Check for Updates

O oráculo como elo entre a jurisdição e os *smart contracts*

The oracle as a link between jurisdiction and smart contracts

Jan Felipe Silveira

Universidade do Vale do Rio dos Sinos – UNISINOS

janfelipesilveira@gmail.com

Conflito de interesses: nada a declarar. Financiamento: nada a declarar.

Histórico:
Submissão | Received: 22/03/2022
Aprovação | Accepted: 28/03/2022
Publicação | Published: 30/04/2022

Resumo

O artigo tem como elemento central o estudo dos reflexos da adoção de *smart contracts* nas relações privadas. O trabalho concentra sua abordagem na possibilidade de esvaziamento das formas de jurisdição tradicionais, pela característica da auto executoriedade das cláusulas contratuais, como consequência da utilização da tecnologia blockchain. A tecnologia blockchain vem se tornando um dos maiores protagonistas na transformação das tecnologias digitais e isso se deve a sua peculiar característica de gestão descentralizada das informações, além de sua confiabilidade. A análise parte da identificação dos elementos intrínsecos dos *smart contracts*, demonstrando, de maneira dedutiva, suas especificidades e seus pontos de intersecção com a teoria contratual tradicional. Com a ampliação da utilização dos *smart contracts* para regular cada vez mais situações da vida privada, estabeleceu-se a necessidade de incorporar um elemento exógeno ao sistema, que é a figura do oráculo, cuja função é alimentar com dados externos a blockchain. Tem-se, portanto, um elo entre o mundo fenomênico e o mundo puramente virtual, através da tecnologia blockchain. Desse modo, a partir da concepção do oráculo, abre-se a possibilidade de ligação entre a jurisdição e os *smart contracts*.

Palavras-chave: *Smart contracts*, *Blockchain*, Oráculo, Jurisdição

Abstract

The article has as its central element the study of the impact of the adoption of smart contracts in private relations. The work focuses its approach on the possibility of emptying traditional forms of jurisdiction, due to the characteristic of self-execution of contractual terms, as a consequence of the use of blockchain technology. Blockchain technology has become one of the biggest protagonists in the transformation of digital technologies and this is due to its peculiar characteristic of decentralized information management, in addition to its reliability. The analysis starts from the identification of the intrinsic elements of smart contracts, demonstrating, in a deductive way, their specificities and their points of intersection with the traditional contractual theory. With the expansion of the use of smart contracts to regulate more and more situations of private life, it was established the need to incorporate an exogenous element into the system, which is the figure of the oracle, whose function is to feed external data to the blockchain. There is, therefore, a link between the phenomenal world and the purely virtual world, through blockchain technology. In this way, from the conception of the oracle, the possibility of linking the jurisdiction and smart contracts opens up.

Keywords: Smart contracts, Blockchain, Oracle, Jurisdiction

1. Introdução

A proposta apresentada no artigo será abordar a figura do oráculo como elo entre a jurisdição e os *smart contracts*. Em um primeiro momento, serão estudadas as principais características da *blockchain*, a partir da abordagem de elementos técnicos que viabilizaram a introdução dessa tecnologia.

Como o surgimento da tecnologia *blockchain* está intimamente ligado ao desenvolvimento da criptomoeda Bitcoin, far-se-á uma digressão acerca de suas principais características e suas perspectivas de aplicação.

Após os conceitos introduzidos com o estudo do Bitcoin, serão abordados os *smart contracts* e suas aplicabilidades práticas. Em sequência, será feita uma análise da figura do oráculo e suas principais características, bem como serão abordadas as diferenças existentes na utilização da tecnologia *blockchain* utilizada em criptomoedas daquela usada nos *smart contracts*, a partir das distintas informações exigidas para que os *smart contracts* tenham operabilidade.

Por fim, será feita uma análise inovadora acerca da figura do oráculo e sua capacidade de interligar a jurisdição tradicional com os *smart contracts.*

2. *Blockchain*

O espaço cibernético representa um campo novo para a reestruturação das relações interpessoais, especialmente no que se refere ao sistema regulatório e normativo. Sob essa nova perspectiva paradigmática, Lawrence Lessig cunhou a expressão "*code is law*", numa alusão à ideia de que o código computacional passará a estabelecer, progressivamente, as regras que irão reger o comportamento no mundo real. Segundo essa hipótese, a previsibilidade e a impessoalidade das regras atingiriam uma regulamentação quase perfeita (Lessig, 2006, *Passim*).

Segundo Lawrence Lessig (2006, p. 3):

> *Cyberspace would be a society of a very different sort. There would be definition and direction, but built from the bottom-up. The society of this space would be a fully self-ordering entity, cleansed of governors and free from political hacks.*

Neste contexto, a *blockchain* pode representar uma mudança significativa na maneira com que os indivíduos se relacionam em sociedade, uma vez que essa tecnologia possui um regramento algorítmico específico, seguro e adaptável a diferentes aplicações. Em uma operação entabulada com o uso da tecnologia *blockchain,* o código é, efetivamente, a lei.

A *blockchain* é uma tecnologia que utiliza uma arquitetura de programação que acrescenta uma nova "camada" na utilização dados através de protocolos preexistentes na internet. Essa nova "camada" de utilização de dados permite a realização de transações econômicas, tanto pagamentos imediatos de moeda digital (em uma criptomoeda universalmente utilizável), quanto financeira de longo prazo e também operações mais complexas, como executar um contrato.

Conforme Melanie Swan (2015, p. X, XI), a *blockchain* pode ser entendida como:

> *The blockchain is like another application layer to run on the existing stack of Internet*

> *protocols, adding an entire new tier to the Internet to enable economic transactions, both immediate digital currency payments (in a universally usable cryptocurrency) and longer-term, more complicated financial contracts. A blockchain is quite literally like a giant spreadsheet for registering all assets, and an accounting system for transacting them on a global scale that can include all forms of assets held by all parties worldwide. Thus, the blockchain can be used for any form of asset registry, inventory, and exchange, including every area of finance, economics, and money; hard assets (physical property); and intangible assets (votes, ideas, reputation, intention, health data, etc.) […] The economy that the blockchain enables is not merely the movement of money, however; it is the transfer of information and the effective allocation of resources that money has enabled in the human- and corporate-scale economy.*

Uma *blockchain* funciona como uma planilha em larga escala que registra todos os fluxos patrimoniais em um sistema contábil, permitindo transacioná-los em uma escala global. Assim, a *blockchain* pode ser usada para qualquer forma de registro, inventário e troca de ativos, incluindo todas as áreas de finanças, economia, ativos tangíveis e ativos intangíveis. A economia que a *blockchain* possibilita não é apenas em relação ao fluxo monetário, mas também a transferência de informações e a alocação efetiva dos mais diversos ativos financeiros (Swan, 2015, p. X, XI).

Para entender melhor as características de uma *blockchain*, é importante conhecer sua relação com o Bitcoin, já que sua arquitetura de programação é o elemento central da infraestrutura tecnológica que permitiu a criação dessa criptomoeda.

O Bitcoin foi desenvolvido por um programador que utilizou o pseudônimo Satoshi Nakamoto (2008), indicado como autor de um *White Paper* que descreve os conceitos básicos de funcionamento do Bitcoin. Em termos gerais, o Bitcoin pode ser descrito como uma moeda eletrônica descentralizada, de código aberto, baseada em software e *peer-to-peer* (P2P), que tem a seguinte definição: "a arquitetura P2P (peer-to-peer) é uma arquitetura de redes em que cada par, ou nó, coopera entre si para prover serviços um ao outro, sem a necessidade a priori de um servidor central. Todos os pares são clientes e servidores (Redes Par A Par – UFRJ, 2019).

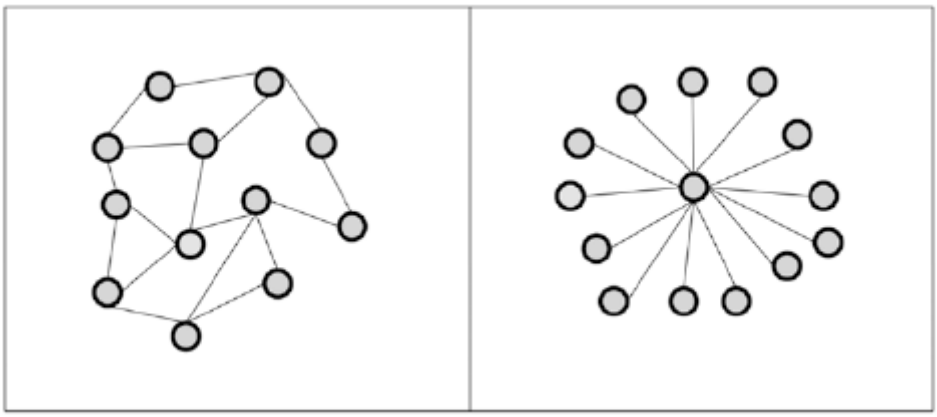
As principais características do Bitcoin são as seguintes:

Natureza descentralizada: O Bitcoin não possui um centro de custódia ou emissão de moeda conferido a alguma de autoridade ou a qualquer instituição centralizada. A manutenção das transações dessa criptomoeda é realizada por uma rede interconectada através de um software. Sob o aspecto técnico, o Bitcoin representa apenas um arquivo computacional, formulado a partir de algoritmo específico e que é processado nas plataformas de hardware dos integrantes da comunidade Bitcoin (Savelyev, 2017).

Até mesmo os desenvolvedores do protocolo de criptografia do Bitcoin não têm controle sobre transações ocorridas com essa moeda. A inexistência de uma instituição centralizadora permite a circulação de uma moeda desatrelada a um Banco Central, pois não necessita de uma instituição que a emita ou de instituições privadas, como as *fintechs* de intermediação de recebíveis, que custodiem o numerário (Moreira, 2019).

Para melhor ilustrar uma arquitetura de software descentralizada, como é o caso da *blockchain*, vejamos a figura a seguir (Figura 1).

Figura 1 – Modelos de representação software descentralizado e centralizado.



Fonte: Drescher (2017)

Os círculos na figura representam componentes do sistema, também chamados de *nodes,* ou nós (Blockchain: O Que São "Nodes" E Super-Nodes"?, 2019), e as linhas representam conexões entre eles. Neste ponto, não é importante conhecer os detalhes do que esses componentes fazem e quais informações são trocadas entre os nós. O ponto importante é a existência dessas duas maneiras diferentes de organizar sistemas de software. No lado esquerdo da figura, há uma distribuição distribuída e a arquitetura é ilustrada onde os componentes são conectados sem um elemento central. É importante ver que nenhum dos componentes está conectado diretamente com os demais. No entanto, todos componentes estão conectados um ao outro pelo menos indiretamente. Do lado direito, por seu turno, é ilustrada uma arquitetura centralizada, em que cada componente está conectado a um ente central e os componentes não estão conectados um com o outro diretamente (Drescher, 2017).

Natureza anônima: O Bitcoin pode ser utilizado sem que haja qualquer registro ou identificação. Basta que se instale um aplicativo *wallet,* carteira (Dayal, 2018), que sirva de plataforma para as transações a serem realizadas com essa criptomoeda. Cada carteira consiste em unidades Bitcoin, que possui uma chave pública e outra privada, senão vejamos:

> *A blockchain is essentially a distributed database of records or public ledger of all transactions or digital events that have been executed and shared among participating parties. Each transaction in the public ledger is verified by consensus of a majority of the participants in the system. (Crosby, Nachiappan, Pattanayak, Verma & Kalyanaraman, 2016)*

A chave privada é usada para transferir uma unidade Bitcoin da carteira de um usuário para a de outro. Sem o conhecimento da chave privada, a transação não pode ser assinada e a unidade Bitcoin não pode ser gasta. Já a chave pública é usada para que outras pessoas enviem unidades de Bitcoin para a carteira do usuário destinatário. Assim, o Bitcoin é uma moeda pseudônima, no sentido de que os fundos não estão vinculados a entidades do mundo real. Seus proprietários não são explicitamente identificados, mas todas as transações com essa criptomoeda são públicas.

Algoritmo matemático como elemento base de valoração do Bitcoin: O Bitcoin não é uma moeda lastreada, ou seja, ela não possui um valor intrínseco, bem como não está vinculada a qualquer autoridade fiduciária. No entanto, isso não significa que Bitcoin não possa ter um backup de seu valor. As unidades de Bitcoin são criadas durante um processo conhecido

como “mineração”. Cada pessoa que instalou software especializado pode "minerar" um Bitcoin como recompensa por resolver um problema matemático complexo, associado à verificação de transações realizadas com Bitcoins (Savelyev, 2017).

Ausência de administrador único de transações: Um grande risco para as operações eletrônicas são os gastos duplos. Os mecanismos tradicionais de moeda eletrônica evitam gastos duplos tendo um administrador confiável que segue o processo estabelecido para autorizar cada transação. O problema com esta solução é que o destino de todo o dinheiro depende da empresa que executa a função administrativa, com todos os envolvidos na transação tendo que passar por eles, assim como uma instituição bancária (Ulrich, 2014, p. 18). No caso do Bitcoin, o gasto duplo é resolvido através do uso da criptografia de chave pública. Esse sistema faz com que a cada usuário sejam atribuídas duas “chaves”, uma privada e outra pública. A primeira é mantida em sigilo e a segunda pode ser compartilhada com todos, desse modo, é possível traçar o histórico das transações com cada unidade de Bitcoin específica, graças à tecnologia *blockchain* (Savelyev, 2017).

Segurança contra manipulações: A criptografia usada no processo de criação de registros em transações com o Bitcoin, através do banco de dados em *blockchain*, impede adulterar o conteúdo de tais registros e garantir sua natureza perpétua, a ver:

> *Uma das inovações do blockchain foi armazenar em um bloco o hash do bloco anterior e organizar as transações de um bloco em uma árvore de Merkle. Assim, qualquer modificação em uma transação é percebida por causa da mudança da raiz da árvore de Merkle e qualquer adulteração em um bloco é perceptível devido à discrepância que surge com o hash armazenado no cabeçalho do próximo bloco. (Henriques, 2018, p. 8)*

Desse modo, sempre que duas pessoas trocam unidades de Bitcoin, um registro criptografado da transação é enviado para todos os outros nós na rede Bitcoin (Savelyev, 2017).

As características da arquitetura computacional por trás do Bitcoin são possíveis por causa da *blockchain*, que como visto, assegura a descentralização de armazenamento, a segurança das operações, a inviolabilidade de dados e a imutabilidade de transações.

3. Smart Contracts

Um *smart contract* (contrato inteligente) consiste em uma série de instruções pré-determinadas capazes de executar um acordo usando a tecnologia *blockchain.* Essas instruções estão atreladas a eventos externos, que irão estabelecer quais serão os desdobramentos futuros do contrato, a partir de uma execução automática. O objetivo de um *smart contract* é garantir a observância de condições contratuais comuns (como o adimplemento, a garantia, a confidencialidade e até mesmo cumprimento forçado), mitigando objeções tanto maliciosas quanto acidentais, e retirando a necessidade de terceiros intermediários confiáveis. Outros ganhos econômicos relacionados incluem a diminuição das despesas com fraudes, arbitragem e custos de execução contratual, além de outros diversos custos de transação.

Sob o tema, Nick Szabo (1994) esclarece:

> *A smart contract is a computerized transaction protocol that executes the terms of a contract. The general objectives*

> *of smart contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitration and enforcement costs, and other transaction costs.*

Para Nick Szabo, um *smart* contract pode ser comparado a um contrato que rege a operação feita através de uma *vending machine* com o consumidor. Em um contrato "tradicional", as partes estipulam as regras que irão reger a relação e, a partir daí, formalizam um instrumento contratual. Com uma *vending machine*, a operação é simplificada e potencialmente menos arriscada, pois basta inserir o dinheiro que o equipamento fará a entrega do produto, de forma imediata. A formalização da transação é validada a partir de um protocolo pré-determinado que controla a máquina, tornando desnecessária a formalização de um instrumento. Desse modo:

> *The basic idea of smart contracts is that many kinds of contractual clauses (such as liens, bonding, delineation of property rights, etc.) can be embedded in the hardware and software we deal with, in such a way as to make breach of contract expensive (if desired, sometimes prohibitively so) for the breacher. […] Smart contracts go beyond the vending machine in proposing to embed contracts in all sorts of property that is valuable and controlled by digital means. Smart contracts reference that property in a dynamic, proactively enforced form, and provide much better observation and verification where proactive measures must fall short. (Szabo, 1996)*

O resultado final obtido através de um *smart contract* não se resume a uma ação alcançada por um computador, após a execução de certo código, já que esse resultado foi validado por um conjunto de computadores interligados uns aos outros. Ainda, o resultado dessa ação é gravado em um registro público que permite a detecção de alterações subsequentes da mesma. O registro público, por sua vez, é mantido para sempre pelos demais computadores do sistema ou para uma parcela significativa dessa rede (Guardeño, Vico & Encinas, 2019, p. 76-77).

O *smart contract* necessita de uma plataforma digital para ser desenvolvido. Atualmente, a plataforma descentralizada Ethereum é a mais difundida mundialmente para esse propósito. O Ethereum atua como um computador mundial que se aproxima de uma máquina virtual, denominada de Ethereum Virtual Machine (EVM), com uma linguagem de computação própria, conhecida por *Turing*, que por sua vez, tem a capacidade de solucionar diversos problemas usando linguagem computacional de *script* universal conhecida como S*olidity*. Segundo Vitalik Buterin (2014), a Ethereum pode ser usada para construir quaisquer comandos matematicamente descritíveis através de contratos auto exequíveis. Essa linguagem computacional permite aos programadores desenvolver e disseminar seus próprios *smart contracts*, através da rede descentralizada do Ethereum (Luciano, 2018).

A ideia elementar dos *smart* contracts é que muitos tipos de estipulações contratuais podem ser adicionados ao protocolo de software, de maneira a tornar a violação do contrato algo dispendioso e indesejável. Os *smart contracts* são mais abrangentes do que aquela relação existente na operação de uma *vending machine,* ao propor a incorporação de contratos com praticamente todos os tipos de ativos, desde que possam ser controlados por meios digitais.

Os *smart contracts* seguem os fundamentos da lógica da programação. Sob essa perspectiva, é plausível imaginar uma possível a incorporação de todas as cláusulas de um contrato tradicional em uma estrutura de *blockchain* autoexecutável. Atualmente, muitas das estipulações contratuais, geralmente as cláusulas operacionais, podem ser codificadas e cumpridas a partir de uma rede *blockchain*, o

que as torna automáticas. Com a introdução da rede Ethereum, altamente difundida e mais refinada do que a rede Bitcoin, estima-se que sejam criadas plataformas específicas que incorporem todas as estipulações contratuais, não só aquelas puramente operacionais (Fazano-Filho, 2018).

Pelo observado, um *smart contract*, ao contrário do que seu nome possa sugerir, não diz respeito à aplicação de uma inteligência artificial a um instrumento contratual. Trata-se de um mecanismo que envolve ativos digitais de duas ou mais partes que, conforme os termos estipulados, são redistribuídos automaticamente entre os contratantes, seguindo uma fórmula específica baseada em dados previamente estabelecidos.

É importante destacar que existem dois paradigmas distintos que podem ser classificados como *smart contracts*. O primeiro envolve *smart contracts* criados e implementados sem uma ligação a qualquer texto base. Por exemplo, duas partes acordam um entendimento verbal sobre o relacionamento comercial que desejam realizar e, em seguida, reduzem esse entendimento diretamente em um código executável. Neste caso, estar-se-ia diante de um *code-only smart contract* (contrato inteligentes somente de código). O segundo paradigma envolve o uso de *smart contracts* como veículos para efetivar disposições de um contrato tradicional, no qual o próprio instrumento faz menção ao uso do contrato inteligente para efetivar certas disposições. Esses *smart contracts* são classificados como *ancillary smart contracts* (contratos inteligentes auxiliares) (Lipton & Levi, 2018).

Outro ponto essencial para entender o funcionamento dos *smart contracts* é o estudo dos "oráculos", que representam um elemento de conexão entre a *blockchain* e o mundo exterior. Oráculos podem ser tanto *softwares* quanto agentes físicos que vivem fora de contratos inteligentes, mas que fornecem informações acerca de eventos que podem desencadear a execução de suas cláusulas. Em um contrato de seguro, por exemplo, o oráculo pode certificar que, em determinado dia, horário e local, a temperatura de uma carga atingiu o limite estipulado no contrato e isso desencadeou a auto execução de uma cláusula indenizatória (Treiblemaier & Beck, 2018, p. 282).

4. Os oráculos

Os oráculos elementos são essenciais para a utilização dos *smart contracts,* quando a execução de suas cláusulas necessitar de uma conexão com uma fonte de dados externa. A ausência dessa fonte externa restringiria enormemente a utilização desses contratos. É inevitável que os *smart contracts* de maior complexidade exijam, em algum momento, que a *blockchain* seja alimentada com dados do mundo real, tais como: apostas, contratos financeiros, informações do mercado acionário, notícias, e até informações de outras *blockchains*. Em razão de aspectos técnicos, geralmente, todo *smart contract* acabará dependendo de um *middleware* para resolver esse problema. Esse *middleware* é chamado de oráculo.

Conforme Shermin Voshgir (2019), os oráculos podem ser entendidos como:

> *Oracles feed the smart contract with external information that can trigger predefined actions of the smart contract. This external data stems either from so ware (Big-data application) or hardware (Internet-of-Things). Such a condition could be any data, like weather*

> *temperature, successful payment, or price fluctuations. However, it is important to note that a smart contract does not wait for the data from an outside source to ow into the system. The contract has to be invoked, which means that one has to spend network resources for calling data from the outside world. This induces network transaction costs. In the case of Ethereum, this would be 'gas.*

As *blockchains* não acessam diretamente a informação exterior, fora da cadeia de blocos, não existindo uma forma direta para validar as condições preestabelecidas nos *smart contracts*. Desse modo, oráculo atua como um intermediador da informação colhida no mundo exterior e a transporta para dentro da *blockchain* (Buck, 2017).

Para um *smart contract* cujas condições de execução estão vinculadas a marcos temporais ou a ações executadas na própria *blockchain*, a verificação é automática. Todavia, se for preciso verificar de alguma condição externa, será necessária a presença de um terceiro confiável, um oráculo. O oráculo pode ser um terceiro escolhido pelas partes, como uma instituição de prestígio ou até mesmo um grupo colegiado.

Sobre o tema, importante a visão de Laurent Leloup (2017), que aborda o tema sob a ótica da confiança:

> *Pour un contrat intelligent dont les conditions d'exécution sont liées à des indicateurs temporels ou à des écritures dans la blockchain, la vérification est automatique. En revanche, dans le cas où il faut vérifier une condition externe (que le colis a bien été reçu), il faut faire appel à un tiers de confiance, un Oracle dans le jargon d'Ethereum. L'Oracle peut être un tiers désigné par les deux parties, un institut/association de confiance ou encore un consensus de nombreux tiers (projet Oraclize).*

Shermin Voshmgir (2019) lista os diferentes tipos de oráculos:

A. Oráculo de software: lida com dados de informações originários de fontes *online*, como temperatura, preços de mercadorias e mercadorias, atrasos nos voos ou trens etc.

B. Oráculo de hardware: alguns contratos inteligentes precisam de dados coletados diretamente de fenômenos físicos, por exemplo, um carro atravessando uma barreira em que os sensores de movimento devem detectar o veículo e enviar os dados para um contrato inteligente, ou sensores RFID no setor da cadeia de suprimentos.

C. Oráculo de entrada: fornece dados do mundo externo para a *blockchain*.

D. Oráculo de saída: fornece informações através de *smart contracts* com a capacidade de enviar dados para o mundo externo.

E. Oráculos baseados em consenso: os dados são obtidos através de mercados de consenso e de previsão, podendo derivar de plataformas como Augur e Gnosis. Usar apenas uma fonte de informação pode ser arriscado e não confiável. Para evitar manipulação do mercado, os mercados de previsão implementam um mecanismo de classificação para oráculos. Para maior segurança, um conjunto de oráculos distintos pode ser utilizado para validar uma movimentação específica na *blockchain.*

Simon Polrot (2016) afirma que a existência do oráculo equivale à introdução de um terceiro confiável, mas ressalta que esse terceiro

possui um poder tão exorbitante quanto seu equivalente mitológico, pois em verdade, é ele quem decide o resultado dos *smart contracts*, contrariando a máxima de que tais contratos seriam inatingíveis ou impossíveis de serem parados. O autor exemplifica ao trazer um caso em que o oráculo silencia, não fornecendo informações essenciais para o prosseguimento do contrato, assim, suas cláusulas não poderão ser executadas. Nesses casos, os programadores devem fornecer uma porta de saída para esse cenário, como o cancelamento do instrumento na ausência de informações em uma data específica. Se nada for planejado, no entanto, existe o risco de que as quantias envolvidas fiquem eternamente bloqueadas. Outra situação crítica seria o envio de informações falsas, de maneira equivocada ou voluntária. Nesse caso, é impossível retroceder a ação executada, a menos que o contrato preveja uma porta de saída, pois as informações são inseridas e salvas permanentemente na *blockchain*.

Uma característica importante é que oráculo pode servir como mecanismo para o exercício da função jurisdicional tradicional em relação ao *smart contracts*, uma vez que uma ordem judicial poderá intervir diretamente na fonte da informação que alimenta a *blockchain.* Essa característica traz um novo panorama para os *smart contracts,* que é a possibilidade de instauração de procedimentos para resolução de disputas, que irão interferir na execução dos contratos.

5. O oráculo como elo entre a jurisdição e os *smart contracts*

Em um primeiro momento, a utilização dos *smart contracts* pode passar a impressão de que as relações privadas estarão cada vez mais vinculadas a uma noção de normatividade cibernética ou computacional, cuja consequência seria o gradativo esvaziamento da função jurisdicional tradicional, decorrente da automação proporcionada pelo sistema da *blockchain*. Por analogia, essa mudança seria um retorno ao modelo de autocomposição privada existente no período pré-oitocentista, cujo ciclo foi encerrado por um grande marco na história do Direito, após os Estados soberanos avocarem para si o monopólio da jurisdição, a partir da edição de códigos como o napoleônico (Coelho, 2013, p. 27).

Todavia, como visto anteriormente, a execução dos comandos contratuais sob o protocolo dos *smart contracts* pode ser dependente de informações do mundo real, remanescendo a necessidade de existir um terceiro confiável para determinar os rumos da relação. Esses terceiros, também chamados de oráculos, portanto, podem ser considerados como um o elo entre a jurisdição e os *smart contracts*, uma vez que, estando fora da *blockchain*, estão sujeitos aos regramentos legais tradicionais e mais do que isso, são suscetíveis à intervenção humana.

As inovações trazidas pela *blockchain* tendem a alterar significativamente o cenário jurídico como o conhecemos, uma vez que as novas tecnologias envolvem questões técnicas e multidisciplinares que transcendem a compreensão do jurista. O entendimento das cláusulas contratuais, por exemplo, não dependerá somente de uma hermenêutica tradicional, mas também, de uma compreensão de códigos e comandos computadorizados. A existência dos oráculos pode chancelar o surgimento de um Sistema Judicial híbrido, que comporta tanto as inovações trazidas pelas

novas tecnologias ao mundo jurídico, quanto mantém a possibilidade de submissão das relações à jurisdição.

O mecanismo dos oráculos pode facilmente ser submetido a uma ordem de adiamento de decisão, por exemplo, o que impede a execução de um mandamento contratual preestabelecido. Independentemente de onde partiu a ordem, se de uma Corte Arbitral eleita pelas partes ou de um Tribunal Estatal, o *smart contract* permanece inerte, até que seja dirimida a eventual controvérsia. Nesse ponto, importante citar Pietro Ortolani (2019, p. 439):

> *The mechanism of oracles can be readily applied to arbitration; a smart contract can defer to the decision of a third party adjudicator, such as an arbitral tribunal, and determine the final recipient of certain disputed assets on the basis of a ruling made by that oracle. In other words, the external information retrieved by the smart contract could be an arbitral award, and software script could be used to enforce the outcome of the procedure.*

Essa possibilidade de intervenção da jurisdição nos *smart contracts*, inversamente do que muitos possam vir a afirmar, de que isso afetaria a liberdade de contratar, não nos parece ser um argumento sustentável. Isso por que, uma normatividade cibernética, conforme descrita por Lawrence Lessig (2006, p. 3), em que o código seria a lei, pode apresentar problemas ao não conseguir dirimir infrações por parte dos contratantes, que sob o manto da imutabilidade do contrato, estariam salvaguardados.

Desse modo, se o código computacional for a única lei a ser respeitada pelas partes, é questão de tempo para transgressões éticas e comportamentos oportunistas serem práticas costumeiras e preponderantes nessas relações envolvendo os *smart contracts*.

Sob essa perspectiva, entendemos que a existência dos oráculos servirá para resguardar os interesses dos contratantes, pois permitirá que questões controvertidas possam ser submetidas à análise jurisdicional antes que a ação do *smart contract* venha a ser efetivamente executada.

Portanto, da mesma forma que os contratantes estipulam comandos automáticos para seus contratos, eles poderão eleger qual o meio mais adequado para a solução de controvérsias, submetendo eventual decisão ao oráculo responsável por alimentar a *blockchain.*

A resolução de disputas no âmbito dos *smart contracts* certamente irá emergir como um vasto campo de atuação, refletindo as profundas mudanças sociais que a tecnologia tem proporcionado à humanidade (Goldenfein & Leiter, 2018). Entretanto, até que se desenvolva um novo sistema normativo, que possibilite uma maior automação e independência, ainda existirá a necessidade de intervenção jurisdicional nos moldes tradicionais.

6. Considerações Finais

Conforme verificado, a figura dos oráculos possui papel importante na disseminação da utilização dos *smart contracts*, não só por sua característica intrínseca de alimentar a *blockchain* com informações do mundo exterior, mas, especialmente, por representar um meio efetivo de comunicação da jurisdição tradicional com essa nova modalidade contratual.

Esse atributo conferido ao oráculo pode fazer com que os *smart contract*s sejam ainda mais popularizados, alcançando novas modalidades

de contratações e mudando significativamente as relações privadas, através de maior segurança, velocidade e menores custos de transação.

Até que se desenvolva um sistema normativo que rompa com os paradigmas clássicos, as relações interpessoais e os contratos ainda necessitarão da chancela da jurisdição tradicional.

BIBLIOGRAFIA

Buck, J. (2017). *Blockchain Oracles, Explained*. Disponível em:<https://cointelegraph.com/explained/blockchain-oracles-explained>. Acesso em: 18 dez. 2019.

Buterin, V. (2014). *A next-generation smart contract and decentralized application platform*. Disponível em: <https://www.weusecoins.com/assets/pdf/library/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf>. Acesso em: 19 dez. 2019.

Coelho, F. (2013). *Manual de Direito Comercial*. 25. ed. São Paulo: Saraiva.

Crosby, M., Nachiappan, Pattanayak, P., Verma, S. & Kalyanaraman, V. (2016). *Blockchain Technology: Beyound Bitcoin*. Sutardja Center. Berkeley University of California. Disponível em:< https://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf>. Acesso em: 18 dez. 2019.

Dayal, P. (2019). *What is Blockchain Wallet and How does it work?* 2018. Disponível em: < https://www.newgenapps.com/blog/what-is-blockchain-wallet-and-how-does-it-work>. Acesso em: 10 dez. 2019.

Dresher, D. (2017). *Blockchain basics: a non technical introduction in 25 steps*. Frankfurt: Apress.

Fazano Filho, J. (2018). *Perspectivas para a tecnologia blockchain*. *Revista de Direito Bancário e do Mercado de Capitais, São Paulo*, *v. 81*, p. 141-158.

Goldenfein, J. & Leiter, A. (2018). Legal engineering on the Blockchain: 'Smart Contracts' as Legal Conduct. *Law and Critique, Netherlands: Springer, v. 28,* p. 141-149.

Guardeño, D., Vico, J. & Encinas, L. (2019). *¿QUÉ SABEMOS DE? Blockchain*. Madrid: Catarata.

Leloup, L. (2017). *Blockchain: La révolution de la confiance*. Paris: Eyrolles.

Lessig, L. (2006). *Code: version 2.0*. New York: Basic Books.

Lipton, A. & Levi, S. (2019). *An Introduction to Smart Contracts and Their Potential and Inherent Limitations*. 2018. Disponível em: < https://corpgov.law.harvard.edu/contributor/stuart-levi>. Acesso em: 19 dez. 2019.

Lucena, A. & Henriques, M. (2018). *Estudo preliminar da adoção de assinaturas baseadas em hash no blockchain do Bitcoin*. Disponível em: <https://www.semanticscholar.org/paper/Estudo-preliminar-da-ado%C3%A7%C3%A3o-de-assinaturas-baseadas-Lucena-Henriques/0d8ba05269373519aeb302a6fcd44a48ccc21cf8> Acesso em: 18 dez. 2019.

Luciano, R. (2018). Aplicação da Smart Contract nos Contratos de Gás Natural: Uma Análise Exploratória. *Revista de Administração Contemporânea*, Maringá, *v. 22.*

BIBLIOGRAFIA

Moreira, R. (2019) Investigação preliminar sobre o blockchain e os smart contracts. *Revista de Direito e as Novas Tecnologias*, São Paulo, *v. 3*.

Nakamoto, S. (2008). *A Peer-to-Peer Electronic Cash System*. 2008. Disponível em: < https://bitcoin.org/bitcoin.pdf>. Acesso em: 11 dez. 2019.

Ortolani, P. (2019). The impact of blockchain technologies and smart contracts on dispute resolution: arbitration and court litigation at the crossroad. *Oxford Uniform Law Review*,v. 24, Issue 3. *Oxford Uniform Law Review*, 2019. p. 439. Disponível em: < https://academic.oup.com/ulr/issue/24/3>. Acesso em: 19 dez. 2019.

Polrot, S. (2016). *Les Oracles, lien entre La blockchain et Le monde*. Disponível em:< https://www.ethereum-france.com/les-oracles-lien-entre-la-blockchain-et-le-monde>. Acesso em: 12 dez. 2019.

Savelyev, A. (2017). Contract law 2.0: 'Smart' contracts as the beginning of the end of classic contract law. *Information & Communications Technology Law*, v. 26, Issue 2, Australia: University of Newcastle, 2017. Disponível em: <https://www.tandfonline.com/action/doSearch?AllField=Alexander+Savelyev&SeriesKey=cict20>. Acesso em: 16 dez. 2019.

Swan, M. (2015). *Blockchain: Blueprint for a New Economy*. Sebastopol: O'Reilly, 2015.

Szabo, N. (1994). *Smart Contracts*. Disponível em: <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html>. Acesso em: 14 dez. 2019.

Szabo, N. (1996) *Smart Contracts: Building Blocks for Digital Markets*. Disponível em: <http://www.truevaluemetrics.org/DBpdfs/BlockChain/Nick-Szabo-Smart-Contracts-Building-Blocks-for-Digital-Markets-1996-14591.pdf>. Acesso em: 14 dez. 2019.

Tasca, P. (2019). Insurance Under the Blockchain Paradigm. TREIBLEMAIER, Horst; BECK, Roman (Org.). *Transformation through Blockchain*. v. 1, Cham, Switerland: Palgrave Macmillan, 2019.

UFRJ. (2019). *Redes Par-a-Par (Peer to Peer Networks)*. Disponível em: <https://www.gta.ufrj.br/ensino/eel878/redes1-2018-1/trabalhos-v1/p2p/arquitetura.html>. Acesso em: 11 dez. 2019.

Ulrich, F. (2014) *Bitcoin: a moeda na era digital*. São Paulo: Instituto Von Mises Brasil.

Universocripto. (2019). Blockchain. *O que são "Nodes" e "SuperNodes"?*. Disponível em: < https://universocripto.net/blockchain-o-que-sao-nodes-e-supernodes> Acesso em: 17 dez. 2019.

Voshmgir, S. (2019). *Blockchain Oracles.* 2019. Disponível em: < https://blockchainhub.net/blockchain-oracles>. Acesso em: 15 dez. 2019.