar até certo ponto estes riscos é a realização de meticulosas negociações preliminares entre as partes. Segundo Maria Helena Diniz (2008, p. 34) as negociações preliminares não fazem parte do contrato, não há criação de vínculos entre as partes, mas são muito úteis para o estabelecimento de cláusulas contratuais mais bem definidas e com maior precisão daquilo que se deseja contratar. Mesmo depois deste prévio trabalho, é necessário que o software desenvolvido para implementar o Contrato Inteligente na *Blockchain* seja exaustivamente testado antes de ser colocado em produção, sendo um trabalho a ser feito de forma multidisciplinar, tanto por operadores do Direito quanto por analistas e programadores.

Os operadores de Direito também precisam ponderar se os Contratos Inteligentes são, em seu estado tecnológico atual, aplicáveis a todos os negócios jurídicos e suas respectivas relações contratuais. Há casos, já apresentados neste estudo, em que a lei determina escritura pública, conforme artigo 108 do Código Civil ou forma específica prevista em lei conforme artigo 166, IV do mesmo diploma legal (BRASIL, 2002). A implementação dos Contratos Inteligentes nestes casos seria limitada à algumas etapas ou, talvez, nem teria utilidade possível. Conforme discorre Luciano Glória (2017, p. 86), há outros casos apresentam limitações legais a respeito dos direitos tutelados envolvidos, quando a lei faculta a uma das partes a interrupção, descontinuidade, cessação, ou, ainda, com maior garantia, o direito das partes em resilir o contrato a qualquer momento por meio de distrato, a seguir listados de forma exemplar, mas não exaustiva:

(i) contrato de adesão civil, com renúncia antecipada de direito - art. 424 do Código Civil (BRASIL, 2002);

(ii) obra protegida por direito personalíssimo ou autoral, em que a ininterrupção do contrato é vedada pela lei - art. 12 do Código Civil, e art. 24, inciso VI da Lei nº. 9.610/1998 (BRASIL, 1998);

(iii) consumidor, em que haja impossibilidade de rescisão - art. 49 do Código de Defesa do Consumidor (BRASIL, 1990), ou arrependimento em compras em sites de *e-commerce* conforme Decreto n. 7.962/2013) (BRASIL, 2013);

(iv) matéria de ordem pública em direito público e privado, necessária para assegurar a função social da propriedade e do contrato - art. 2.035, Parágrafo único do Código Civil (BRASIL, 2002).

De todo modo, há situações nas quais, mesmo sem ressalva legal, a implementação da autoexecução disponibilizada pelos Contratos Inteligentes pode desencadear danos às partes ou a terceiros. A cessação destes danos é impraticável, uma vez que iniciada a execução na *Blockchain* de um Contrato Inteligente, não é mais possível interrompe-la, a não ser que se desligue os nodos em que o código está sendo executado. E como isso é improvável, talvez impossível, a alternativa seria reparar os danos *a posteriori*. Porém, o tempo que leva para esta reparação pode causar danos irreversíveis e insuportáveis.

Por fim, entende-se que a flexibilidade presente nos contratos tradicionais os torna menos eficientes em termos de execução, porém facilita alguns mecanismos que protegem partes menos favorecidas (consumidores, por exemplo) que podem invocar algumas situações de nulidade ou anulabilidade contratual tais como assimetrias de informação, coação, abusividade, inconsciência e incapacitação. Por outro lado, a assertividade determinística dos Contratos Inteligentes não dá margem para este tipo de salvaguarda e a autoexecução, característica peculiar deste tipo de tecnologia precisa ser utilizada com prudência para um aproveitamento otimizado dos promissores recursos dos Contratos Inteligentes.

3.2.2 As duas faces da imutabilidade

Uma característica intrínseca da tecnologia *Blockchain* muito festejada é a imutabilidade. Por meio desta característica obtém-se a tão desejada incorruptibilidade das informações registradas, promovendo confiança de que o for registrado naquela cadeia de blocos será eternizado de forma indelével. Os Contratos Inteligentes ora em estudo, por serem implementados com base nesta tecnologia subjacente se beneficiam desta característica particular: as informações produzidas para e pelas relações contratuais tornam-se invioláveis, permanentes e fidedignas (GOMES, 2018, p. 81).

A imutabilidade das informações registradas na *Blockchain* também vem de encontro a um dos princípios contratuais mais antigos, o "*Pacta sunt servanda*". Ao aderir a um Contrato Inteligente as partes assumem que estão vinculadas às regras e determinações codificadas em software registrado na *Blockchain*. Este princípio dispõe sobre a força obrigatória dos contratos, definindo a máxima "o contrato faz lei entre as partes", previsto no artigo 1.134 do Código Civil Francês[18] (FRANÇA, 1804) ou seja, tudo o que for combinado entre as partes não pode ser alterado de forma unilateral. É necessário, portanto, que haja sempre o consentimento bilateral para a realização de alterações no contrato celebrado. Nem mesmo judicialmente se pode alterar unilateralmente o conteúdo de um contrato, pois segundo Maria Helena Diniz (2008, p. 37), "o ato negocial, por ser uma norma jurídica, constituindo lei entre as partes, é intangível, a menos que ambas as partes o rescindam voluntariamente ou haja a escusa por caso fortuito ou força maior", conforme o Código Civil, artigo 393, parágrafo único (BRASIL, 2002).

Porém, logo a seguir, a renomada doutrinadora expõe que, em certas circunstâncias excepcionais ou extraordinárias que impossibilitem a previsão de excessiva onerosidade no cumprimento das obrigações contraídas, que o magistrado possa mitigar a força vinculante dos contratos. Inclusive destaca-se que há várias previsões legais nesse sentido, citando como exemplo não exaustivo, os casos da Lei n. 8.078/1990, artigos 6º, V, e 51, IV (BRASIL, 1990) e o disposto no Código Civil nos artigos 317, 478, 479 e 480 (BRASIL, 2002). Tem-se então o fundamento legal do princípio "*Rebus sic stantibus*" que permite a revisão das condições contratuais se ocorrer mudança imprevista em relação ao momento da celebração, razoavelmente imprevisível e inimputável às partes, que causem desproporção excessiva na relação das partes, de modo que uma aufira vantagem exagerada em detrimento da desvantagem da outra (TARTUCE, 2017, p. 182). Aparentemente o princípio "Rebus sic stantibus" é antagônico ao princípio "Pacta sunt servanda", porém pode-se dizer que eles se completam, visto que o bom uso combinado de ambos traz equilíbrio e serena as relações contratuais.

[18] No original Art. 1.134. "*Les conventions légalement formées tiennent lieu de loi à ceux qui les on faites*", ou em livre tradução: "Os acordos legalmente formados tomam o lugar da lei para aqueles que os fazem". Disponível em: http://www.assemblee-nationale.fr/evenements/code-civil/cc1804-l3t03.pdf e http://www.assemblee-nationale.fr/evenements/code-civil-1804-1.asp.

De todo modo, se o princípio "*Pacta sunt servanda*" muito bem se implementa nos Contratos Inteligentes pela característica da imutabilidade da tecnologia *Blockchain*, o mesmo não é possível ser dito em relação do princípio "rebus sic stantibus". Se nos contratos tradicionais é possível fazer, por meio de aditamentos, ajustes em alguma cláusula específica ou ainda realizar complementos em face a uma situação superveniente à celebração do contrato original, nos Contratos Inteligentes isso não é possível, visto que as informações registradas em um bloco da *Blockchain* é imutável, seja este bloco composto por alguma informação útil ao contrato ou até mesmo o código do software em que o contrato foi programada, não é passível de alteração.

Também é necessário que se enfrente neste contexto o problema das informações que registradas de forma equivocada na *Blockchain*. Estas informações podem ser referentes às partes, informações dos objetos ou até mesmo o próprio código programado (software) do Contrato Inteligente. Se o erro for descoberto em tempo de não dar início à execução o respectivo Contrato Inteligente, é possível cancelar aquele registro e fazer um novo contrato, mesmo com todo desventura que isso venha causar. Porém, uma vez posto o contrato em funcionamento, como visto na seção anterior, suas cláusulas serão autoexecutadas de forma ininterrupta, agravando as consequências (LEMIEUX *et al.*, 2018, p. 30).

Um debate muito interessante que surge diz respeito ao tratamento dos dados em face às novas leis de proteção de dados que estabelecem que os usuários devem ter controle sobre seus dados em todos os momentos. Os exemplos mais notórios destas novas legislações são a *General Data Protection Regulation* (GDPR) na Europa (EU GDPR, 2018) e a recentemente promulgada Lei 13.709/2018, Lei Geral de Proteção de Dados brasileira - LGPD, que entrará em plena eficácia em fevereiro de 2020 (BRASIL, 2018).

Em um relatório publicado em outubro de 2018, o *European Union Blockchain Observatory and Forum* argumenta que o cumprimento da GDPR é fundamentalmente menos sobre a tecnologia em si e mais sobre como essas tecnologias são usadas (EU *BLOCKCHAIN*, 2018, p. 4). Este mesmo relatório apresenta alguns pontos constituem verdadeiros desafios para a implementação plataformas que utilizem a tecnologia *Blockchain*, dentre as quais, os Contratos Inteligente, ora objeto deste estudo. São 3 pontos de tensão bem explícitos: (i) Determinação de obrigações para controladores e processadores

de dados; (ii) Garantir a anonimização dos dados pessoais e (iii) Definição do controle dos usuários sobre suas informações (EU *BLOCKCHAIN*, 2018, p. 5).

Estes pontos precisam ser diligenciados em duas vertentes com base nos tipos de *Blockchain*, conforme apresentado no item 1.5 deste trabalho. A primeira vertente trata se a *Blockchain* for privada ou permissionada, formada por um consórcio de participantes conhecidos que detém o poder de consenso das informações da *Blockchain*. A segunda vertente trata dos casos das *Blockchain*s não permissionadas ou públicas, como, por exemplo *Bitcoin* e *Ethereum*.

Considerando as *Blockchain* privadas, mesmo sendo implementadas por protocolos muito complexos, seria possível negociar uma mudança no protocolo da cadeia de blocos para implementar a conformidade diante da GDPR em prol de atender aos três requisitos acima dispostos. De outro lado, se o caso versar sobre *Blockchain*s públicas, torna-se praticamente impossível alterar o seu protocolo, já que a tarefa de o processamento de dados é dividida um número incontável de nós que criam e validam os blocos da cadeia *Blockchain.*

O cenário torna-se mais complicado no caso do direito dos usuários de controle sobre seus dados. É importante esclarecer que a tecnologia *Blockchain* não permite a edição ou a remoção de informações uma vez que inseridos nos blocos de sua cadeia. Trata-se da característica da imutabilidade, ora em estudo. O próprio relatório do *European Union Blockchain Observatory and Forum* apresenta alguns princípios para os desenvolvedores de plataformas baseada em *Blockchain*, com o objetivo de manter a conformidade com a GDPR. A primeira das alternativas sugere ponderar ser realmente a aplicação a ser desenvolvida necessita da tecnologia *Blockchain* ou se poderia ser utilizado outro tipo de tecnologia. A segunda alternativa é evitar gravar dados pessoais dos usuários na *Blockchain*, utilizando-se de banco de dados alternativos, centralizados e controlados para tal fim. Obviamente esta alternativa é diametralmente oposta ao ideal da descentralização e desintermediação da tecnologia *Blockchain*. Em terceiro lugar, propõe-se inserir os dados pessoais dos usuários em uma *Blockchain* privada. E, por fim, o relatório sugere, de forma vaga e imprecisa, que as empresas a sempre “inovar” e permaneçam “transparentes” com os usuários. Infelizmente, o relatório não elabora o que isso realmente significa (EU *BLOCKCHAIN*, 2018, p. 28).

No caso da lei brasileira conhecida como Lei Geral de Proteção de Dados – LGPD (BRASIL, 2018), que busca preservar a privacidade e a autonomia dos usuários na Internet, também é possível por analogia, notar conflitos da mesma ordem que o estudo apresentado acima sobre a GDPR.

Em primeiro lugar, a LGPD traz em seu artigo 3º a determinação de obrigações para controladores e processadores de dados (BRASIL, 2018):

> Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:
> I - a operação de tratamento seja realizada no território nacional;
> II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou
> III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

Também a LGPD se manifesta em relação à anonimização dispondo sobre este preceito no artigo 5º, III (BRASIL, 2018):

> Art. 5º Para os fins desta Lei, considera-se:
> III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

E depois estatui que o usuário titular da informação pode solicitar a anonimização do seu dado, conforme estabelecido no art. 18, IV (BRASIL, 2018), que será visto a seguir.

Em relação aos direitos do usuário titular das informações, também a LGPD apresenta resolução expressa e clara em seu artigo 18, no qual pode-se destacar que há patente conflito com a característica da imutabilidade da *Blockchain* em especial nos incisos III, IV, V, VI e IX (BRASIL, 2018):

> Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
> I - confirmação da existência de tratamento;
> II - acesso aos dados;
> III - correção de dados incompletos, inexatos ou desatualizados;
> IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;

> V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador;
> VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
> VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
> VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
> IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

De toda esta análise, é possível concluir que tanto a GDPR quando a LGPD entram em choque frontal e direto com a característica da imutabilidade das informações na *Blockchain*. Tendo que os Contratos Inteligentes são implementados sobre esta tecnologia, este conflito também os afeta diretamente.

As soluções apresentadas pelo relatório do *European Union Blockchain Observatory and Forum* (EU *BLOCKCHAIN*, 2018) podem ser consideradas como alternativas para superar estes conflitos no caso da GDPR e também, por analogia, podem ser adaptadas para o caso da LGPD. Porém, nenhuma destas alternativas apresenta um caminho pacífico e sem perdas de funcionalidades da tecnologia *Blockchain* e dos Contratos Inteligentes.

3.2.3 Desconstruindo entes centralizadores e eliminando intermediários

Por séculos os bancos atuam como centralizadores do registro de crédito e débito das transações financeiras, gerenciando investimentos e poupança, controlando os fluxos de entrada e saída de riqueza e possibilitando a realização de negócios. Os governos também centralizam a tomada de decisão e realizam escolhas, democraticamente ou não, a respeito dos destinos dos concidadãos, coletando tributos e aplicando investimentos, realizando políticas públicas, redistribuindo riquezas e mantendo a ordem social. O judiciário mantém o controle jurisdicional aplicando a lei para resolver litígios e disputas. Também instituições civis e corporações concentram ao redor de si o poder que decisão sobre negócios e assuntos de seus respectivos grupos associados, partes interessadas e comunidades. A centralização, portanto, é um fator comprovadamente presente e socialmente aceitável, necessário ou até mesmo desejável. Assim sendo, os atuais modelos estão consolidados em forte regulamentação que justifica, legitima e reforça o papel de todos estes

agentes centralizadores em prol de promover a confiança necessária às relações negociais (RASKIN, 2017, 316).

A própria Internet, mesmo sendo desenvolvida de acordo com uma estrutura distribuída, amplamente interconectada e originalmente sendo influenciada pelos anseios libertários de seus pioneiros (MAY, 1988), acabou reproduzindo a estrutura de poder centralizado de instituições e corporações poderosas que acabaram por utilizar todos os seus avançados recursos tecnológicos para ampliar seus tentáculos controladores sobre os grupos sob sua influência: governos e grandes corporações se aproveitaram do poder da Internet para aumentar ainda mais a influência e o controle sobre a vida das pessoas (GOLDSMITH, WU, 2006, p. 142). É notório que Internet acelerou a forma de interação entre pessoas, corporações instituições, governos. Porém a questão da centralização e do controle foi replicada e intensificada também no mundo digital. E, mesmo com todos os controles centralizadores e entes que supostamente promovem relações de confiança, eles continuam sendo pontos de falha e não foram erradicados problemas como, por exemplo, "fraudes eletrônicas, estelionatos, perda de materiais, divulgação sem controle de documentos sigilosos, prejuízos materiais e morais oriundos de fatos ocorridos no mundo digital" (PARCHEN; FREITAS; EFING, 2013, p. 344).

Com o advento da tecnologia *Blockchain*, surge uma possibilidade de reversão deste cenário, pois, ao contrário dos atuais sistemas estruturados em organizações controladas por entes centralizadores, os Contratos Inteligentes implementados nesta tecnologia são autoexecutados sem a necessidade de um ente centralizador que traga confiança às partes contratantes, mediante custos de intermediação. Para Szabo (1997), qualquer intermediário pode, em princípio, ser substituído por um computador virtual confiável. No caso da tecnologia *Blockchain*, esta confiança é gerada automaticamente por protocolos baseados em forte criptografia, pelo estabelecimento de consenso sobre a validade das transações e sua replicação nos nodos participantes da rede em que se sincroniza a cadeia de blocos invioláveis e imutáveis. Deste modo, sem a necessidade de intermediários, os Contratos Inteligentes podem reduzir os custos marginais nas relações contratuais assim como a Internet possibilitou a redução dos custos de comunicação (DE FILIPPI; WRIGHT, 2015, p. 24).

A redução dos gastos com intermediários é uma das vantagens da descentralização propiciada pela tecnologia *Blockchain*. O Banco Central do Brasil publicou importante estudo sobre o impacto da tecnologia de registro de dados distribuída (*Distributed Ledger Technology* – DLT) em que apresenta outras vantagens propiciadas pela tecnologia *Blockchain* e enaltece a robustez da tecnologia em termos de proteção dos dados nela registrados, pois cria-se um ambiente mais seguro em termos de proteção das informações visto que estas são distribuídas em grande quantidade de nodos sincronizados, criando redundância e resiliência às informações (BCB, 2017, p. 4). Também se ressalta a autonomia das partes em realizar negócios jurídicos sem necessidade de um ente centralizador, empoderando as pessoas a realizarem transações por meio de novos modelos de negócios que permitem a utilização de plataformas digitais ágeis, seguras e sem burocracia (TAPSCOTT, 2016, p. 252).

Em que pese há atraentes argumentos teóricos para a defender os benefícios acima citados, não se pode olvidar alguns pontos críticos que precisam ser enfrentados para implementação de negócios por meio da plataforma *Blockchain*, incluindo os Contratos Inteligentes, objetos deste estudo. O primeiro deles trata da possibilidade de dispensa de entes centralizadores, o que afeta diretamente a atividade de notários e registradores. No Brasil a atividade notarial tem importante papel a fim de disponibilizar agentes confiáveis para instrumentalizar e dar fé pública aos negócios jurídicos (BRANDELLI, 2007, p. 4). Por vezes a necessidade da atividade notarial e registral tem origem em previsão legal, como, por exemplo, nos referidos registros dispostos no art. 1º parágrafo 1º da Lei de Registros Públicos – Lei 6015/1973 (BRASIL, 1973), nas escrituras de imóveis (art. 108, do Código Civil (BRASIL, 2002), dos pactos antenupciais e das adoções (art. 1657 do Código Civil e artigos 167, I, 12 e 178, V, da Lei de Registros Públicos) (BRASIL, 1973) Outras tantas vezes a atividade notarial tem necessidade implícita para prover confiança entre as partes contratantes e, consequentemente, segurança jurídica por meio de registro oficial com valor probante em Juízo.

A este respeito, em se tratando do registro de informações realizado por meio da tecnologia *Blockchain*, é importante fazer uma abordagem sobre o valor probante das informações dos Contratos Inteligentes, que sabidamente, ficam registradas em *Blockchain*. A este respeito Alexandre Morais da Rosa e Felipe Navas Próspero, discorrem com

pertinência e clareza (ROSA, PRÓSPERO, 2019), ressaltando que a Medida Provisória 2.200-2/2001 que institui a Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, traz regulamentação importante para o reconhecimento do mecanismo dos Contratos Inteligentes, conforme se observa em seu artigo 1º (BRASIL, 2001):

> Art. 1º - Fica instituída a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, **para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras** (grifo nosso).

Mesmo considerando que nas plataformas desenvolvidas com base na tecnologia *Blockchain* podem utilizar outras formas de assinaturas ou provas de autenticidade, ainda que não prescritas na referida Medida Provisória, estas podem se considerar como válidas, o que dá pleno respaldo aos documentos registrados em *Blockchain*, conforme prescrito no artigo 10 da referida Medida Provisória (BRASIL, 2001):

> Art. 10. Consideram-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos de que trata esta Medida Provisória.
>
> § 2º O disposto nesta Medida Provisória **não obsta a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento** (grifo nosso).

A plena viabilidade jurídica e validade de provas que sejam oriundas de documentos registrados e autenticados pelas chaves privadas em uma estrutura *Blockchain*, é ainda corroborada pelo que estabelece o Código de Processo Civil em seu art. 369 que dispõe que (BRASIL, 2015):

> As partes têm o direito de empregar **todos os meios legais**, bem como os moralmente legítimos, **ainda que não especificados neste Código**, para provar a verdade dos fatos em que se funda o pedido ou a defesa e influir eficazmente na convicção do juiz (grifo nosso).

Mais adiante no Código de Processo Civil vem o art. 411, II e sacramenta a possibilidade de comprovação da autenticidade de um documento em que a sua autoria esteja "identificada por qualquer outro meio legal de certificação, inclusive eletrônico, nos termos da lei" (BRASIL, 2015).

De todo modo, mesmo que sejam admitidas por um Juiz provas processuais com base em informações extraídas de uma *Blockchain*, haverá certa apreensão dos membros do em frente à linguagem computacional daquela plataforma, lembrando que as cláusulas em um Contrato Inteligente são escritas em código de software, sendo oportuno e até mesmo indispensável o auxílio de peritos de tecnologia da informação a fim de auxiliar na interpretação de detalhes técnicos das cláusulas de um Contrato Inteligente.

Por fim, é relevante considerar que, de forma diversa das estruturas tradicionais centralizadas, nos Contratos Inteligentes as identidades, informações e transações estão sincronizadas em muitos nodos distribuídos pela Internet, sem limitações geográficas, ou seja, podem estar operando em simultaneamente em muitas jurisdições e podem se distribuir pela *Blockchain* e não sendo controladas por nenhuma corporação ou entidade central, o que suscita também outro problema: o Contrato Inteligente pode operar em muitas jurisdições simultaneamente, muitas vezes com regramentos conflitantes entre si. Deste modo, conta-se com a boa vontade daqueles que implementaram o Contrato Inteligente em estar em conformidade com os ordenamentos jurídicos no quais vai atuar.

Se os Contratos Inteligentes não implementarem em seu código regras em conformidade com as jurisdições em que vão operar, muito possivelmente, haverá transgressões legais em um momento ou outro. E pouco podem os governos fazer na prática com exceção de medidas drásticas como banir a tecnologia, criminalizar os desenvolvedores de software de desenvolvimento e de infraestrutura, criar filtros para bloquear serviços de Internet ou ainda violar a privacidade dos cidadãos monitorando suas atividades (DE FILIPPI; WRIGHT, 2015, pp. 55-56).

3.3 MECANISMOS DE REGULAÇÃO A PARTIR DO MODELO DE LAWRENCE LESSIG

Os Contratos Inteligentes apresentam um conjunto *sui generis* de características que promovem a autoexecução das cláusulas celebradas, economia em termos financeiros e de outros recursos por meio da desintermediação e maior segurança contratual por meio da garantia de registros indeléveis e seguros. Por outro lado, os Contratos Inteligentes não podem ser considerados hermeticamente fechados em sua própria infraestrutura tecnológica. Eles necessariamente estabelecem interfaces com outros sistemas e também com

seus usuários e por meio de conexões com a Internet, são dependentes de uma comunidade de mineradores e também são condicionados à uma gama inumerável de fornecedores de software e hardware que fornecem os equipamentos para se utilizar todos os recursos da tecnologia. Cada um destes atores opera em determinada jurisdição (por vezes mais de uma) e, de certa forma, podem ser alcançados e regulados pela estrutura estatal na qual opera (DE FILIPPI; WRIGHT, 2018, p. 3555).

Enfrentando esta realidade, torna-se necessário admitir que há limitações importantes à total independência e autonomia da tecnologia dos Contratos Inteligentes. Nota-se que há alternativas consistentes para sua regulação. Um estudo alternativas para a regulação de tecnologias da informação e comunicação foi proposto por Lawrence Lessig em seu artigo intitulado "*New Chicago School*" (1998). Esta mesma teoria foi atualizada em sua obra posterior em que analisa a regulação do Ciberespaço, sendo foi denominada "*Pathetic Dot Theory*" (2008). Em que pese o foco do estudo de Lessig aborda de forma generalista a regulação da Internet como um todo, sua teoria aplica-se impecavelmente à tecnologia *Blockchain* e suas aplicações, como o caso em estudo dos Contratos Inteligentes, sendo muito útil para demonstrar que o controle da tecnologia da informação não emana somente de leis em sentido estrito, mas também de outras fontes como normas sociais, forças de mercado e contornos da arquitetura tecnológica (LESSIG, 2008, p. 2901).

A seguir são apresentados cada um dos quatro mecanismos de regulação propostos pela teoria de Lessig (leis, normas sociais, forças de mercado e arquitetura tecnológica) e sua aplicação em face às características intrínsecas de descentralização, imutabilidade e autoexecução dos Contratos Inteligentes, sem perder de vista que aqueles mecanismos podem operar individualmente ou de forma conjugada ao combinar sua influência de acordo com as variadas situações.

3.3.1 Leis estabelecidas pelo Estado

A forma mais direta de controle do comportamento das pessoas são as leis e regulamentos postos pelos entes estatais e seus representantes. Em face a estas leis os indivíduos tem a chance de atuar em conformidade com ordenamento legal com o qual guardam íntima relação ou enfrentar as penalidades pelo não cumprimento daquelas

normas legais (LESSIG, 2008, p. 2016). Os governos podem se valer do mecanismo de criação de lei para impor controles à tecnologia. Há vários níveis de atuação legislativa dos Estados nesse sentido, desde o controle indireto por meio de taxação de serviços, passando por regulamentação explícita do uso da tecnologia e até mesmo posições mais radicais como o que acontece em países nos quais estas limitações são sumárias, provocando inclusive o banimento de certas tecnologias que, segundo sua percepção, oferecem riscos à sua posição ideológica, como é o caso da regulação coercitiva, censura e filtros de Internet que ocorrem na em países governados por regimes ditatoriais (KELLY; COOK, 2011).

Em se tratando dos Contratos Inteligentes, o objeto da regulamentação por meio de criação de leis parece estar desaparecendo ao ser substituído por sistemas baseados em códigos autônomos que operam independentemente de qualquer pessoa física ou jurídica e se espraiam por meio de diversas jurisdições. À primeira vista, pode-se perceber que os governos estão perdendo sua capacidade de controlar as plataformas baseadas em redes *Blockchain* e os serviços nelas prestados (DE FILIPPI; WRIGHT, 2018, p. 3376).

A maneira mais direta pela qual os governos podem controlar uma tecnologia é impondo leis e regulamentos diretamente aos usuários finais. Para tanto é necessária a identificação dos agentes envolvidos em determinada situação que seja possível a aplicação da legislação posta. Todavia, os Contratos Inteligentes dificultam o atendimento a este primeiro requisito pois para participar da *Blockchain* em que operam este tipo de contratos, as partes realizam seus cadastros baseados em pseudônimos que, não necessariamente tem relação com sua identidade real. Também as técnicas de proteção de dados baseadas em forte criptografia que protege as transações dificultam o rastreamento dos seus autores para eventual imputação de responsabilidade civil ou criminal. Além do mais, os Contratos Inteligentes são programados, distribuídos e executados em um número sem limite de nodos por meio da descentralização da *Blockchain*, pulverizando a interação dos envolvidos e tornando a identificação dos envolvidos pouco eficaz.

Nota-se reiteradamente que os governos e grandes corporações tem uma insaciável sanha de controle sobre as pessoas. Independentemente se o objetivo deste controle é legítimo ou não, no caso dos Contratos Inteligentes não será diferente. Implementados em tecnologia *Blockchain*, as identidades e transações podem ser escrutinizadas por meio

de sistemas de *data mining*[19] de tal modo a resultar em informações úteis sobre os comportamentos das partes. Já há comprovações que mesmo o sistema de contas com pseudônimos na *Blockchain* pode ser possível inferir a identificação de uma pessoa associada a determinado endereço na cadeia de blocos (MEIKLEJOHN *et al*., 2013).

Outra providência passível de ser implementada pelos governos é a determinação de identificação das partes por meio da obrigatoriedade de mecanismos registro, monitoramento, auditoria e analise de informações dos clientes (*Know Your Customer* – KYC) de prevenção de lavagem de dinheiro (*Anti Money Laundry* – AML). Estas e outras medidas podem deturpar e inverter o propósito inicial dos Contratos Inteligentes, transformando-os em uma ferramenta poderosa de vigilância e controle (DE FILIPPI; WRIGHT, 2015, p. 54).

Ainda neste contexto, uma alternativa que resta aos governos seria criar mecanismos de responsabilização indireta daqueles que sustentam a cadeia de blocos subjacente aos Contratos Inteligentes. O primeiro alvo de uma regulamentação repressiva poderia ser focado nos provedores de Internet, visto que grande parte da comunicação na Internet se estrutura por meio de provedores serviços de Internet que fornecem serviços para acessar, usar ou participar da Internet. Estes provedores de Internet são facilmente identificáveis e estão, necessariamente, sujeitos a determinada jurisdição que pode ser utilizada para que os governos possam regular o comportamento dos cidadãos interagem com a Internet (GOLDSMITH, WU, 2006, p. 10).

De todo modo, esta maneira de controle ainda é ineficiente, visto que pode faltar um nexo de causalidade que comprove que a atuação de alguém que participava de uma rede que sustentava uma *Blockchain*, tinha ciência que em seu nodo estavam sendo transacionadas operações ilegais, pois nem os provedores de Internet nem os mineradores são capazes de identificar o conteúdo que passa pelos seus nodos, uma vez que a comunicação das transações ocorre de forma criptografada. Também nesse sentido, no Brasil, vem em socorro o Marco Civil da Internet – Lei n.º 12.965/2014 (BRASIL, 2014), que em seu artigo 18, tutela o Princípio da Inimputabilidade da Rede (no caso, da Internet) que

[19] *Data mining* significa mineração de dados. Trata-se de um processo computacional usado para extrair dados de um conjunto maior de dados brutos. Implica a análise de padrões de dados em grandes lotes de dados usando um ou mais softwares. Não confundir com mineração de blocos, utilizada pela tecnologia Blockchain.

protege os prestadores de serviços de conexão e hospedagem de serem imputados de culpa por delitos quando as ferramentas de conexão e de aplicações por eles fornecidas forem utilizadas, por seus usuários, para fins ilícitos:

> Art. 18. O provedor de conexão à internet **não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros** (grifo nosso).

Pode haver um efeito colateral da aplicação deste princípio da inimputabilidade presente no Marco Civil da Internet se for considerado que pode ser impossível atender o estabelecido no artigo 19 do mesmo diploma legal, que prevê que aquele responsável pelo provimento dos serviços de Internet, após notificação judicial, deve de tornar indisponível o conteúdo em questão, o que seria impossível em uma estrutura *Blockchain* devido à sua característica de imutabilidade. Felizmente, o artigo traz uma tábua de salvação ao prever que as providências devem ser tomadas no "no âmbito e nos limites técnicos do seu serviço" (BRASIL, 2014):

> Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, **no âmbito e nos limites técnicos do seu serviço** e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário (grifo nosso).

Além do Marco Civil Brasileiro da Internet há outras normas jurídicas específicas que tutelam as questões tecnológicas tais como a Lei nº 8.248/1991 (BRASIL, 1991), que dispõe sobre a capacitação e competitividade do setor de informática e automação; a Lei nº 11.077/2004 que atualizou sobremaneira o diploma anterior (BRASIL, 2004); a Lei que trata informatização dos processos judiciais - Lei n.º 11.419/2006 (BRASIL, 2006); a Medida Provisória nº 2.200-2/2001 que institui a infraestrutura de Chaves Públicas Brasileira - ICP-Brasil (BRASIL, 2001); a Lei nº 12.527/2011, Lei de Acesso à Informação (BRASIL, 2011); a Lei nº 12.737/2012, que tipificou crimes informáticos, também conhecida como Lei Carolina Dieckmann (BRASIL, 2012); o Decreto nº 7.962/2013 que regulamentou o Código de Defesa do Consumidor para dispor sobre a contratação no comércio eletrônico (BRASIL, 2013); a Lei nº 13.243/2016 que dispõe sobre estímulos ao desenvolvimento científico, à pesquisa, à capacitação científica e tecnológica e à inovação (BRASIL, 2016) e mais recentemente a Lei Geral de Proteção de Dados – LGPD,

Lei n.º 13.709/2018 (BRASIL, 2018). Esta lista não é exaustiva. E também é necessário apensar neste rol o sem número de preceitos presentes em leis gerais que tratam de assuntos de tecnologia.

Há certa controvérsia a respeito da necessidade de um sistema jurídico específico para regulação do ciberespaço, assim como há um ramo específico do direito para regular o mercado imobiliário ou o direito do consumidor. Há quem argumente que não há necessidade de um novo ramo do direito para regular as relações no mundo digital visto que há leis que podem ser aplicadas por analogia resolvendo as questões naquele contexto (EASTERBROOK, 1996, p. 207). De todo modo, é certo que mesmo todo aquele emaranhado de dispositivos legais não dá conta de abarcar todas situações que envolvem questões tecnológicas. No caso dos Contratos Inteligentes a questão transcende a complexidade em face de suas características que por vezes ofuscam os meios para aplicação das leis. Nesse sentido, quanto a eficácia das normas jurídicas não atinge seus objetivos, Lessig assevera que outros mecanismos, como as normas sociais ditadas pela sociedade, forças de mercado derivadas das leis de oferta e demanda e a arquitetura que molda os mundos físico e digital, podem ser utilizados para uma melhor regulação do contexto tecnológico (LESSIG, 2008, p. 2958).

3.3.2 Normas sociais

As normas sociais desempenham um papel fundamental na regulação das plataformas baseadas em *Blockchain*. A própria concepção desta tecnologia é resultado de um trabalho colaborativo que envolveu cientistas, acadêmicos e desenvolvedores em torno de uma grande comunidade que se valeu, e ainda se vale, da própria Internet para desenvolver seus projetos (ANDREESSEN, 2014). Outro fator fundamental para o desenvolvimento o desenvolvimento desta tecnologia também é originado em movimento importante de compartilhamento do desenvolvimento de softwares por colaboradores do mundo inteiro. Neste contexto, para formalizar a iniciativa de compartilhamento de softwares em código aberto, *a Free Software Foundation* – FSF criou a GPL – *General Public License* ou Licença Pública Geral (FSF, 2015), que fora citada na seção 1.1 desta Dissertação de Mestrado.

Considerando que a maioria dos projetos implementados com base na tecnologia *Blockchain* são construídos como software aberto baseados em licenças como a GPL ou dela derivadas, esta cultura de compartilhamento tornou-se um elemento decisivo para o desenvolvimento desta tecnologia a partir de padrões abertos. Assim sendo as especificações técnicas e protocolos abertos evitaram que cada projeto construísse sua própria plataforma dentro de uma especificação fechada e sem interoperabilidade, o que inviabilizaria o desenvolvimento de uma rede em escala global. Todo esse avanço tecnológico resultante é, portanto, originário no poder da colaboração, que cria um ciclo virtuoso de inovação na comunidade global quebrando o paradigma da centralização dos projetos. Qualquer indivíduo ou qualquer outro projeto pode examinar e trabalhar livremente com o código de outros projetos e trazê-lo para suas próprias implementações. "Esta é toda a proposta do software de código aberto. Isso significa que boas ideias podem gerar sementes mais rapidamente, tornar-se padronizadas por meio de iterações e serem melhoradas através do escrutínio e das contribuições de outras pessoas" (SWAN, 2015, p. 833-837).

Os desenvolvedores, na maioria das vezes voluntários, têm papel muito importante na criação e na manutenção dos protocolos que implementam a rede *Blockchain* e na especificação das linguagens de programação nas quais os Contratos Inteligentes são escritos. É normal que os desenvolvedores se organizem em tornos de projetos que os atraem por desafios, muitas vezes intelectuais. É o caso de Vitalin Buterik que encabeça o projeto da Ethereum, uma das primeiras implementações utilizadas para implementação de plataformas de Contratos Inteligentes (ANTONOPOULOS; WOOD, 2018, p. 654).

Os mineradores, por sua vez, compõem outro grupo social que tem grande relevância na organização que sustenta os Contratos Inteligentes. A validação e a introdução das informações e das transações das cláusulas que compõem o contrato passam pelos mineradores que os introduzem na *Blockchain* conforme os protocolos daquela cadeia de blocos. Estes protocolos precisam ser seguidos para manter o padrão e possibilitar a escalabilidade da rede. O próprio Nick Szabo enaltece a relevância da comunidade manter a integridade dos protocolos que sustentam as redes *Blockchain*, por meio de tomada de decisão descentralizada entre os especialistas na tecnologia, orquestrada pela Internet (SZABO, 2017).

Este sentimento social de pertencimento a um projeto por meio de colaboração tem força vinculante sobre membros da comunidade que desenvolvem as aplicações baseadas na tecnologia *Blockchain*, dentre elas os Contratos Inteligentes. Porém não se pode ignorar que aconteceram casos nos quais a comunidade se dividiu em relação à algum ponto polêmico e foram criadas novas versões dos protocolos conhecidas como *forks*[20].

Dentre vários casos, pode-se ilustrar este fenômeno com o que ocorreu com o protocolo da criptomoeda *Bitcoin* (BTC) que foi dividida e gerou o *Bitcoin Cash* (BCH). No caso da divisão da comunidade do projeto Bitcoin, em apertada síntese, pode-se dizer que uma parte da comunidade original queria mudar a estrutura da *Blockchain* para que aquela criptomoeda fosse mais atrativa em termos de moeda para circulação do que um ativo para investimento, mas outra parte da comunidade, mais conservadora, queria manter a estrutura da maneira original, deixando que o algoritmo fosse evoluindo conforme planejado no início da implantação da criptomoeda *Bitcoin* (BTC) e que o uso da criptomoeda fosse decidido pelo próprio mercado. Como não houve consenso entre estes dois grupos antagônicos, houve a cisão da comunidade e nasceu uma criptomoeda chamada *Bitcoin Cash* (BCH) (POPPER, 2017).

Nem mesmo a especificação flexível do protocolo *Ethereum* foi suficiente para evitar que a sua comunidade se dividisse ocasionando a cisão do protocolo original *Ethereum* (ETH), gerando o *Ethereum Classic* (ETC). Este *fork* aconteceu depois após um *cracker* roubar cerca de 50 milhões de dólares em Ether (unidade de troca do Ethereum) de um fundo da The DAO, uma organização autônoma descentralizada digital construída utilizando a *Blockchain* do *Ethereum* (PEARSON, 2016). Parte da comunidade em torno do projeto da Ethereum queria mudar o protocolo da cadeia *Blockchain* para devolver os fundos desviados para aqueles que foram lesados e, por outro lado, parte da comunidade tinha uma postura mais dogmática ao apoiar a imutabilidade da *Blockchain* – estes criaram um *Blockchain* derivativo chamado "*Ethereum Classic*" (ETC).

[20] Em engenharia de software, uma bifurcação ou ramificação (em inglês: *fork*) acontece quando um desenvolvedor (ou um grupo de desenvolvedores) inicia um projeto independente com base no código de um projeto já existente, ou seja, quando um software é desenvolvido com base em outro, já existente, sem a descontinuidade deste último. Fonte: https://pt.wikipedia.org/wiki/Bifurcação_(desenvolvimento_de_software). Acesso em : 15 fev. 2019.

Estes exemplos ilustram que mesmo a imutabilidade da *Blockchain* pode ser relativizada em face à acontecimentos que podem alterar os planos das comunidades que mantém ativos os projetos nela construídos. O interessante é que mesmo depois de criadas novas plataformas derivadas das plataformas originais, estas podem continuar ativas e, desta forma, as informações e os Contratos Inteligentes nelas implantados continuam em produção.

Nesta seara da regulação pelas normas sociais, os governos podem se utilizar do seu poder de criar regulamentos, incentivos para utilizar a força de convencimento para induzir o comportamento social, inclusive promovendo políticas públicas que incentivem (ou desmotivem) o uso desta tecnologia (DE FILIPPI; WRIGHT, 2018, p. 3640).

3.3.3 Forças de Mercado

Há também uma forma de regulação imposta pelo mercado. Os instrumentos desta regulação são operados por meio da lei da oferta e da procura, da escassez, da busca do lucro. O mercado apresenta um conjunto distinto de restrições sobre o comportamento individual e coletivo. Estabelece uma terceira faixa de restrição no comportamento (LESSIG, 2008, p. 663).

Em se tratando dos Contratos Inteligentes, um dos pontos nos quais as forças de mercado opera de forma mais notável é a questão dos mineradores que arcam com os custos da infraestrutura computacional, incluindo elevados gastos com energia elétrica, para realizar complexos cálculos com o objetivo de criar blocos válidos em uma cadeia *Blockchain*, blocos estes que serão utilizados pelas plataformas para armazenar informações e executar os comandos de software que compõem os referidos Contratos Inteligentes. Ora, estes mineradores trabalham com interesse nos incentivos que o protocolo da respectiva cadeia *Blockchain* lhes promete por meio de micropagamentos em criptomoedas daquela plataforma realizados aos nodos dos mineradores que validam as transações e as submetem à gravação na *Blockchain* subjacente que dá sustentação àquele Contrato Inteligente. Considerando, então, que as redes dependem de mineradores para validade e inserir blocos na cadeia da *Blockchain* e que estes mineradores trabalham sob motivação de um sistema de incentivos, estes incentivos podem ser afetados por políticas de taxação dos insumos necessários para a sustentação da tecnologia *Blockchain* (equipamento,

servidores, *links* de internet, *chips* de alta capacidade, energia elétrica, etc.), ou ainda, o endurecimento da regulação sobre a circulação destas criptomoedas afeta frontalmente o desenvolvimento e a sustentação da rede de nodos das *Blockchains* (DE FILIPPI, WRIGHT, 2018, p. 3482).

E o efeito cascata se propaga: se o número de minerados em uma *Blockchain* pública for muito influenciado por ações governamentais, há possibilidade de redução da quantidade destes atores e, com um número muito reduzido, aumenta o risco de um possível ataque aos nodos visto que, em menor número, torna-se mais fácil a manipulação do consenso quando da validação dos blocos.

Se no início da expansão da tecnologia *Blockchain* havia uma expectativa da criação de rede igualitária que sustentasse o consenso por meio do poder computacional oferecido pelos próprios usuários, este idealismo vem sendo esmaecido devido ao grau de centralização dos nodos de mineração de novos blocos para a *Blockchain*. Um usuário individual não consegue concorrer com os "*pools* de mineração"[21] centralizados que agregam os recursos computacionais de várias máquinas para aumentar a probabilidade de receber uma recompensa em bloco. Hoje, o grau de centralização é gritante - quatro pools de mineração controlam juntos mais de 50% do *Blockchain* do Bitcoin e dois pools de mineração controlam mais de 50% do *Blockchain Ethereum*. Esses pools de mineração poderiam funcionar juntos ou conspirar para bloquear uma *Blockchain* (DE FILIPPI, WRIGHT, 2018, p. 3501).

Um dos pilares fundamentais dos Contratos Inteligentes reside na confiança das partes que a estrutura tecnológica não vai falhar ou ser manipulada. No caso das *Blockchain* públicas, a concentração dos mineradores pode ser um percalço que solapa esta confiança. Este cenário de centralização dos atores que sustentam as *Blockchain* públicas gera um clima de incerteza que abala a confiança na promessa de inviolabilidade e segurança desta tecnologia, ao menos no seu modo de operação por consenso por meio de "prova de trabalho" de mineradores voluntários. Há, então, uma tendência de migração

[21] *Pools* de mineração são uma forma de os mineradores agregarem seus recursos para criar novos blocos em uma *Blockchain*, recebendo como pagamento frações de criptomoedas daquela plataforma, enquanto dividem a recompensa de acordo com a quantidade de esforço que cada um contribuiu. É possível acompanhar a dinâmica desse mercado por meio do sites Blockchain.info, "Distribuição de Hashrate", https://blockchain.info/pools; Etherscan, "Ethereum Top 25 Miners por Blocos", https://etherscan.io/stat/miner?range=7&blocktype=blocks.

de várias organizações para *Blockchains* privadas e permissionadas (conceito apresentado no item 1.5 deste trabalho), nas quais o controle fica compartilhado por um consórcio limitado de participantes (LEMIEUX *et. al*, 2018, p. 30).

Porém, para utilizar uma *Blockchain* permissionada com a mesma capacidade computacional de uma *Blockchain* pública seria necessário construir parcerias com diversas instituições interessadas em participar na rede como um nodo, inviabilizando uma prova de conceito realizada em pouco tempo. Outro problema deste modelo resulta que, em uma rede permissionada com poucos nodos, há maior possibilidade de conluio entre os nodos da rede no momento da execução do algoritmo de consenso (JUNIOR *et. al*, 2018, p .4).

3.3.4 Arquitetura tecnológica

É possível regular o ciberespaço por meio de controle na arquitetura dos componentes de hardware e de software que compõem as interfaces pelas quais os usuários acessam e utilizam os recursos tecnológicos daquele ambiente. O código, software, arquitetura e protocolos definem estas interfaces, que são selecionados pelos criadores de código. Eles controlam a conduta dos usuários ao tornar comportamento possíveis ou impossíveis. Assim, nos primórdios do desenvolvimento da Internet, havia uma grande expectativa que sua arquitetura descentralizada levaria à desintermediação generalizada e à remoção de todos os intermediários. Porém, ao contrário do que se esperava, a concentração dos provedores de acesso, mecanismos de busca e prestadores de serviços desvirtuou aquela pretensão libertária (LESSIG, 2008, p. 125).

No caso da tecnologia *Blockchain*, também se pode observar a mesma tendência frustrante. Os usuários não acessam diretamente a *Blockchain*, portanto, no caso dos Contratos Inteligentes, há necessidade de uma plataforma a ser utilizada para programar e executar as cláusulas programadas em software. Como nem todos os serviços implementados em uma cadeia *Blockchain* são completamente autônomos, é necessária uma plataforma, normalmente oferecida por um site ou por um aplicativo em um *smartphone* para que sejam realizadas as operações que, posteriormente serão gravadas em uma *Blockchain*. Somente a partir deste momento a informação resta eternizada na *Blockchain* e pode ser acessada para confirmar aquela operação existiu mesmo, sua data e hora e outras

informações registradas. Deste modo, muito se depende das empresas de tecnologia, sistemas operacionais, linguagens de programação e desenvolvedores de plataformas.

Em um primeiro momento poderia parecer que os governos iriam perder o controle das operações realizadas na rede compostos pelos nodos da *Blockchain*, mas isso pode ser decepcionante, visto que os governos podem editar leis que influenciem os comportamentos daqueles que fornecem os recursos para que aquela tecnologia possa se desenvolver e operar eficientemente. Apesar de toda empolgação, em última análise os Contratos Inteligentes dependem substancialmente dos dispositivos computacionais conectados à arquitetura da Internet.

Uma das formas pouco elegantes, mas eficiente, é a possibilidade de instituições como governos e grandes corporações, imporem a implementação de mecanismos de controle oculto, conhecidos pelo jargão técnico *backdoor*, que em português significa, literalmente, porta-dos-fundos. Trata-se de um acesso oculto à percepção dos usuários que traz grande poder àquelas instituições de tal modo que podem ter conhecimento do que ocorre e lhes dá poder de desabilitar Contratos Inteligentes autônomos ou suspender um aplicativo baseado em *Blockchain* que não esteja em conformidade com a lei ou com seus interesses (DE FILIPPI, WRIGHT, 2018, p. 3519).

Todavia, o efeito colateral de implantar *backdoors* nos Contratos Inteligentes traz um gravíssimo efeito colateral. Ao mesmo tempo que os fabricantes e instituições podem fazer acesso a esta porta-dos-fundos para ter controle sobre as operações, abre-se uma brecha para que qualquer um, incluindo aqueles com interesses escusos, que tenha acesso a esta via, possa ter total acesso às informações e transações. Seria como deixar a chave da porta embaixo do capacho de entrada (ABELLSON *et al*, 2015, p. 24-26).

Na década de 1990, o governo americano tentou impor aos fabricantes de chips que implementassem uma funcionalidade para que fosse possível que as agências governamentais pudessem descriptografar informações. O projeto, além de socialmente antipático e polêmico, resultou na descoberta de inúmeras brechas de segurança que poderiam ser exploradas por atacantes mal-intencionados e o projeto acabou sendo descontinuado (LEVY, 1994). Portanto, a implementação deste tipo de mecanismo na tecnologia dos Contratos Inteligentes resulta em um enfraquecimento dos benefícios em termos de

autonomia, inviolabilidade e resiliência, ao mesmo passo que suscita vulnerabilidades e, consequentemente, afeta a segurança e a confiança.

Outra forma de regulação por meio de limitações aos contornos da arquitetura da tecnologia foi percebida quando da pressão para que os fabricantes de sistemas operacionais que praticamente dominam o mercado global (Google Android, Apple iOS e Microsoft Windows) diminuíssem a eficiência dos protocolos de criptografia em seus sistemas, ideia proposta pelo então primeiro ministro britânico David Cameron, com o intuito de possibilitar ao estado a quebra de sigilo de comunicação de suspeitos alvo de investigação policial (THE GUARDIAN, 2015). Esta medida é muito controversa pois, além de caracterizar abuso de poder ao violar a privacidade dos cidadãos, apresenta efeitos colaterais para as corporações e para os próprios governos que precisam destes protocolos de criptografia para manter a segurança dos seus sistemas. Felizmente esta iniciativa acabou por não prosperar.

3.4 CONTRATOS INTELIGENTES COMO INSTRUMENTO DE CONFIANÇA E TRANSPARÊNCIA

A regulamentação da tecnologia é uma tarefa inglória para qualquer governo. A velocidade da evolução da tecnologia é assombrosamente maior do que a capacidade legislativa de qualquer ente estatal. Mesmo os mecanismos apresentados na seção anterior, sejam considerados individualmente ou combinados entre si, não são capazes de dar conta de prever todas as situações. Ao passo que as entidades estatais se deparam realizando um trabalho de Sísifo[22], desperta-se a consciência para uma possibilidade de utilizar a tecnologia *Blockchain* e as aplicações dela derivadas, neste contexto os Contratos Inteligentes, como aliados na consecução da aplicação de suas próprias leis e regulamentos, tal como já ocorre com o uso da Internet e de outras tecnologias digitais que se tornam instrumentos para estabelecer seu próprio sistema de regras e regulamentos,

[22] A expressão "trabalho de Sísifo" tem origem na mitologia grega na qual conta-se que Sísifo enganou os deuses várias vezes, fugindo da morte, e por isso despertou a ira daqueles, sendo condenado a passar a eternidade empurrando uma pedra até o cume de uma montanha. No entanto, sempre que a pedra estava prestes a chegar ao seu objetivo, rolava montanha abaixo e Sísifo tinha que voltar a executar o trabalho todo novamente. Por isso quando há uma tarefa interminável, cita-se esta expressão (SANTOS, 2015, p. 1090).

implementados usando autoexecução por meio de sistemas baseados em código computacional (DE FILIPPI; WRIGHT, 2018, p. 3762).

Uma expressiva gama de provisões legais e contratuais pode ser traduzida em regras simples e determinísticas implementadas por meio de software e executadas automaticamente em uma rede *Blockchain*, promovendo transparência aos atos públicos por meio de registros invioláveis e amplamente distribuídos na rede de nodos, o que seria um remédio muito eficiente para o combate da corrupção. Nesse sentido afirma Ronaldo Lemos que a tecnologia *Blockchain* pode ser usada também no setor público como ferramenta anticorrupção: "É como um gigantesco cartório, aberto e gratuito, capaz de registrar e dar transparência perpétua para qualquer tipo de operação" (FOLHA DE SÃO PAULO, 2016).

Uma das aplicações interessantes de aplicação da tecnologia *Blockchain* e, em particular, dos Contratos Inteligentes, é sua aplicação para a administração da conduta das pessoas em um sentido até mais eficiente do que a própria lei. No caso desta, é possível ao agente a ela submetido sopesar os incentivos e punições que lhe serão atribuídos, respectivamente, ao cumprir ou não cumprir determinada norma legal, decidindo *ex post* qual será sua conduta. Por outro lado, no caso dos Contratos Inteligentes, as partes são vinculadas às suas cláusulas autoexecutáveis e não tem outra saída senão arcar com o cumprimento que fora estabelecido e programado em software de forma determinística.

É tecnicamente possível que os Contratos Inteligentes sejam programados para conter os comandos previstos em leis e regulamentos, pois notadamente percebe-se que os regulamentos implementados por sistemas de tecnologia, cada vez mais, estão assumindo o mesmo papel e funcionalidade que as regras legais (DE FILIPPI; HASSAN, 2016, p. 12). Também nesse mesmo sentido, Reindenberg desenvolveu o conceito da *Lex Informatica*[23] que trata-se de um sistema normativo alternativo que consiste em um conjunto particular de regras e normas consuetudinárias derivadas das características técnicas de várias plataformas online que que determinam o que pode ou não ser feito e acaba

[23] A expressão *Lex Informatica* é inspirada na expressão *Lex Mercatoria,* um sistema estabelecido de forma voluntária pelos comerciantes dos tempos medievais que precisam realizar negócios em jurisdições de diversos reinos sem necessidade da imposição dos soberanos daquela época, os quais, por vezes, evitavam entrar em discussão e conflitos com outros reinos por motivos comerciais. Com o passar dos tempos, estes costumes e boas práticas foram sendo incorporados no corpo de leis do comércio internacional. (MARRELLA; YOO, 2009, p 811).

sendo aplicado a todos os usuários e se interlaçando com os ordenamentos locais. Da mesma forma os negócios jurídicos podem ser programados como componentes de software, também as leis e os regulamentos podem ser implementados desta forma, em especial aqueles que possuem parâmetros verificáveis de forma objetiva. Ao implementar as regrais legais em sistemas baseados em software, os governos podem assegurar uma maior conformidade legal para os ordenamentos, planejando *ex-ante* a forma como as regras serão aplicadas e reduzindo a incerteza a respeito da interpretação ou aplicação das regras. Isso porque, ao codificar regras em um sistema de software, é empregada linguagem de computador, muito mais precisa do que a linguagem humana, não deixando espaço para interpretações ambíguas (REIDENBERG, 1997, p. 553-555).

Situando o conceito da *Lex Informatica* dentro do contexto atual em que se encontra a tecnologia *Blockchain* e os Contratos Inteligentes, é possível fazer uma referência direta com a Teoria da *Lex Cryptographia* apresentada por Aaron Wright e Primavera De Fillippi. Esta teoria apresenta um modelo de governança privada e também estatal por meio da criação de organizações descentralizadas e potencialmente autônomas controladas por um conjunto de regras regidas por meio de Contratos Inteligentes autoexecutáveis escritos em *Blockchain*. Este cenário, segundo os autores desta teoria, tem o potencial de se tornar um novo sistema de administração de normas na sociedade a ser construído nos pilares da confiança e da transparência (DE FILIPPI; WRIGHT, 2015, p. 48).

A autoexecução das cláusulas quando determinada condição programada *ex ante* nos Contratos Inteligentes é satisfeita é um importante atributo em favor da desburocratização. Naturalmente a programação destas cláusulas será um trabalho extremamente exaustivo pois, como já apresentado neste trabalho, as linguagens de computador em que são programados os Contratos Inteligentes são determinísticas e não tem margem para flexibilizar a interpretação como ocorre com as linguagens naturais das pessoas. Em um primeiro momento, esta limitação pode se constituir em um obstáculo para a larga escala da construção da *Lex cryptografia* da forma como propõem De Filippi e Wright, porém a galopante evolução do poder computacional pode possibilitar a consolidação da tecnologia da Inteligência Artificial, em que os algoritmos computacionais irão se aproximar cada vez mais da linguagem humana.

Deixando um pouco de lado este exercício de futurologia, pode-se voltar ao estudo de alguns modelos teóricos e práticos que servem para ilustrar como a tecnologia *Blockchain* e os Contratos Inteligentes podem colaborar, de imediato, na construção de organizações mais transparentes e confiáveis. Serão apresentados dois casos de uso em que os Contratos Inteligentes se encaixam com perfeição.

3.4.1 Promovendo a transparência na administração pública

A participação ativa dos cidadãos é fundamental para a construção e para a manutenção de uma sociedade democrática dentro do Estado de Direito. Para que os cidadãos possam participar de forma eficiente é necessário que seja garantido o direito à informação por meio da transparência dos atos dos seus representantes (MARTINS, 2014). Esta garantia encontra guarida na Constituição Federal por meio do direito de acesso à informação pública (art. 5º, XXXIII, art. 37, art. 216, § 2º) que tutela o acesso a informações constantes nos registros do Estado (BRASIL, 1988). Também se encontra regulamentação própria, nesse sentido, na Lei de Acesso à Informação, Lei nº 12.527/2011, que tem como mister regulamentar a publicidade das informações dos atos dos entes estatais e seus responsáveis e tutelar o direito à informação pública (BRASIL, 2011).

O desafio, então, é viabilizar ao cidadão meios para a efetivação do seu direito positivado estabelecido. Não se trata de tarefa fácil tornar transparentes os atos dos entes estatais. É necessário comprometimento do administrador e um esforço do poder público para seja instrumentalizado aquilo que se encontra previsto em lei, com objetivo de divulgar as despesas realizadas pelos órgãos e entidades da administração pública, informações sobre execução orçamentária, licitações, contratações, convênios, diárias e passagens, entre outros. Atualmente a consecução do objetivo de transparência pública já se apresenta por meio de portais da transparência disponíveis na Internet que constituem um caminho para a viabilização das informações públicas por meio de uma página na Internet do órgão público, Federal, Estadual ou Municipal, destinada a divulgar, pela Internet, as informações referentes aos atos administrativos dos órgãos da Administração Pública, dados e demonstrativos sobre a execução orçamentária de cada exercício fiscal, nos termos da Lei de Responsabilidade Fiscal – Lei Complementar nº 101/2000 (BRASIL, 2000), bem como informações sobre desembolso com fornecedores em suas diversas modalidades (SÁ, 2014).

Nesse sentido, os Contratos Inteligentes podem desempenhar papel ímpar para a automação da coleta e validação das informações produzidas pelos diversos entes estatais. Ao traduzir os preceitos estabelecidos nas respectivas leis que promovem a transparência em um Contrato Inteligente e exigindo que os entes estatais interajam com esses Contratos Inteligentes ou as incorporem diretamente em seus sistemas de informação locais, torna-se possível automatizar a coleta das informações de forma online, instantânea ao tempo que ocorrem, dispensando a necessidade de envio de lotes de informações produzidas pelos mais diversos sistemas, desintegrados e incompatíveis (SWAN, 2015, p. 1474).

Considerando que os Contratos Inteligentes são replicados de forma distribuída e redundante na rede *Blockchain* na qual são armazenados e executados e que não podem ser alterados unilateralmente por uma única parte, cria-se um ambiente seguro garantindo a conformidade com os padrões legais previamente estabelecidos. Não mais é necessário confiar nos sistemas locais centralizados de cada um dos entes que compõem administração pública. Com a validação das informações pelas cadeias de consenso é possível garantir que publicou determinada informação em determinada data e hora, com precisão e segurança. Se necessária alguma retificação posterior, nova transação deve ser gerada, validada e registrada de forma permanente. Deste modo, tanto a informação prévia, bem como a retificação ficam registradas de forma indelével, formando um histórico confiável. Isso torna possível alcançar uma nova forma de responsabilização técnica – que é ditada pela tecnologia e que é menos dependente da aplicação *ex post* tradicional (DE FILIPPI; WRIGHT, 2018, p. 3837).

Outro ponto relevante aperfeiçoado por este modelo é automação de auditorias, promovendo a credibilidade na transparência das informações. Considerando que as informações coletadas são validadas, registradas e imediatamente disponíveis em uma *Blockchain*, as auditorias também podem ser realizadas por outros Contratos Inteligentes programados para tal finalidade. Como os softwares destes Contratos Inteligentes são abertos, eles também podem ser auditados pela própria sociedade pois estão disponíveis para o escrutínio de pesquisadores e de organizações não governamentais que trabalham em prol da fiscalização da transparência governamental.

3.4.2 Construindo confiança no uso dos recursos públicos

Os benefícios propiciados pelos Contratos Inteligentes em prol do uso racional e probo dos recursos públicos também podem ser percebidos em projetos já em execução à época em que se realiza esta pesquisa. Exemplo disso são as iniciativas implementadas em *Blockchain* para rastrear e tornar públicos os financiamentos de projetos que se valem de recursos públicos.

O Banco Nacional de Desenvolvimento Econômico e Social (BNDES) está trabalhando em algumas frentes. Há um projeto conhecido como TrueBudget, desenvolvido pelo BNDES em parceria com o banco de desenvolvimento estatal alemão KfW Development Bank. Este projeto será desenvolvido em uma *Blockchain* privada em que somente instituições convidadas oficialmente poderão ter acesso às informações e aos Contratos Inteligentes nela implementados. O objetivo deste projeto é bastante específico e visa rastrear as doações de recursos para o Fundo Amazônia cuja procedência de recurso é majoritariamente da Noruega e Alemanha (MARY, 2018).

O BNDESToken é outro projeto que está sendo implementado em tecnologia *Blockchain* pelo BNDES. O projeto, que ainda está em projeto piloto, está sendo implementado na *Blockchain* pública Ethereum, já possui especificações técnicas de funcionalidades detalhadas e disponível no site do BNDES. Para sua implementação aberta uma consulta pública e proposto um concurso de inovação interno com mais de trezentos concorrentes (BNDES, 2018). Trata-se de um *token* lastreado no Real, moeda oficial do Brasil, análogo a um título de crédito para futuro recebimento do recurso, que vai servir para rastrear o uso dos financiamentos concedidos pelo BNDES. "Cada unidade do *BNDESToken* equivale a um Real (1:1). A cotação fixa é um modo simples de criar uma marcação na moeda nacional" (JUNIOR *et. al*, 2018, p. 2). Esta paridade significa que a emissão dos *tokens* não representa aumento da base monetária nacional, simplificando o processo e evitando conflitos regulatórios. A circulação deste *token* será restrita e controlada pelo BNDES para evitar a criação de uma "moeda paralela". Outra característica do projeto do BNDESToken é que, mesmo utilizando Ethereum, ele não está vinculado ao *Ether* – criptomoeda implementada por esta *Blockchain*, evitando a volatilidade e riscos cambiais de conversão da criptomoeda para Reais, custos com corretores (*exchanges*) e, por fim, também evitando potenciais conflitos regulatórios.

O projeto de *tokens* do BNDES utiliza a *Blockchain* pública do *Ethereum*, portanto, considerando que a *Blockchain* utilizada já prevê a implementação de Contratos Inteligentes de forma nativa, o BNDESToken pode utilizar todo o potencial desta tecnologia (JUNIOR *et al.*, 2018, p. 4). Sua especificação prevê que o cadastro de contas na plataforma deverá ser realizado por meio do certificado digital do e-CNPJ[24] da empresa que está obtendo o financiamento. Uma vez cadastrada no sistema, a empresa que recebeu o financiamento poderá pagar seus fornecedores com estes tokens, ou seja, estes fornecedores também precisam se cadastrar na plataforma do BNDESToken criando uma conta na *Blockchain* Ethereum, registrando o relacionamento entre o seu e-CNPJ e um endereço de carteira Ethereum pertencente àquela pessoa jurídica. Em que pese este procedimento desvia um tanto do conceito de pseudônimos oferecido pela tecnologia *Blockchain*, ele adere ao procedimento de conformidade (*compliance*) das regras de conhecimento de cliente (*Know Your Client – KYC,* em inglês).

Os fornecedores, por sua vez, poderão converter seus créditos em BNDESToken em moeda fiduciária, ou seja, Reais, junto ao BNDES. Ressalta-se que estes créditos são intransferíveis a terceiros, evitando a criação de um mercado paralelo. Uma vez que o ciclo daquele *token* esteja concluído e o mesmo tenha retornado ao banco no momento do resgate e da conversão em reais, aquele *token* será marcado como "queimado" e não poderá ser utilizado novamente.

Esta plataforma vai permitir que o BNDES possa rastrear com precisão onde estão gastos os recursos emprestados, garantindo transparência na gestão dos recursos públicos. Todo este processo será realizado por meio de Contratos Inteligentes programados na linguagem *Solidity* e armazenados e executados na cadeia *Blockchain* Ethereum. As regras de utilização dos recursos obtidos no financiamento concedido serão implementadas em um Contrato Inteligente que vai verificar, automaticamente, se as regras de solicitação de resgate foram atendidas – por exemplo, o *token* já passou pelo número mínimo de pessoas jurídicas necessários e a solicitação está dentro do prazo. Também será possível utilizar as chaves privadas utilizadas na *Blockchain* para que cada parte

[24] O Certificado Digital e-CNPJ é um documento eletrônico de identidade que garante a autenticidade dos emissores e destinatários de documentos e dados que trafegam na internet, bem como assegura a privacidade e a inviolabilidade destes. Trata-se de um tipo de certificado digital do governo mantido pelo ICP-Brasil – Infraestrutura de Chaves Públicas Brasileira. Disponível em: http://www.iti.gov.br/icp-brasil. Aceso em 17 fev. 2019.

contratante assine digitalmente as transações com segurança. Lembrando que as chaves privadas são vinculadas a contas na *Blockchain* que, no caso específico desta plataforma, são associadas como e-CNPJ daquela parte.

Deste modo será possível utilizar qualquer ferramenta pública disponível na Internet para consultar a *Blockchain* do Ethereum e verificar em tempo real, de forma transparente, os eventos dos contratos e suas as informações. A transparência obtida com esta solução torna-se também uma ferramenta de combate à corrupção, pois as informações da *Blockchain* podem ser acessadas em tempo real para saber, com precisão informações sobre onde, quando e com quem os recursos foram destinados. Elimina-se muito da burocracia e dos custos da prestação de contas. Instituições de fiscalização como o Tribunal de Contas da União, Tribunais de Contas estaduais, entidades representantes da sociedade e mesmo o cidadão individualmente, podem ter acesso à estas informações de forma prática, confiável e sem burocracia. Considerando-se que os ativos financeiros dos empréstimos em questão tornam-se ativos inteligentes, é possível programar mecanismos que rastreiam a cadeia *Blockchain* para analisar os dados dos contratos de empréstimos e fornecer relatórios analíticos em tempo real dos recursos públicos.

3.4.3 Riscos do uso de Contratos Inteligentes na aplicação das leis

Se de um lado a implementação de soluções com a tecnologia dos Contratos Inteligentes proporciona muitos benefícios, de outro lado não se pode ignorar as armadilhas que podem ser criadas pelo seu uso indiscriminado. É necessário, portanto, ponderar sobre usos distorcidos, abusos e, mesmo problemas acidentais da tradução dos preceitos legais para código computacional a ser executado sumariamente em uma *Blockchain*.

Em um primeiro plano já é necessário rememorar que não são todos os casos de leis que podem ser transcritos para software. O estágio atual das linguagens de computador não proporciona a flexibilidade inerente do texto produzido pelo legislador, que por meio de cláusulas abertas consegue permitir que o intérprete da lei possa albergar situações que não eram possíveis de serem previstas *ex ante* ao momento da criação daqueles preceitos legais. Nem mesmo considerando o contexto pátrio em que há predominância do Direito positivo seria possível traduzir todo o ordenamento jurídico na forma de

software. Em suma, o atual desenho dos Contratos Inteligentes não é adequado para implementar provisões legais abertas (DE FILIPPI; WRIGHT, 2018, p. 3898).

O potencial de automação dos Contratos Inteligentes combinado com tecnologias de armazenamento de dados em larga escala, conhecidas como *Big Data*, pode resultar em uma impressionante e perfeita personalização da aplicação das leis. Todavia, isto pode conduzir a exageros como acontece no caso dos algoritmos que produzem *profiling* ou perfilamento dos dados que por meio de métodos e técnicas computacionais aplicados aos dados pessoais ou não dos usuários com o objetivo tanto para descobrir padrões quando para determinar interesses, comportamentos e tendências das pessoas (BOFF; FORTES; FREITAS, 2018, p. 162). Além de violar o direito constitucional à privacidade, neste caso a tecnologia pode gerar problemas como discriminação contra os cidadãos quem estariam sujeitos a regras personalizadas dependendo de sua identidade, perfil ou comportamento atual ou passado.

Em que pese a utilização de Contratos Inteligentes podem reduzir o custo para se obter a conformidade regulatória por meio da automação da execução das cláusulas previamente programadas, há uma preocupante limitação da liberdade do cidadão. No modelo atual, as regras legais dependem de um sistema de punição *ex post*. As pessoas são livres para decidir sozinhas se seguem essas regras, e aqueles que violarem a lei são punidos após o fato. A autoexecução de um Contrato Inteligente, por se tratar de um sistema programado *ex ante*, não deixa margem às pessoas, senão cumprirem o que foi programado no código e enviado para a *Blockchain*. Considerando que seria praticamente impossível prever todas as situações que podem se desenrolar, é muito provável que em alguns casos condutas que poderiam ser interpretadas como legais, acabam sendo punidas pela programação rígida e estrita codificada em software (DE FILIPPI; WRIGHT, 2018, p. 3941).

Por fim, mas não menos importante nem com presunção de esgotar o rol dos riscos a utilização de Contratos Inteligentes na aplicação das leis, alerta-se para a possibilidade de na redução da autonomia, autodeterminação pessoa e na própria liberdade, um direito fundamental de cada indivíduo, aproximando-se de um despotismo tecnológico que poderia resultar em um sistema totalitário que violaria direitos e garantias constitucionais. O início deste tipo de exagero inicia com uma singela governança algorítmica.

Nas palavras de De Fillipi e Wright (2015, pp. 41-43), governança algorítmica é um sistema normativo capaz de regular a sociedade de maneira mais eficiente, reduzindo os custos da aplicação da lei e permitindo um sistema personalizado de regras personalizado a todos os cidadãos, constantemente revisado com base nas preferências e perfis correspondentes. Em uma primeira vista, este é um cenário sedutor, mas este sistema pode eventualmente resultar em um sistema altamente prescritivo e determinístico; um sistema em que as pessoas são, de fato, livres para decidir o conjunto específico de regras a que desejam obedecer, mas - após a escolha - não podem mais se desviar dessas regras, na medida em que os Contratos Inteligentes são automaticamente impostos por o código subjacente da tecnologia, independentemente da vontade das partes, problemas podem surgir, por exemplo, quando Contratos Inteligentes desligam automaticamente o acesso à Internet, telefones celulares e outras distrações, a fim de garantir que cumpramos com nossos objetivos e critérios predefinidos.

3.5 ALGUMAS CONSIDERAÇÕES AO FINAL DO CAPÍTULO 3

Este capítulo propôs-se a realizar uma abordagem sobre as possíveis formas para a regulamentação dos Contratos Inteligentes em face da necessidade imprescindível de assegurar segurança jurídica diante da radical transformação que esta nova forma contratual suscita na celebração de negócios jurídicos. Foi, então, realizado o enquadramento da natureza jurídica dos Contratos Inteligentes como negócios jurídicos em sentido estrito, classificando-os como contratos eletrônicos intersistêmicos com equivalência funcional e jurídica aos contratos tradicionais, reconhecidos como válidos e eficazes no ordenamento brasileiro. Deste modo, a legislação posta no Brasil pertinente à regulamentação dos contratos eletrônicos e outros institutos legais que regulamentam o uso de tecnologia da informação também serve muito bem para regular os Contratos Inteligentes.

Ponto importante destacado neste capítulo foram as algumas especificidades dos Contratos Inteligentes que podem suscitar desafios jurídicos. Em que pese as plataformas de Contratos Inteligentes apresentem interfaces amigáveis com os seus usuários, a complexidade tecnológica imanente da tecnologia *Blockchain*, base para implementação dos Contratos Inteligentes, suscita desafios para que os operadores do Direito possam ter controle das consequências da translação das cláusulas contratuais codificadas em software,

visto que imutáveis e sem possibilidade de serem interrompidas depois de iniciada sua execução. Também a interpretação jurisdicional se torna complexa uma vez que a tecnologia *Blockchain* apresenta características técnicas que podem atropelar convenções como a identificação das partes e imputação de responsabilidades, visto que neste novo modelo as partes podem ser apresentar como agentes autônomos sem definição precisa de sua personalidade jurídica. Além do mais, os Contratos Inteligentes não têm um local físico, específico e determinado onde são armazenados e postos em execução, podendo estar dispostos de forma distribuída por um incalculável número nodos dentro de uma rede *Blockchain*, podendo operar em várias jurisdições ao mesmo tempo, com regramentos conflitantes entre si. Nesse sentido o estudo de Lawrence Lessig (2008) traz importantes contribuições para se entender que formas de regulação seriam realmente efetivas para propiciar segurança jurídica à implementação dos Contratos Inteligentes sem criar amarras que prendam a sua evolução tecnológica.

Por fim, ressalta-se a possibilidade de aplicação dos Contratos Inteligentes à serviço da própria governança, seja ela corporativa ou estatal. A sua capacidade de gerar confiança e transparência em todo do tipo de relação de negócios, possibilita a criação de instrumentos para promoção da transparência e combate à corrupção. Não se desconsideram certos efeitos colaterais e riscos que a tecnologia *Blockchain* precisa superar, ao contrário, procura-se revelar e identificar estes problemas para que possam ser mitigados em ordem do aproveitamento pleno do potencial dos Contratos Inteligentes.

CONCLUSÃO

As tecnologias inovadoras apresentam um ciclo de evolução que se inicia com uma grande euforia atraindo a atenção de toda uma comunidade. Este fenômeno, também conhecido como *hype*[25], pode ser perfeitamente observado no caso da tecnologia *Blockchain* em que se constata que o caminho para a consolidação desta tecnologia ainda não está concluído (GAERTNER, 2018).

A euforia inicial, naturalmente, tende a se dissipar no momento em que as promessas são frustradas e que projetos mirabolantes não encontram exequibilidade prática diante de entraves ainda sem solução e planos de negócios que se mostram inviáveis. Este processo de amadurecimento é natural e serve como filtro para uma seleção natural de projetos que tem possibilidade real de contribuição com a sociedade. Deste modo, conclui-se que é necessário, analisar com cautela a tecnologia e suas soluções para verificar se realmente a aplicação da tecnologia *Blockchain* é sensata.

Em que pese a tecnologia *Blockchain* ser apresentada como uma solução praticamente universal aplicável a qualquer tipo de negócio (KAAL; CALCATERRA, 2017, p. 3), há de se considerar que ainda há percalços a serem resolvidos. Nem todos os objetos do mundo analógico estão preparados para serem manipulados de forma digital. Mesmo com a acelerada evolução da Internet das Coisas, ainda não se tem uma universalização consolidada neste sentido (GAERTNER, 2013).

É notório que as criptomoedas, baseadas em tecnologia *Blockchain*, movimentam um volume financeiro considerável ao redor do mundo. Porém, há uma série de desafios importantes que precisam ser considerados tanto em termos tecnológicos, quanto em termos de modelos de negócio (EUROPEAN BANKING, 2014, p. 5). Também se ressalta que a regulamentação das criptomoedas ainda está longe de ser um consenso ao redor do mundo (PERKINS COIE, 2018).

Os Contratos Inteligentes, objeto de estudo desta dissertação, são fundamentalmente desenvolvidos sobre a estrutura tecnológica da *Blockchain* e, por conseguinte, se

[25] *Hype* é um fenômeno de grande euforia em torno de uma novidade que é amplamente anunciada e discutida na mídia e acaba por atrair o muito para atrair o interesse de todos (CAMBRIDGE DICTIONARY, Disponível em: https://dictionary.cambridge.org/pt/dicionario/ingles/hype. Acesso em 25 fev. 2019).

ressentem de todas as vicissitudes a que esta tecnologia está sujeita. Se as cadeias de blocos públicas descentralizadas que registram os dados de forma imutável, resgatam o ideal democrático da Internet em seus primórdios dispensando a necessidade de intermediários e distribuindo o poder de decisão entre os participantes da rede (MAY, 1988), há riscos significativos que precisam ser solucionados para uma plena utilização do potencial dos Contratos Inteligentes.

Riscos em face à confidencialidade e à privacidade dos dados e informações registradas em cadeias públicas de blocos precisam ser encarados, pois em um Contrato Inteligente há informações que precisam ser restritas somente entre as partes contratantes (DE FILIPPI; WRIGHT, 2018, p. 1645).

Problemas estruturais da tecnologia precisam ser enfrentados. A possibilidade de concentração dos nós por grandes grupos de mineradores (*pools* de mineração), descritos no item 2.5.3 desta Dissertação, fragiliza a confiança na *Blockchain* ao permitir que o consenso seja manipulado por conluios formados por poucos grupos que podem assumir facilmente mais da metade do poder de uma *Blockchain* e manipular o seu consenso (ETHEREUM WHITEPAPER, 2015).

Outra questão tormentosa que se apresenta em termos de infraestrutura dos Contratos Inteligentes trata-se da inflexibilidade de sua programação. Implementados a partir de linguagem de computador, de forma estrita e determinística, os Contratos Inteligentes necessitam de um grau de complexidade muito grande para poder albergar as cláusulas jurídicas escritas em linguagem natural. Denota-se que os Contratos Inteligentes podem se beneficiar da evolução da Inteligência Artificial para se tornarem efetivamente inteligentes, com a capacidade de interpretar os anseios das partes contratantes e produzir cláusulas contratuais que reflitam o seu "encontro de mentes" (SZABO, 1997).

Da complexidade de programação deriva-se outra implicação importante a ser considerada. Os Contratos Inteligentes não são codificados para leitura direta de observador humano. Em vez disso, eles são destinados à programação de computadores em uma rede de nós distribuída em uma rede *Blockchain* (KAAL; CALCATERRA, 2016, p. 8). Por seu turno, a complexidade tecnológica das linguagens de programação utilizadas na codificação dos Contratos Inteligentes em linguagem de máquina, substancialmente

diferente da linguagem humana, suscita um desafio no caso de necessidade de interpretação jurisdicional no momento de resolver conflitos entre as partes.

Somando-se a este óbice, a descentralização da execução dos Contratos Inteligentes que podem estar sendo executados em nós nas mais diversas jurisdições, visto que a tecnologia *Blockchain* não se limita a nenhuma fronteira (LAUSLAHTI et al., 2017, p. 6). Outro problema que ganha destaque é a possibilidade de as partes operarem por meio de pseudônimos, o que dificulta a identificação das partes e sua responsabilização, resultando até mesmo na possibilidade de aplicação desta tecnologia para implementação de atividades imorais, ilícitas e até mesmo criminosas.

Estas questões suscitam desafios que precisam ser deliberados também do ponto de vista do Direito, uma vez que a segurança jurídica é um dos pilares que sustenta toda sociedade (RASKIN, 2017, p. 340). Nesse sentido, o presente estudo dedicou-se a uma análise dos instrumentos jurídicos que contribuem na tutela dos Contratos Inteligentes. O ponto de partida foi a definição da natureza jurídica dos Contratos Inteligentes como negócios jurídicos em sentido estrito, com equivalência funcional aos contratos eletrônicos intersistêmicos, já recepcionados pelo ordenamento brasileiro como válidos e eficazes. Assim sendo, todos os instrumentos jurídicos presentes no ordenamento brasileiro que tutelam os contratos eletrônicos também podem ser aplicados na tutela dos Contratos Inteligentes naquelas áreas em que ambos instrumentos se equivalem, sendo apenas necessário tratar das especificidades peculiares dos Contratos Inteligentes.

Estas especificidades, derivadas da tecnologia *Blockchain*, na qual os Contratos Inteligentes são implementados, configuram-se na descentralização, imutabilidade e na autoexecução e foram examinadas nesta Dissertação em termos de suas implicações jurídicas.

No que toca à descentralização, característica que resulta no estabelecimento de confiança nas transações contratuais por meio do consenso entre os participantes da rede *Blockchain* e, consequente, dispensa intermediários, denota-se que seus efeitos não são absolutos, pois há casos nos quais o ordenamento brasileiro estabelece forma prevista em lei ou demanda que uma autoridade certifique o negócio jurídico em questão.

A questão da imutabilidade das informações e das transações em uma cadeia de blocos criptografados que sustenta os Contratos Inteligentes gera conflitos importantes com as leis de proteção de dados, no caso brasileiro com a LGPD – Lei Geral de Proteção de Dados (BRASIL, 2018).

Os benefícios da autoexecução dos Contratos Inteligentes encantam ao propor cumprimento automático e autônomo das cláusulas celebradas em um contrato. Porém os efeitos colaterais da impossibilidade de interromper os processos iniciados apresentam decorrências temerárias que são agravadas pela imaturidade da tecnologia. Inclusive há exemplos que ilustram casos reais em que grandes prejuízos foram verificados (PEARSON, 2016).

Em que pese existirem adversidades no campo jurídico a serem superadas para uma plena e pacífica consolidação dos Contratos Inteligentes como instrumentos para celebração de contratos, o seu potencial é muito precioso e merece ser considerado com especial atenção.

Os benefícios que se vislumbram na implementação desta tecnologia em prol de se estabelecer confiança e transparência nos negócios jurídicos são tão relevantes que justificam o investimento no desenvolvimento de mecanismos de regulação e o esforço dos operadores do Direito em adquirir habilidades e conhecimentos no campo das Tecnologias da Informação e Comunicação (TIC's) para encontrar um caminho para recepcionar os Contratos Inteligentes com segurança jurídica. Nesse sentido é louvável a iniciativa de programas de ensino em Direito que oferecem cadeiras para o estudo de TIC's de forma aplicada, que promovem a reflexão dos impactos dessas TIC's na sociedade e incentivam ponderações sobre seus impactos jurídicos. Por meio desta iniciativas, torna-se possível o diálogo multidisciplinar e a participação cooperativa entre profissionais do Direito e especialistas em Tecnologia da Informação e de outras áreas do conhecimento, para contribuir de forma significativa para a implementação de Contratos Inteligentes como instrumentos para otimizar e aperfeiçoar negócios jurídicos, reduzir divergências e promover mais agilidade ao mesmo tempo que proporcionam maior segurança jurídica para todos os envolvidos.

REFERÊNCIAS

ABELSON, Harold; ANDERSON, Ross; BELLOVIN, Steven M.; BENALOH, Josh; Blaze, Matt; DIFFIE, Whitfield; GILMORE, John; GREEN, Matthew; LANDAU, Susan; NEUMANN, Peter G.; RIVEST, Ronald L.; SCHILLER, Jeffrey I.; SCHNEIER, Bruce; SPECTER, Michael A.; WEITZNER, Daniel J. **Keys under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications**. *In*: Communications of the ACM 58, no. 10 (2015): 24–26. Disponível em: http://hdl.handle.net/1721.1/97690. Publicado em: 06 jul. 2015. Acesso em 26 fev. 2019.

ANDREESSEN, Marc. **Why Bitcoin Matters.** *In*: The New York Times, January 21, 2014. Disponível em: https://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/?_php=true&_type=blogs&_r=0. Publicado em 21 jan. 2014. Acesso em 26 fev. 2019.

ANTONOPOULOS, Andreas; WOOD, Gavin. **Mastering Ethereum**. O'Reilly Media. Edição do Kindle, 2018

ANTONOPOULOS, Andreas. **Mastering Bitcoin**. O'Reilly Media. Edição do Kindle, 2017.

ASSANGE, Julian et. al. **Cypherpunks : liberdade e o futuro da internet.** tradução Cristina Yamagami. - São Paulo : Boitempo, Edição do Kindle, 2013.

AZEVEDO, Antonio Junqueira, de. **Negócio jurídico: existência, validade e eficácia**. 4ª ed. atual. de acordo com o Código Civil (Lei n. 10.406, de 10-1-2002). São Paulo : Saraiva, 2002.

BARLOW, John Perry. **A declaration of the independence of cyberspace**. Disponível em: https://www.eff.org/cyberspace-independence . Publicado em 8 fev. 1996. Acesso em 26 fev. 2019.

BBVA Research. **Digital Economy Outlook**. Disponível em https://www.bbvaresearch.com/wp-content/uploads/2015/10/Digital_Economy_Outlook_Oct15_Cap1.pdf. Publicado em out. 2015. Acesso em 26 fev. 2019.

BCB, Banco Central do Brasil. **Distributed ledger technical research in Central Bank of Brazil. Positioning report**. Disponível em: https://www.bcb.gov.br/htms/public/microcredito/Distributed_ledger_technical_research_in_Central_Bank_of_Brazil.pdf. Publicado em: 31 ago. 2017. Acesso em 26 fev. 2019.

BENKLER, Yochai. **Networks of Power, Degrees of Freedom**. *In*: International Journal of Communication 5 (2011), 721–755. Disponível em: http://faculty.georgetown.edu/irvinem/theory/Benkler-Networks-Power-Freedom-2011.pdf. Publicado em 2011. Acesso em 26 fev. 2019.

BNDES, Site do Banco Nacional de Desenvolvimento Econômico e Social (BNDES). **Consultas Públicas 2018**. Disponível em: https://www.bndes.gov.br/wps/portal/site/home/transparencia/licitacoes-contratos/licitacoes/consultas-publicas/consultas-publicas-2018. Acesso em 26 fev. 2019.

BOFF, Salete Oro; FORTES, Vinícius Borges; FREITAS, Cinthia Obladen de Almendra. **Proteção de dados e privacidade: do direito às novas tecnologias na sociedade da informação**. Rio de Janeiro : Lumen Juris, 2018.

BRANDELLI, Leonardo. **Teoria Geral do Direito Notarial**, 2ª edição. Saraiva, 2007.

BRASIL. **Lei n.º 3.071, de 1º de janeiro de 1916**. Código Civil dos Estados Unidos do Brasil (revogado). Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L3071.htm. Acesso em 26 fev. 2019.

BRASIL. **Lei n.º 6.015, de 31 de dezembro de 1973**. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L6015compilada.htm. Acesso em 26 fev. 2019.

BRASIL. **Lei n.º 8.078, de 11 de setembro de 1990**. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L8078.htm. Acesso em 26 fev. 2019.

BRASIL. **Lei n.º 8.248, de 23 de outubro de 1991**. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L8248.htm. Acesso em 26 fev. 2019.

BRASIL. **Lei n.º 9.610, de 19 de fevereiro de 1998**. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9610.htm. Acesso em 26 fev. 2019.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em 26 fev. 2019.

BRASIL. **Lei complementar n.º 101, de 4 de maio de 2000**. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/LCP/Lcp101.htm. Acesso em 26 fev. 2019.

BRASIL. **Medida provisória n.º 2.200-2, de 24 de agosto de 2001**. Disponível em: http://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200-2.htm. Acesso em 26 fev. 2019.

BRASIL. **Lei n.º 10.406, de 10 de janeiro de 2002**. Código Civil Brasileiro. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/2002/L10406.htm. Acesso em 21 jan. 2019.

BRASIL. **Lei n.º 11.077, de 30 de dezembro de 2004**. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2004/Lei/L11077.htm. Acesso em 26 fev. 2019.

BRASIL. **Lei n.º 11.419, de 19 de dezembro de 2006**. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2006/Lei/L11419.htm. Acesso em 26 fev. 2019.

BRASIL. **Lei n.º 12.527, de 18 de novembro de 2011**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em 26 fev. 2019.

BRASIL. **Lei n.º 12.737, de 30 de novembro de 2012**. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm. Acesso em 26 fev. 2019.

BRASIL. **Decreto n.º 7.962, de 15 de março de 2013**. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Decreto/D7962.htm. Acesso em 26 fev. 2019.

BRASIL. **Lei n.º 12.965, de 23 de abril de 2014**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 26 fev. 2019.

BRASIL. **Lei n.º 13.105, de 16 de março de 2015**. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2015/Lei/L13105.htm. Acesso em 26 fev. 2019.

BRASIL. **Lei n.º 13.243, de 11 de janeiro de 2016**. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Lei/L13243.htm. Acesso em 26 fev. 2019.

BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018**. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em 26 fev. 2019.

CAMERON, James Ball. **Wants to ban encryption – He can say goodbye to digital Britain**. *In*: The Guardian. Disponível: http://www.theguardian.com/commentisfree/2015/jan/13/cameron-ban-encryption-digital-britain-online-shopping-banking-messaging-terror. Publicado em 15 jan. 2015. Acesso em 26 fev. 2019.

CAVEDON, Ricardo; FERREIRA, Heline Sivini; FREITAS, Cinthia Obladen de Almendra. **O meio ambiente digital sob a ótica da Teoria da Sociedade de Risco: os avanços da informática em debate**. *In*: Revista Direito Ambiental e sociedade, v. 5, n. 1, pp. 194-223, 2015

CHOI, Stephen J.; GULATI, Mitu. **Contract as Statute**. *In*: Michigan Law Review, pp 1129–1173. Disponível em https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1537&context=mlr. Publicado em 2006. Acesso em 26 fev. 2019.

CHRISTENSEN, Clayton. M.; RAYNOR, Michael. E.; MCDONALD, Rory. **What Is Disruptive Innovation?** *In*: Harvard Business Review. Disponível em: https://hbr.org/2015/12/what-is-disruptive-innovation. Publicado em dez 2015. Acesso em 26 fev. 2019.

CICCONI, Bruno B. Galli; STABILE, Victor Morandini. **Interoperabilidade na escrituração eletrônica de duplicatas por meio de solução em *Blockchain***. *In*: Laboratório de Inovações Financeiras Tecnológicas – LIFT. Disponível em https://www.liftlab.com.br/docs/LIFT_Resultado_2018_1.pdf. Publicado em 2018. Acesso em 26 fev. 2019.

COELHO, Fábio Ulhôa**. Curso de direito comercial: direito de empresa**. 7. ed. rev. e atual. São Paulo: Saraiva, 2007.

DE FILIPPI, Primavera; HASSAN, Samer. ***Blockchain* Technology as a Regulatory Technology: From Code Is Law to Law Is Code**. *In*: First Monday 21, no. 12. Disponível em: https://www.researchgate.net/publication/311447869_Blockchain_Technology_as_a_Regulatory_Technology_From_Code_is_Law_to_Law_is_Code. Publicado em: nov. 2016. Acesso em 26 fev. 2019.

DE FILIPPI, Primavera; WRIGHT, Aaron. ***Blockchain* and the Law**. Edição do Kindle. Harvard University Press, 2018.

DE FILIPPI, Primavera; WRIGHT, Aaron. ***Decentralized blockchain technology and the rise of lex cryptographia***. *In*: Social Science Research Network. Disponível em: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664. Publicado em: 20 mar. 2015. Acesso em 26 fev. 2019.

DINIZ, Maria Helena. **Curso de direito civil brasileiro: teoria das obrigações contratuais e extracontratuais**. 24ª. ed. rev., atual. e ampl. de acordo com a reforma do CPC e com o Projeto de Lei n. 276/2007. São Paulo: Saraiva, 2008.

DINIZ, Maria Helena. **Tratado Teórico e Prático dos Contratos**. 5º volume. São Paulo: Saraiva, 2002.

EL PAIS. **Os celulares espiam e transmitem nossas conversas, mesmo desligados**. Disponível em: https://brasil.elpais.com/brasil/2019/02/23/tecnologia/1550953521_057163.html. Publicado em 25 fev. 2019. Acesso em 14 abr. 2019.

e-ESTONIA (2016). ***Blockchain* and healthcare: the Estonian experience**. Disponível em: https://e-estonia.com/blockchain-healthcare-estonian-experience. Acesso em 26 fev. 2019.

e-ESTONIA (2018). **We have built a digital society and so can you**. Disponível em: https://e-estonia.com. Acesso em 26 fev. 2019.

EASTERBROOK, Frank H., **Cyberspace and the Law of the Horse**. *In*: University of Chigago Law School. Disponível em: https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=2147&context=journal_articles. Publicado em 1996. Acesso em 26 fev. 2019.

ESMA, The European Securities and Market Authority. **Discussion Paper: The Distributed Ledger Technology Applied to Securities Markets.** *In*: ESMA / 2016 / 773. Disponível em https://www.esma.europa.eu/sites/default/files/library/2016-773_dp_dlt.pdf. Publicado em 2 jun. 2016. Acesso em 26 fev. 2019.

ETHEREUM WHITEPAPER. **A Next-Generation Smart Contract and Decentralized Application Platform**. Disponível em: https://github.com/ethereum/wiki/wiki/White-Paper. Publicado em 10 dez. 2014. Acesso em 26 fev. 2019.

ETHEREUM WIKI, Site da. **Proof of Stake FAQs**. Disponível em: https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQs. Acesso em 26 fev. 2019.

EU *BLOCKCHAIN*. ***Blockchain* and the GDPR. Thematic Report**. Disponível em : https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf. Publicado em 16 out. 2018. Acesso em 26 fev. 2019.

EU GDPR. **2018 reform of EU data protection rules**. Disponível em: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en. Acesso em 26 fev. 2019.

EUROPEAN BANKING AUTHORITY, EBA. **EBA Opinion on virtual currencies.** EBA/Op/2014/08. Disponível em: https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf. Acesso em 02 jul. 2018.

EVANS, Philip; ARÉ, Lionel; FORTH, Patick; HARLÉ, Nicolas; PORTINCASO, Massimo. **O que fazer sobre o *Blockchain***. *In*: HSM Management, ed. n.º 121, mar 2017, pp. 20-24. São Paulo, 2017.

EZE, Peter; EZIOKWU, Tochukwu; OKPARA, Chinedu. **A Triplicate Smart Contract Model using Blockchain Technology**. *In:* Circulation in Computer Science – Special Issue Disruptive Computing, Cyber-Physical Systems (CPS), and Internet of Everything (IoE), pp:1-10, 2017. Disponível em https://www.researchgate.net/publication/317349621_A_Triplicate_Smart_Contract_Model_using_Blockchain_Technology/figures?lo=1&utm_source=google&utm_medium=organic. Publicado em jun. 2017. Acesso em 28 fev. 2019.

FOLHA DE SÃO PAULO. **Atacar a raiz da corrupção**, publicação de 1º de fevereiro de 2016. Disponível em http://www1.folha.uol.com.br/colunas/ronaldolemos/2016/02/1735283-atacar-a-raiz-da-corrupcao.shtml. Acesso em 26 fev. 2019.

FOTIOU, Nikos; POLYZOS, and George. ***Blockchain*-assisted information distribution for the Internet of Things**. *In:* Proceedings of the 2017 IEEE International Conference on Information Reuse and Integration, 2017. Disponível em: https://mm.aueb.gr/publications/2018-BC-EUCNC.pdf. Publicado em 2017. Acesso em 26 fev. 2019.

FRANÇA. **Code civil des Français : édition originale et seule officielle.- A Paris, de l'Imprimerie de la République, An XII 1804**. Disponível em: http://www.assemblee-nationale.fr/evenements/code-civil/cc1804-l3t03.pdf e http://www.assemblee-nationale.fr/evenements/code-civil-1804-1.asp. Acesso em 26 fev. 2019.

FSF, Site da Free Software Foundation. **GNU General Public License.** Disponível em: https://www.gnu.org/copyleft/gpl.html. Acesso em 26 fev. 2019.

GARCIA, Flúvio Cardinelle Oliveira. **Da validade jurídica dos contratos eletrônicos**. *In:* Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 9, n. 264. Disponível em: https://jus.com.br/artigos/4992. Publicado em 28 mar. 2004. Acesso em: 1 fev. 2019.

GARTNER, Site do. **Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020.** Disponível em: https://www.gartner.com/newsroom/id/2636073. Publicado em 12 dez. 2013. Acesso em 26 fev. 2019.

GAERTNER, Trends. **The Reality of *Blockchain***. Disponível em: https://www.gartner.com/smarterwithgartner/the-reality-of-blockchain/. Publicado em 16 out. 2018. Acesso em 26 fev. 2019

GDPO Situation Analysis. **Silk Road and Bitcoin**. Disponível em: https://www.swansea.ac.uk/media/GDPO%20SA%20silk%20rd%20rise%20again.pdf. Publicado em: dez. 2013. Acesso em 26 fev. 2019.

GLÓRIA, Luciano Ribeiro Tambasco. **Relações jurídicas privadas potencialmente vulneráveis na autoexecução de Contratos Inteligentes em plataformas *Blockchain***, *In*: Direito civil e tecnologia [Recurso eletrônico on-line] organização I Congresso de Tecnologias Aplicadas ao Direito – Belo Horizonte, 2017.

GOLDSMITH, Jack; WU, Tim. **Who controls the internet: illusions of a borderless world**. Oxford University Press, Inc., 2006.

GOMES, Delber Pinto. **Contratos *ex machina*: breves notas sobre a introdução da tecnologia *Blockchain* e Smart Contracts**. Disponível em: https://www.cije.up.pt/download-file/2274. Revista Electrónica de Direito N.º 3 (V. 17). Publicado em out. 2018. Acesso em 26 fev. 2019.

GOMES, Orlando. **Contratos**. 26ª edição. Rio de Janeiro: Forense, 2009

GUPTA, Manav. ***Blockchain* For Dummies, IBM Limited Edition**. New Jersey : Wiley & Sons, Inc. 2017

HANADA, Yuichi; HSIAO, Luke; LEVIS, Philip. **Smart Contracts for Machine-to-Machine Communication: Possibilities and Limitations**. Disponível em: https://arxiv.org/pdf/1806.00555.pdf. Publicado em 8 jan. 2019. Acesso em 26 fev. 2019.

HEAP, Imogen. ***Blockchain* pode ajudar músicos a ganhar dinheiro novamente**. *In:* Harvard Business Review Brasil. Disponível em http://hbrbr.uol.com.br/blockchain-pode-ajudar-musicos-ganhar-dinheiro. Publicado em: 10 ago. 2017. Acesso em 26 fev. 2019.

HUGHES, Eric. **A Cypherpunk's Manifesto**. Disponível em https://www.activism.net/cypherpunk/manifesto.html. Publicado em 9 mar. 1993. Acesso em 26 fev. 2019.

JORGE JUNIOR, Alberto Gosson. **Iniciação ao Negócio Jurídico**. Disponível em: http://dx.doi.org/10.15603/2176-1094/rcd.v1n1p9-34. Publicado em 2004. Acesso em 26 fev. 2019.

JUELS, Ari; KOSBA, Ahmed; SHI, Elaine. **The Ring of Gyges: Investigating the Future of Criminal Smart Contracts.** *In:* Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (New York: ACM, 2016), 283–295. Disponível em: http://www.arijuels.com/wp-content/uploads/2013/09/Gyges.pdf . Publicado em 2016. Acesso em 26 fev. 2019.

JÚNIOR, Gladstone Moisés Arantes; JR., José Nogueira D'Almeida; ONODERA, Marcio Teruo; MORENO, Suzana Mesquita de Borba Maranhão; ALMEIDA, Vanessa da Rocha Santos. BNDESToken: **Uma Proposta para Rastrear o Caminho de Recursos do BNDES**. In: WORKSHOP EM BLOCKCHAIN: TEORIA, TECNOLOGIAS E APLICAÇÕES (WBLOCKCHAIN_SBRC), 1., 2018, 1/2018. *In:* Anais do I Workshop em *Blockchain*: Teoria, Tecnologias e Aplicações (WBlockchain - SBRC 2018). Disponível em: http://portaldeconteudo.sbc.org.br/index.php/wblockchain/issue/view/148. Porto Alegre: Sociedade Brasileira de Computação, 2018. Acesso em 26 fev. 2019.

KAAL, Wulf A.; CALCATERRA, Craig. **Smart Contract Dispute Resolution—The Need for an Open Source *Blockchain* Platform Ecosystem**. https://medium.com/@wulfkaal/smart-contract-dispute-resolution-the-need-for-an-open-source-blockchain-platform-ecosystem-e6318610fdef. Publicado em 26 jun. 2016. Acesso em 26 fev. 2019.

KELLY, Sanja; COOK, Sarah. "**Freedom on the Net 2011: A Global Assessment of Internet and the Digital Media**". Disponível em: https://freedomhouse.org/sites/default/files/FOTN2011.pdf. Publicado em 18 abr. 2011. Acesso em 26 fev. 2019.

KfW Development Bank, Site. ***Blockchain* boosts effectiveness of development cooperation**. Disponível em: https://www.kfw.de/KfW-Group/Newsroom/Latest-News/Press-Releases/Pressemitteilungen-Details_426112.html. Publicado em 20 jul. 2017. Acesso em 26 fev. 2019.

KIM, Andrew; SNG, Daryl; YU Soyeon. **The Stateless Currency and the State: An Examination of the Feasibility of a State Attack on Bitcoin**. (2014), http://randomwalker.info/teaching/spring-2014-privacy-technologies/state-attack.pdf. Publicado em 13 mai. 2014. Acesso em 26 fev. 2019.

KOSBA, Ahmed; MILLER, Andrew; SHI, Elaine; WEN, Zikai; PAPAMANTHOU, Charalampos. **Hawk: The *Blockchain* Model of Cryptography and Privacy-Preserving Smart Contracts**. *In:* 2016 IEEE Symposium on Security and Privacy (SP), ed. Michel Locasto, Vitaly Shmatikov, and Ulfar Erlingsson (Piscataway, NJ: IEEE, 2016), 839–858. Disponível em: https://eprint.iacr.org/2015/675.pdf. Publicado em 2016. Acesso em 18 jan. 2019.

LAUSLAHTI, Kristian; MATTILA, Juri, SEPPÄLÄ Timo. **Smart Contracts – How will *Blockchain* Technology Affect Contractual Practices**. *In:* ETLA Reports nº 68, 2017. Disponível em: https://www.etla.fi/wp-content/uploads/ETLA-Raportit-Reports-68.pdf. Publicado em: 09 jan. 2017. Acesso em 26 fev. 2019.

LAWAND, Jorge José. **Teoria geral dos contratos eletrônicos**. São Paulo: Juarez de Oliveira, 2003.

LEAL, Sheila do Rocio Cercal Santos; EFING, Antônio Carlos. **Validade jurídica dos contratos eletrônicos via internet**. 2003. ix, 198 p. Dissertação (Mestrado) - Pontifícia Universidade Católica do Paraná, Curitiba, 2004.

LEMIEUX, Victoria; FLORES, Daniel; LACOMBE, Claudia. **Registro de transações imobiliárias em *Blockchain* no Brasil - Estudo de Caso 1**. Disponível em: https://www.researchgate.net/publication/322665300_Registro_de_transacoes_imobiliarias_em_*Blockchain*_no_Brasil_RCPLAC-01_-_Estudo_de_Caso_1/citations Publicado em jan. 2018. Acesso em 26 fev. 2019.

LESSIG, Lawrence. **Code: And Other Laws of Cyberspace, Version 2.0** (English Edition) [eBook Kindle]. Basic books. 2008.

LESSIG, Lawrence. **The New Chicago School**. *In:* The Journal of Legal Studies 27, no. S2, pp. 661-691. Disponível em https://doi.org/10.1086/468039. Publicado em jun, 1998. Acesso em 26 fev. 2019.

LEVY, Steven. **Battle of the Clipper Chip**. *In:* The New York Times Magazine. Disponível em: https://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html. Publicado em 12 jun. 1994. Acesso em 26 fev. 2019.

LIM, Cheng. **Smart Contracts: Bridging the Gap Between Expectation and Reality.** Disponível em: https://www.law.ox.ac.uk/business-law-blog/blog/2016/07/smart-contracts-bridging-gap-between-expectation-and-reality. Publicado em 11 jul. 2016. Acesso em 26 fev. 2019.

LINUX FOUNDATION. **Linux Foundation Unites Industry Leaders to Advance *Blockchain* Technology**. Disponível em https://www.linuxfoundation.org/press-release/2015/12/linux-foundation-unites-industry-leaders-to-advance-*blockchain*-technology/. Publicado em 17 dez. 2015. Acesso em 26 fev. 2019.

LÔBO, Paulo. **Direito Civil : contratos**. 3. ed. – São Paulo : Saraiva, 2017

MARRELLA, Fabrizio; YOO, Christopher S. **Is Open Source Software the New Lex Mercatoria?**. *In:* Faculty Scholarship at Penn Law, ed. 165. Disponível em: https://scholarship.law.upenn.edu/faculty_scholarship/165. Publicado em: 27 ago. 2007. Acesso em 26 fev. 2019.

MARTINS, Ricardo Marcondes. **Direito fundamental de acesso à informação**. A&C – Revista de Direito Administrativo & Constitucional, Belo Horizonte, ano 14, n. 56, p. 127-146, abr./jun. 2014.

MARY, 2018. **Tecnologia *Blockchain* será objeto de cooperação entre BNDES e KfW**. Disponível em: https://www.bndes.gov.br/wps/portal/site/home/imprensa/noticias/conteudo/tecnologia-*blockchain*-sera-objeto-de-cooperacao-entre-bndes-e-kfw. Publicado em 22 fev. 2018. Acesso em 26 fev. 2019.

MAY, Timothy. **The Crypto Anarchist Manifesto**. Disponível em https://www.activism.net/cypherpunk/crypto-anarchy.html. Publicado em 1988. Acesso em 26 fev. 2019.

MEIKLEJOHN, Sarah; POMAROLE, Marjori; JORDAN, Grant; LEVCHENKO, Kirill; MCCOY, Damon; VOELKER, Geoffrey M.; SAVAGE, Stefan. **A Fistful of Bitcoins: Characterizing payments among men with no names**. Disponível em https://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf. Publicado em 23 out. 2018. Acesso em 26 fev. 2019.

MODI, Ritesh. **Introduction to *Blockchain*, Ethereum and Smart Contracts. Disponível em** https://medium.com/coinmonks/https-medium-com-ritesh-modi-solidity-chapter1-63dfaff08a11. Publicado em 16 mai. 2018. Acesso em 26 fev. 2019.

MORGAN, Pamela. **Using *Blockchain* Technology to Prove Existence of a Document. Empowered Law**. http://empoweredlaw.wordpress.com/2014/03/11/using-*blockchain*-technology-to-prove-existence-of-a-document/. Publicado em 11 mar. 2014. Acesso em 26 fev. 2019.

NAKAMOTO, Satoshi. **Bitcoin: A Peer-to-Peer Electronic Cash System**, https://bitcoin.org/bitcoin.pdf. Publicado em out. 2009. Acesso em 26 fev. 2019.

NARAYANAN, Arvind; BONNEAU, Joseph; FELTEN, Edward; MILLER, Andrew; GOLDFEDER, Steven (2016): **Bitcoin and Cryptocurrency Technologies**; Draft, Feb 9, 2016. Disponível em: https://lopp.net/pdf/princeton_bitcoin_book.pdf. Publicado em 06 fev. 2016. Acesso em 26 fev. 2019.

ONU, Conselho dos Direitos Humanos. **Resolução A/HRC/20/L.13. Promoción, protección y disfrute de los derechos humanos en Internet**. Disponível em: http://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_20_L13.pdf. Publicado em 20 jun. 2012. Acesso em 26 fev. 2019.

PARCHEN, Charles Emmanuel; FREITAS, Cinthia Obladen Almendra; EFING, Antônio Carlos. **Computação em Nuvem e Aspectos Jurídicos da Segurança da Informação**. *In:* Revista Jurídica CESUMAR. Mestrado, v. 13, pp. 331-355. Disponível em: http://periodicos.unicesumar.edu.br/index.php/revjuridica/article/view/2705/1905. Publicado em jan. 2013. Acesso em 26 fev. 2019.

PEARSON, Jordan. **The Ethereum Hard Fork Spawned a Shaky Rebellion**. *In:* Motherboard. Disponível em: https://motherboard.vice.com/en_us/article/z43qb4/the-ethereum-hard-fork-spawned-a-shaky-rebellion-ethereum-classic-etc-eth. Publicado em 15 Mai 2017. Acesso em 26 fev. 2019.

PERKINS COIE, Site. **Virtual Currencies: International Actions and Regulations**. Disponível em: https://www.perkinscoie.com/en/news-insights/virtual-currencies-international-actions-and-regulations.html. Acesso em 26 fev. 2019.

POPPER, Nathaniel. **Some Bitcoin Backers Are Defecting to Create a Rival Currency**. *In:* The New York Times. ISSN 0362-4331. Disponível em: https://www.nytimes.com/2017/07/25/business/dealbook/bitcoin-cash-split.html. Publicado em 24 jul. 2017. Acesso em 26 fev. 2019.

RABIN, Claudio Goldberg. **BNDES criará Token no *Blockchain* da Ethereum**. Disponível em: https://portaldobitcoin.com/bndes-criara-token-no-*blockchain*-da-ethereum/. Publicado em 05 mar. 2018. Acesso em 26 fev. 2019.

RASKIN, Max. **The Law and Legality of Smart Contracts**. *In:* Georgetown Law Technology Review 304. Disponível em: https://ssrn.com/abstract=2959166. Publicado em 22 set. 2016. Acesso em 26 fev. 2019.

REBOUÇAS, Rodrigo Fernandes. **Contratos Eletrônicos**. Edição do Kindle. São Paulo : Almedina, 2015.

REED, Jeff. **Smart Contracts: The Essential Guide to Using *Blockchain* Smart Contracts for Cryptocurrency Exchange**. Kindle Edition. Amazon, 2016.

REIDENBERG, Joel. **Lex Informatica: The Formulation of Information Policy Rules through Technology**. Disponível em https://ir.lawnet.fordham.edu/faculty_scholarship/42/. Publicado em 1997. Acesso em 26 fev. 2019.

ROSA, Alexandre Morais da; PRÓSPERO, Felipe Navas. **Qual a validade jurídica dos documentos pela rede *Blockchain*?** Disponível em: https://www.conjur.com.br/2019-jan-11/limite-penal-qual-validade-juridica-documentos-rede-*blockchain*#author. Publicado em 11 jan. 2019. Acesso em 26 fev. 2019.

SANTOS, Antônio Carlos. **O mito de Sísifo: Teatro Antigo - as 13 mais belas lendas da mitologia greco-romana.** Amazon : Edição do Kindle, 2015

SANTOS, Manoel Joaquim Pereira dos; ROSSI, Mariza Delapieve. **Aspectos legais do comércio eletrônico: contratos de adesão.** Revista de Direito do Consumidor, n. 36, p. 106–129. São Paulo, 2000.

SWAN, Melanie. ***Blockchain*: Blueprint for a New Economy**. O'Reilly Media. Edição do Kindle, 2015.

SZABO, Nick. **Formalizing and securing relationships on public networks**. *In:* First Monday, vol. 2, n. 9–1, 1997. Disponível em http://firstmonday.org/ojs/index.php/fm/article/view/548/469. Acesso em 26 fev. 2019.

TAPSCOTT, Don; TAPSCOTT, Alex. ***Blockchain* Revolution : como a tecnologia por trás do Bitcon está mudando o dinheiro, os negócios e o mundo**. São Paulo : SENAI-SP Editora, 2016.

TARTUCE, Flávio. **Direito civil, v. 3: teoria geral dos contratos e contratos em espécie**; 13. ed. rev., atual. e ampl. – Rio de Janeiro: Forense, 2018.

TRUFFLE Overview. Disponível em: https://truffleframework.com/docs/truffle/overview. Acesso em 26 fev. 2019.

ULRICH, Fernando. **Bitcoin: a moeda na era digital**. São Paulo: Instituto Mises Brasil. 2014.

UNCITRAL, Site. **Lei Modelo Uncitral sobre o Comércio Eletrônico**. Disponível em: http://www.lawinter.com/1uncitrallawinter.htm. Acesso em 26 fev. 2019.

VIANA, Marco Aurelio. **Curso de Direito Civil – Contratos**. Rio de Janeiro: Forense, 2008.

WALL, Eric; MALM, Gustaf. **Using *Blockchain* Technology and Smart Contracts to Create a Distributed Securities Depository**. *In:* Lund University Libraries Student Papers. Disponível em: http://lup.lub.lu.se/student-papers/record/8885750. Publicada em 29 jun. 2016. Acesso em 26 fev. 2019.

WORSTALL, Tim. **Fascinating Number: Bitcoin Mining Uses $ 15 Million's Worth of Electricity Every Day.** *In:* Forbes Magazine. Disponível em https://www.forbes.com/sites/timworstall/2013/12/03/fascinating-number-bitcoin-mining-uses-15-millions-worth-of-electricity-every-day/#3cf80b7d525d. Publicado em 3 dez. 2013. Acesso em 26 fev. 2019.

ZHENG, Zibin; XIE, Shaoan; DAI, Hong-Ning; CHEN, Xiangping; WANG, Huaimin. ***Blockchain* challenges and opportunities: a survey.** *In:* Inderscience Enterprises Ltd. Disponível em: https://www.henrylab.net/pubs/ijwgs_*blockchain*_survey.pdf. Publicado em 2018. Acesso em 26 fev. 2019.