UNIVERSIDADE DE BRASÍLIA - UnB
Faculdade de Direito

JOSEMARÍA DIAS DE PAULA FREITAS PORTELLA

DESCUMPRIMENTO DE SMART CONTRACTS

A prevenção por meio da tecnologia e solução pelo Judiciário

Breach of Smart Contracts
Prevention through technology and resolution by the Judiciary

Brasília
2025

Josemaría Dias de Paula Freitas Portella

DESCUMPRIMENTO DE SMART CONTRACTS

A prevenção por meio da tecnologia e solução pelo Judiciário

Monografia apresentada à Faculdade de Direito da Universidade de Brasília, como requisito parcial à obtenção do grau de Bacharel em Direito.

Orientador: Prof. Dr. João Costa-Neto

Brasília
2025

FOLHA DE APROVAÇÃO

Trabalho de Conclusão de Curso apresentado à banca examinadora, para fins de avaliação, em 21 de junho de 2025.

BANCA EXAMINADORA

_____

Prof. Dr. João Costa-Neto
Orientador

_____

Prof. Dr. Ives Gandra da Silva Martins Filho
Examinador

_____

Prof. Dr. Pedro Henrique de Moura Gonet Branco
Examinador

Aprovado em: 21 de junho de 2025.

Para José Francisco e Maria de Fátima,
Marina, José Ângelo e Maria Alice.
Um agradecimento especial a Sandro e a Andréa.

RESUMO

Os *smart contracts* estão sujeitos a descumprimentos e, no contexto de compra e venda de mercadorias físicas, esse descumprimento pode se dar pela não entrega do produto ou a entrega com algum defeito. Com base nessa problemática, este trabalho visa, em um primeiro momento, a buscar métodos de se garantir que o contrato chegue a seu adequado cumprimento ou, ao menos, que as partes de boa-fé não saiam prejudicadas. Os métodos de se alcançar tal objetivo já partem da escolha do modelo de *smart contract* do tipo *escrow* e se complementam pelo uso de oráculos e pela contratação de seguradoras. Após esta etapa, o trabalho se dedica, em um segundo momento, a identificar como o Poder Judiciário pode julgar litígios oriundos de contratos inteligentes de compra e venda. Para tal, a discussão se cinge a, primeiramente, provar que o Judiciário tem jurisdição sobre tais causas - ainda que *smart contracts* não estejam regulamentados no Brasil -, objetivo alcançado sob o fundamento do princípio da inafastabilidade. Uma vez concluída essa primeira discussão, parte-se para um segundo objetivo, qual seja o de como este Poder pode solucionar tais demandas. Nesse ponto, a discussão se centra especificamente em como ser feito o sopesamento entre dois princípios que regem o direito dos contratos: de um lado, o *pacta sunt servanda* e, de outro, o *rebus sic stantibus*. Isso porque, considera-se que em litígios envolvendo contratos inteligentes de compra e venda de mercadorias, na grande maioria dos casos, a lide pode ser dirimida com a aplicação de tais princípios. Para tal, em primeiro lugar, faz-se uma discussão acerca da validade dos contratos inteligentes, fato que deve preceder à aplicação de princípios de direito dos contratos a essa nova modalidade de contratação. Uma vez concluído que *smart contracts* consistem em contratos válidos à luz do Direito brasileiro, dedicou-se- à identificação de como deve ser realizado o sopesamento dos princípios ao dirimir tais tipos de lides. O trabalho foi feito por meio de uma pesquisa bibliográfica e documental.

Palavras-chaves: *Smart contract*. Oráculos. *Pacta sunt servanda. Rebus sic stantibus*.

ABSTRACT

Smart contracts are subject to breaches, and in the context of the purchase and sale of physical goods, such breaches may occur through non-delivery of the product or delivery with defects. Based on this issue, this study initially aims to explore methods to ensure that the contract is duly fulfilled or, at the very least, that the parties acting in good faith are not unfairly harmed. The methods to achieve this goal begin with the selection of the escrow-type smart contract model and are complemented by the use of oracles and the involvement of insurance companies. Following this first stage, the study then turns to examining how the Judiciary can adjudicate disputes arising from smart contracts for the sale of goods. To this end, the discussion is initially focused on demonstrating that the Judiciary does have jurisdiction over such cases—even though smart contracts are not yet regulated in Brazil—based on the constitutional principle of inafastabilidade (the guarantee of access to justice). Once this point is established, the study moves to a second objective: analyzing how the Judiciary may resolve such disputes. At this stage, the discussion centers on how to balance two fundamental principles of contract law: on one hand, *pacta sunt servanda* (agreements must be kept), and on the other, *rebus sic stantibus* (contracts may be modified in light of changed circumstances). This is because, in most disputes involving smart contracts for the sale of goods, the conflict can be resolved by applying these principles. To this end, the study first addresses the validity of smart contracts, an issue that must be resolved before the application of traditional contract law principles to this new form of agreement. Once it is established that smart contracts are valid under Brazilian law, the study focuses on how the balancing of these principles should be conducted in resolving such disputes. The research was conducted through bibliographic and documentary analysis.

Keywords: Smart contract. Oracles. *Pacta sunt servanda*. *Rebus sic stantibus*.

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

Smart contracts, ou contratos inteligentes, constituem uma forma de contratação desenvolvida, entre outros intuitos, para garantir maior segurança aos contratantes, no que se refere ao cumprimento da avença. Isso porque, considerando sua natureza, seu descumprimento é mais difícil do que o de contratos convencionais. Essa dificuldade surge, em primeiro lugar, do fato de eles serem executados de forma autônoma, isto é, uma vez firmada a avença entre as partes, não é possível sua reversão.

Esse atributo provém de sua natureza: *smart contracts* são códigos armazenados em *blockchains* e não há quem possa impedir a execução autônoma desses código.[1] O segundo atributo que torna este tipo de contrato seguro consiste na impossibilidade de alteração dos termos acertados, visto que a alteração de um código armazenado em um bloco integrante dessa cadeia de blocos - *blockchain* - implica tal esforço que, na prática, é impossível corrompê-lo.

Esse esforço se compreende no fato de que a alteração de blocos[2] resulta na necessidade de se descobrir o código gerado para o bloco que se pretende criar ou modificar - código este chamado *hash* - para que todos os dados contidos sejam validados e anexados à *blockchain*, tarefa essa que, por si só, já é extremamente onerosa.[3]

A dificuldade, no entanto, não se limita à descoberta do código do bloco que contém o contrato que se deseja alterar, mas esta tarefa deve ser executada em relação a todos os blocos seguintes, já que a alteração da *hash* de um bloco implica a alteração da *hash* do subsequente, sendo necessário alcançar os códigos de todos os blocos seguintes. Dessa forma, a menos que se forme um consenso entre usuários que torne viável o empreendimento tratado, é praticamente impossível que se altere um contrato contido em *blockchain*, o que denota sua segurança.

O terceiro atributo que faz dos *smart contracts* extremamente seguros é sua resiliência. Tal atributo se baseia no fato de que as *blockchains* são redes compartilhadas por usuários em todo o mundo, de forma que eventos pontuais que impeçam o acesso de usuários em alguma localidade - seja por catástrofe ambiental ou por medida censória governamental - não invalidam ou fazem perder os dados armazenados, porque a tecnologia é replicada por todos os computadores a ela ligados.[4]

---

[1] DE FILIPPI, Primavera de; WRIGHT, Aaron. **Blockchain and the law: the rule of code**. Cambridge, Massachusetts: Harvard University Press, 2019, pgs. 74-75.
[2] A mudança de um contrato contido implica alteração de todo o bloco.
[3] DE FILIPPI;WRIGHT, op. cit., p. 36.
[4] Ibid., p. 36.

A partir dessas características - que tornam os *smart contracts* muito mais seguros que contratos convencionais -, pode-se pensar que essa modalidade contratual conferiria às partes envolvidas uma garantia de que a avença se cumpriria sem percalços. No entanto, isso ainda não é realidade na totalidade dos casos, sendo possível que um contrato inteligente permita o descumprimento do acordo estipulado.

Um dos cenários de descumprimento é o de contratos inteligentes de compra e venda de produtos. Sim, de fato, um *smart contract*, conquanto apresente todos os atributos citados, pode permitir que um produto negociado seja entregue com defeito, gerando uma situação litigiosa entre as partes.

Nesse contexto, é particularmente curioso pensar na comercialização de produtos fisicamente tangíveis e enviadas por correios ou empresas de transporte. Nesses casos, a probabilidade de que o produto não seja entregue ou chegue ao destino com algum defeito é muito maior do que um produto virtual, visto que vários fatores podem desviar o contrato de seu cumprimento ideal, tais como: necessidade de comparecimento presencial do vendedor a uma agência para enviar o produto; possível erro da transportadora ao encaminhar a mercadoria; ou mesmo a sujeição do produto a intempéries.

Nesse cenário, o presente trabalho busca identificar, em um primeiro momento, meios de minimizar as chances de descumprimento de um contrato inteligente de compra e venda de produto físico. Essa abordagem, porém, centra-se em uma visão preventiva, ou seja, em como evitar que, ao se utilizar *smart contracts* de compra e venda de mercadorias, produtos sejam entregues com defeito ou nem mesmo sejam entregues.

Já a segunda parte do trabalho se propõe a identificar como o Poder Judiciário pode solucionar litígios oriundos de *smart contracts* de compra e venda. Para tal, a discussão se concentra em discutir como deve o juízo sopesar dois princípios: o *pacta sunt servanda* e o *rebus sic stantibus* ao julgar litígios que versem sobre contratos inteligentes de compra e venda. Antes, porém, de identificar como deve o Judiciário dirimir tais lides, será feita uma discussão acerca da possibilidade de jurisdição desse Poder sobre tais demandas, haja vista a inexistência de regulamentação de tais tecnologias no país. Em seguida, analisa se contratos inteligentes podem ser considerados existentes, válidos e eficazes à luz do Direito, de modo a concluir se a eles é aplicável o sopesamento dos princípios contratuais mencionados.

Assim, no primeiro capítulo, delimita-se o objeto da pesquisa a ser realizada, determinando-se que o modelo de contrato inteligente a respeito do qual serão analisadas formas de solucionar o problema posto é o modelo de contrato *escrow*. A escolha do modelo se deu pelo fato de que este é o que melhor garante segurança às partes entre todos os que há.

Dessa forma, muito mais eficiente, para os fins da pesquisa, mostram-se formas de garantir segurança às partes, com base em um modelo que já é mais seguro por si próprio.

No segundo capítulo, então, são efetivamente abordadas as formas de se solucionar a primeira problemática proposta. Nesse ponto, são tratados os oráculos como ferramentas centrais de modelos contratuais nos quais as chances de haver os problemas propostos são consideravelmente minimizadas.

O primeiro subcapítulo consiste em uma introdução à temática dos oráculos, apresentando-os como mecanismos hábeis a transitar informações entre os ambientes interno e externo à *blockchain*, de modo a garantir adequado funcionamento de contratos inteligentes. Para melhor explanar o conceito, são trazidos um exemplo prático e um esquema gráfico que expõe o funcionamento de um oráculo.

No segundo subcapítulo, abordam-se alguns dos tipos de oráculos, apresentando-se conceitos e exemplos. Nesse ponto, trata-se, primeiramente, da distinção entre oráculos de entrada e de saída, sendo estes aqueles que introduzem dados externos na *blockchain* e aqueles os que operam a transição de dados no sentido contrário. Entre estas duas classes, apresentam os oráculos de entrada maior número de subgrupos, de modo que maior ênfase será dada a esta classe, sendo apresentadas as seguintes classificações: oráculos de *software*; de hardware; de computação; oráculos baseados na agregação de dados; oráculos descentralizados; oráculos inteligentes; e oráculos humanos.

Uma vez exposta tal visão ampla de oráculos, propõe-se, no terceiro subcapítulo, uma discussão acerca da confiabilidade dos dados fornecidos por oráculos. Esta dúvida é pertinente ao se considerar que o bom funcionamento de um contrato inteligente depende diretamente da idoneidade de um oráculo e da consequente veracidade dos dados obtidos. Para responder a tal indagação, expõe-se que, dada a variedade de oráculos e suas diferenças essenciais, não há formas de garantir a veracidade dos dados aplicáveis a todos os oráculos de forma geral.

Nesse contexto, então, a primeira alternativa apresentada é a obtenção de informação de uma fonte notoriamente confiável, opção que não está isenta de erro e que peca por ser uma forma concentrada de funcionamento, contrariando o "espírito" que rege *blockchains*, pautado pela descentralização.

A segunda, por seu turno, consiste na técnica de busca, por apenas um oráculo, de uma mesma informação em distintas fontes, de modo a identificar a informação que mais provavelmente seja a adequada.

A terceira alternativa consiste no princípio aplicado em oráculos descentralizados, ou seja, informações a serem utilizadas em contratos podem passar por um mecanismo de

"confirmação" por outros integrantes do sistema antes que seja usada em um contrato. Esse mecanismo é melhor tratado ao final do trabalho, ao ser abordado um modelo de contrato que utiliza uma rede de oráculos descentralizados.

Ao final, discorre-se, mais detidamente, sobre a idoneidade de oráculos humanos, visto que tal tipo de oráculo, conquanto esteja sujeito a falhas – inerentes à natureza humana -, mostra-se bastante efetivo.

Após este subtópico, são apresentados modelos de contratos inteligentes que lançam mão de alguns dos oráculos abordados de modo a anular ou, ao menos minimizar, as possibilidades de o produto não ser entregue ou ser entregue com defeito.

Assim, o primeiro modelo apresentado consiste em contrato que se vale exclusivamente de oráculo humano a fim de remediar eventual conflito entre as partes. Nesse caso, é visto que um oráculo baseado em inteligência humana pode analisar provas e versões apresentados pelas partes de modo a determinar a quem será enviado o montante "preso" no contrato.

O segundo modelo, por seu turno, consiste em proposta de contrato com ênfase na utilização de oráculos de *hardware*, os quais obtêm informações a partir de sensores instalados nos produtos ou nas embalagens com as quais são transportados. Neste modelo, outrossim, é sugerida a contratação de seguro com o fim de ressarcir o comprador na hipótese de haver descumprimento do contrato por culpa da transportadora.

O terceiro modelo, por fim, apresenta a utilização de dois tipos de oráculos – de *hardware* e humano -, porém utilizados de maneira descentralizada, o que garante maior veracidade aos dados. Nesse modelo, assim como no anterior, é proposta a contratação de uma empresa seguradora.

Com essa organização da primeira parte do trabalho, portanto, busca-se lograr o primeiro objetivo proposto, qual seja o de buscar formas de minimizar ou anular as chances de ocorrência de problemas envolvendo contratos inteligentes de compra e venda de mercadorias físicas.

A primeira parte do trabalho, como se depreende, traz uma perspectiva preventiva em relação litígios em contratos de compra e venda, propondo formas de evitar que as avenças sejam descumpridas. Na segunda parte, por seu turno, o objetivo é remediativo e se volta a identificar a atuação do Poder Judiciário na solução de tais litígios.

Essa parte é desenvolvida no terceiro capítulo, sendo que o primeiro subcapítulo se presta a introduzir toda a temática que será discutida. Apresenta-se, nesse ponto, que em casos nos quais há descumprimento de contratos inteligentes de compra e venda, é possível conceber formas distintas de solução a depender se as partes agem de boa-fé ou se há má-fé de uma delas.

Agindo todas as partes com boa-fé, nada obsta que a falha ocorrida no contrato seja resolvida extrajudicialmente, seja com ou sem arbitragem. No entanto, havendo má-fé por parte de um dos polos, defende-se que a questão inevitavelmente deve ser levada ao Poder Judiciário. Introduzem-se, então, duas questões a serem desenvolvidas, quais sejam: se o Judiciário pode julgar tais causas, haja vista a falta de regulamentação; e como deve o Poder Judiciário julgar tais litígios, com enfoque no embate entre os princípios da força obrigatória dos contratos e da onerosidade excessiva.

No segundo subcapítulo, é desenvolvida a primeira discussão proposta, ou seja, se o Poder Judiciário tem competência para julgar tais lides. Tal problema pode surgir sob a égide de uma aplicação estrita do princípio da legalidade, a qual poderia levar a um dos litigantes a sustentar a impossibilidade de responsabilização por dano cometido por meio de tecnologia desconhecida pelo ordenamento jurídico brasileiro. O problema é solucionado com a aplicação do princípio da inafastabilidade, o qual impede que o Poder Judiciário se negue a julgar uma questão pelo simples fato de não haver regulamentação da matéria.

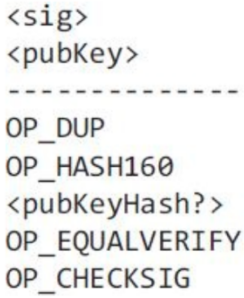
Uma vez abordado que o Poder Judiciário deve apreciar tais lides, o terceiro subcapítulo aborda o enfoque que se deu, neste trabalho, ao julgamento pelo Judiciário, ou seja, o sopesamento entre os princípios do *pacta sunt servanda* e do *rebus sic stantibus*. O subcapítulo se inicia com uma introdução aos princípios tratados e se subdivide em duas partes: uma voltada a analisar a validade dos *smart contracts* para o Direito brasileiro e a outra apresenta efetivamente como o Poder Judiciário deve ponderar a aplicação dos princípios.

2 O MODELO DE CONTRATO A SER CONSIDERADO

Os contratos inteligentes operam por meio de códigos de computação e, a depender de como são programados, executam funções específicas. Essas funções são determinadas pelo que os estudos denominam *script,* que nada mais é do que um comando redigido em linguagem de programação.[5] Um comando, nesse contexto, é uma previsão do contrato que determina que, observados alguns requisitos, uma consequência é prevista. Um exemplo de comando seria uma transação de certa quantia a uma "pessoa" – tecnicamente "endereço" – determinada, tal como este: "o valor de 0,0001 BTC pode ser resgatado pela chave pública 1KLasYmn3 CnFaJgg Uwq 3pdC9s93ebgVEs, cujo *hash* resulta em f54a1c3d7b2e9a1f4e9c7c07eab5c9c6421b2e2a". Nesse caso, o *script* determina que somente o titular da referida chave pública - que resulta no *hash* mencionado quando codificada – pode resgatar o ativo em Criptomoedas em questão.

Como mencionado, o comando é escrito em linguagem de programação, sendo os *scripts* compostos por poucos caracteres, como: "OP_DUP", "OP_HASH160", "MULTISIG" ou "OP_EQUALVERIFY". A figura 1 elucida como se apresentam os comandos de um *smart contract* de maneira mais real e concreta:

Figura 1 – Configuração dos comandos de *smart contracts*



Fonte: NARAYANAN, Arvind; BONNEAU, Joseph *et al*. **Bitcoin and cryptocurrency technologies: a comprehensive introduction**. Princeton, Nova Jersey: Princeton University Press, 2016. E-book, item 3.2, página variável.

Considerando a natureza dos comandos, pode-se deduzir que uma das funções mais relevantes desempenhadas por eles é determinar como as transações financeiras são operadas.

[5] NARAYANAN, Arvind BONNEAU, Joseph *et al*., **Bitcoin and cryptocurrency technologies: a comprehensive introduction**. Princeton, Nova Jersey: Princeton University Press, 2016. E-book, item 3.2, página variável.

Isso porque, sobretudo no estudo de contratos inteligentes de compra e venda, a forma como ocorre a transação dos criptoativos é o que determina se o contrato cumpriu adequadamente os seus fins ou se produziu uma relação injusta ou desequilibrada.

Imagine-se, nesse contexto, que duas pessoas elaboram um contrato de compra e venda de um produto físico, usando um *script* que permita o resgate automático de um valor tão logo seja notificado ao contrato que o produto foi postado pelo correio. Nesse caso, a utilização do *script* é inapropriada e gera desequilíbrio na relação contratual, porque é possível que o produto seja entregue com defeito e que já não haja como reverter a transação, pois os contratos inteligentes aplicam o código automaticamente, não havendo interferência externa que os faça parar. Assim, o uso de um *script* inapropriado permite que o vendedor receba a quantia acordada e que o comprador receba um produto defeituoso, desfecho injusto em relação ao comprador.

Por esse entendimento, compreende-se a variedade de contratos que há no que diz respeito à forma como a transação é realizada. Há contratos que determinam uma transação direta de criptoativos entre as partes, utilizando-se de *scripts* como "Pay to Public Key Hash (P2PKH)" ou "Pay to Script Hash (P2SH)".[6] Há contrato baseado no uso do *script* "MULTISIG", que permite a transferência dos criptoativos somente se múltiplas assinaturas forem dadas à transação, assemelhando-se a uma operação bancária de *escrow*.[7] A intenção dessa funcionalidade é conferir maior segurança às partes, já que a transferência de criptomoedas somente se dará se todas as partes envolvidas concordarem com a transferência ou, havendo discordância, se um terceiro de confiança tomar partido por algum dos lados.

Considerando os múltiplos contratos que podem se formar com a utilização de *scripts* de transferência, este trabalho terá como foco contratos *escrow*, ou seja, os que utilizam o *script* "MULTISIG". Essa escolha se fundamenta no propósito da pesquisa, qual seja, identificar formas de se garantir uma relação contratual não prejudicial às partes. É que, consonante o exposto, o modelo de contrato eleito já é, por si só, um mecanismo apto a minimizar as chances de um contrato de compra e venda promover um desfecho desequilibrado. Dessa forma, seria contraproducente conceber mecanismos de segurança aplicáveis a contratos cujos formatos já seriam facilitadores de relações comerciais não exitosas.

---

[6] BASHIR, Imran. **Mastering blockchain:** distributed ledger technology, decentralization, and smart contracts explained. 2ª ed. Birmingham, Reino Unido: Packt Publishing, 2018, p. 156 – 157.

[7] ORTOLANI, Pietro. Self-Enforcing Online Dispute Resolution: Lessons from Bitcoin. Publicação *online*: **Oxford Journal of Legal Studies**, 2015, p. 15.

2.1 O termo *escrow* e características do respectivo contrato

O modelo *escrow*, contrato inteligente enfocado neste trabalho, tem referências que remontam aos primórdios da tecnologia *blockchain.* Conhecer um pouco a origem do termo pode auxiliar entender o mecanismo de funcionamento desse tipo de contrato.

No âmbito de *blockchains*, o termo é usado para designar o modelo de transferência, no qual o fluxo de criptoativos é realizado somente com uma pluralidade de assinaturas.[8] A título exemplificativo, já em 2010, Satoshi Nakamoto[9] se referia à possibilidade de realização desse tipo de transação na plataforma *blockchain* em um fórum Bitcoin.[10]

A denominação *escrow*, no entanto, era utilizada antes do desenvolvimento de *smart contracts* no meio bancário e designava um modelo de transação, cuja essência era idêntica à ora operada em *blockchains*.[11] Na seara bancária, a parte que se compromete a realizar um aporte primeiramente movimenta o valor em questão para a conta de um terceiro que seja de confiança de ambas as partes. Assim, somente após o cumprimento de determinada cláusula, o terceiro transfere a quantia de sua conta para a parte credora.[12]

Esse modelo de transferência é utilizado como um meio de assegurar, àquele que transfere à conta *escrow,* que o dinheiro somente será destinado à outra parte se a contraprestação efetivamente ocorrer. Ele também confere maior segurança à outra parte sob o aspecto de que é mínima a chance de não receber, já que a parte contrária transferiu a quantia a um terceiro de confiança de ambos.

A transferência bancária, portanto, mostra-se bastante similar à técnica operada em *blockchains*, ressalvando-se, grosso modo, o meio em que opera – a operação em *blockchain* é diferente da realizada por um banco - e o fato de que, em *smart contracts*, não há propriamente uma "conta" à qual se possa transferir valores; há a titularização de criptomoedas que se dá de maneira peculiar.

Ante o exposto, é possível afirmar que a denominação *escrow* é utilizada em *smart contracts* em virtude de sua semelhança a uma classe de movimentação financeira já praticada por bancos. Ambos os modelos, ainda que estruturados sobre bases tecnológicas distintas, compartilham a mesma lógica de funcionamento: a interposição de um terceiro ou de um

---

[8] NARAYANAN, op. cit., item 3.3, página varivável.
[9] Pseudônimo da pessoa(as) responsável(is) pela criação do Bitcoin, primeira *blockchain* e criptoativo criados.
[10] NAKAMOTO, Satoshi. **Re: Transactions and Scripts:** DUP HASH160 ... EQUALVERIFYCHECKSIG." Fórum de Bitcoin, 17 Jun, 2010. Disponível em: https://bitcointalk.org/ Acesso em: 10 jun, 2025.
[11] Ibid.
[12] Ibid.

mecanismo imparcial que assegure o cumprimento das obrigações assumidas por ambas as partes. Assim, o modelo *escrow,* aplicado em *smart contracts,* representa uma reinterpretação técnica de um mecanismo de confiança que há muito tempo serve à segurança das relações negociais.

2.2 Operabilidade de contratos *escrow*

Compreendido o termo que designa a operação ora tratada, é oportuno analisar mais detidamente como ocorre uma transação *escrow*. Esse tipo de operação ocorre em *blockchain* com base em um *script* "MULTISIG". Diz-se que a transferência é de "múltiplas assinaturas" porque a movimentação do valor "estocado" por ela dá-se, apenas, com um número determinado de assinaturas.[13]

Nos termos de estudos internacionais, como os Bashir, Narayan e Filippi e Wright, nesse tipo de contrato, é necessário um "M de N" assinaturas: a letra "M" significa a palavra "mínimo" (ou *minimum*), usada para fazer referência ao mínimo necessário de assinaturas para que a transação seja autorizada; a letra "N" para significar a palavra "número" (ou *number*), em referência ao número total de endereços que podem autorizar a transação.[14]

A fim de elucidar o funcionamento dessa transação, entende-se oportuno fazê-lo por meio de um exemplo prático. Suponha-se que José Ângelo e Maria Alice – vendedor e compradora – queiram formalizar um contrato de compra e venda de um smartphone e, para tanto, utilizem um contrato inteligente do tipo *escrow*. Para que o contrato traga maior segurança para as partes, é constituído um terceiro, Josemaría, que assim como os outros dois, possui o poder de assinar a transação, determinando a transferência dos fundos a qualquer uma das partes. No contrato, ficou estipulado que o valor depositado na conta poderá ser enviado ao vendedor ou devolvido ao comprador – em caso de litígio – mediante duas assinaturas no mínimo, as quais podem ser dadas pelos três envolvidos.

Nessa condição, Maria Alice criará uma transação do tipo *multisig,* que é o contrato em si, segundo a qual somente poderá ser resgatado o valor previsto, 0,0076 Bitcoins (BTC)[15], referente ao produto negociado, a uma conta *escrow*, que não é administrada por uma pessoa,

---

[13] BASHIR, 2018, p. 113. "Assinatura" é uma assinatura digital, criada por um processo criptográfico que garante a autenticidade e a integridade de uma transação. :

[14] LANTZ, Lorne; CAWREY, Daniel**. Mastering blockchain:** unlocking the power of cryptocurrencies, smart contracts, and decentralized applications. Sebastopol, California: O'Reilly Media, 2021. E-book, Capítulo 5, item *Multisignature Contracts*, página variável. (página variável.

[15] XBT é também uma sigla usada para Bitcoins, criptomoeda utilizada no exemplo.

mas que se rege autonomamente com base na tecnologia *blockchain*.[16] Conforme o contrato firmado – que consiste na transferência *multisig* -, somente poderá ser resgatado o valor do produto mediante assinatura de, ao menos, duas das três partes. A assinatura é computada a partir de o envio, pela parte, de uma mensagem assinada à conta *escrow*.[17]

Essa transação, ao ser incorporada à *blockchain*, passa a ser válida coletivamente, o que dá segurança a José Ângelo e o faz enviar o bem negociado a Maria Alice. Uma vez recebido o smartphone, Maria Alice e José Ângelo assinam a transferência criada e, automaticamente, o valor indicado pela compradora passa para o vendedor. Ou seja, somente com o recebimento das duas assinaturas – número mínimo estipulado – houve a transação do valor ao vendedor.

Imagine-se, em outro aspecto, que o produto não tenha chegado ao endereço de Maria Alice por má-fé do vendedor e que, em consequência, ela não queira assinar a transferência. Nesse caso, o número mínimo de assinaturas somente será alcançado se for acionado o terceiro constituído. Assim, as partes enviam dados e provas a Josemaría para esse possa decidir quem tem a razão e ele conclui que José Ângelo agiu de má-fé, intentando obter lucro sem o envio do produto. Dessa forma, Josemaría e Maria Alice irão enviar duas mensagens assinadas à conta *escrow* determinando o estorno em favor da compradora.

Veja-se, portanto, que José Ângelo não está apto a tornar-se proprietário do valor acordado somente com sua assinatura; é necessário que outra parte assine para que efetivamente ocorra a transação. Da mesma forma, se Maria Alice estivesse descontente com a compra por algum motivo – seja pelo não recebimento ou por algum defeito na mercadoria – , não poderia determinar que o valor retornasse a ela novamente somente com sua assinatura. Por razões como essas, a constituição de Josemaría, neste caso, é recomendável, já que ele pode analisar a questão e decidir como irá assinar, determinando a quem a quantia se destinará.

Como visto, a transação *escrow* é um mecanismo do *script* MULTISIG em *blockchain,* que proporciona maior segurança às partes envolvidas em negócios, vendedores e compradores, ao exigir um número mínimo de assinaturas ("M"), entre o número total de assinaturas possíveis ("N"), para movimentação dos fundos. Essa estrutura garante que nenhuma das partes aja unilateralmente. A inclusão de um terceiro imparcial fortalece a confiança, ao mediar disputas e concluir a quem o valor do negócio será destinado; assegurando a lisura da transação.

[16] DE FILIPPI; WRIGHT, op. cit., p. 76.
[17] Ibid.

2.2.1 Comparação com transferências bancárias

Uma transação *escrow* em *blockchain* é essencialmente idêntica a uma transação *escrow* operada por um banco. Em ambos os casos, envolve-se um terceiro para intermediar o processo, de modo que a movimentação definitiva da importância ocorra somente com a anuência de ambas as partes ou que, ao menos, se dê com a anuência de uma das partes e do terceiro constituído, esse, de confiança dos contratantes.[18]

As diferenças entre a transação *escrow* em *blockchain* e a *escrow* dos bancos são em relação ao ambiente em que ocorrem e à forma de operacionalizar a movimentação. No sistema bancário, a transferência se dá por meio da movimentação de um valor para a conta de um terceiro, o qual, quando for oportuna a movimentação para o credor, realiza uma transferência de sua conta bancária ao beneficiário. Nesse meio, o terceiro – ainda que sob pena de responder judicialmente por descumprimento de um contrato – tem a liberdade de transferir o valor ainda que não se cumpram as cláusulas. Isto é, uma transferência bancária, geralmente, não é automatizada; depende da ação de um terceiro para que a movimentação se realize. Para além disso, uma transferência bancária é centralizada no sentido de que depende da intermediação de um órgão central que controle todas as transações e que as operacionalize.

Já no sistema *blockchain*, o valor é transferido pela parte pagadora a uma conta *escrow*, controlada por um terceiro, mas que possui autonomia. Nesse modelo, a conta *escrow* somente promove a movimentação a da quantia "estocada" para uma das partes se houver um número mínimo de assinaturas.[19] Alcançado o número mínimo de assinaturas, então, a transferência ocorre automaticamente e não pode ser revertida. Assim, cumpridos os requisitos, não há como evitar que ocorra o que foi acordado, isto é, não pode haver transferência antes do cumprimento dos requisitos.

Percebe-se, portanto, duas diferenças fundamentais em relação ao sistema bancário: a conta *escrow* não é titularizada por uma pessoa, e a transferência se realiza automaticamente, se cumpridos os requisitos.[20] Por fim, a operação se dá em *blockchain* de maneira descentralizada, visto que o acordo se cumpre sem necessidade de uma autoridade central que intermedeie as movimentações, o que se passa em uma transferência bancária.

Conclui-se que a transação ***escrow*** em ***blockchain***, embora conceitualmente similar à operada por bancos, ao envolver um intermediário e a anuência das partes, difere

[18] NARAYANAN et. al., op. cit.,item 3.3 página variável.
[19] O cômputo da assinatura é realizado na conta *escrow* a partir do envio de uma mensagem digitalmente assinada pela parte ou pelo terceiro envolvido – árbitro.
[20] DE FILIPPI; WRIGHT, op. cit., p. 76.

fundamentalmente dessa em sua operacionalização e ambiente. Enquanto no sistema bancário a transferência depende da ação manual e centralizada de um terceiro, com a possibilidade de descumprimento, em *blockchain*, a quantia é enviada a uma conta *escrow* autônoma. Essa conta é desprovida de titularidade humana e executa a movimentação de forma automática e irreversível**,** uma vez atingido o número mínimo de assinaturas. Essa característica assegura a descentralização e a execução inalterável dos acordos, eliminando a dependência de uma autoridade central e conferindo maior segurança e previsibilidade às partes envolvidas.

3 UTILIZAÇÃO DE ORÁCULOS

O capítulo anterior delimitou o objeto de estudo deste trabalho, introduziu os contratos inteligentes de múltiplas assinaturas e esclareceu que esta modalidade de contrato oferece maior segurança às partes, já que uma parte não pode resgatar o valor acordado por si só. Pelo descrito, é possível cogitar que o problema proposto pudesse estar respondido, bastando utilizar uma *escrow account* para remediar uma situação na qual o comprador sai prejudicado da compra.

De fato, a transação *escrow* é uma ferramenta que remedeia alguns possíveis problemas. Porém, o formato do contrato, puro e simples, não solucionaria o problema se não contasse com a inteligência humana aplicada, representada, no exemplo, pela figura de Josemaria. A inteligência humana envolvida – capacidade de discernir a quem cabe a razão – é algo externo ao contrato, já que foge aos códigos que compõem a transação. Daí, deduz -se que a *escrow account* não resolve o problema por si só, mas sim, deve ser aliada a elementos que permitam trazer um código externo à *blockchain,* de modo a conferir cumprimento ao contrato inteligente.

Esses elementos, que trazem informações do ambiente externo à *blockchain,* para que o *smart contract* funcione adequadamente, é denominado oráculo. Oráculos, portanto, constituem parte da solução para eventuais na transação.

3.1 Introdução

A solução de problemas na compra e venda de produtos, realizada por meio de *smart contracts,* pode se dar com base na utilização de oráculos. Antes, porém, de se justificar a aplicação dessa tecnologia aos contratos, explicar-se-á em que consistem os oráculos.

Oráculos são indivíduos ou programas que trazem informações do mundo real para o âmbito dos contratos inteligentes, para que esses funcionem adequadamente.[21] Em termos técnicos, são serviços que levam dados de recursos *off-chain*[22] (ambiente externo à *blockchain)* às *blockchains;*[23] tecnologia fundamental para esse fim, já que tais contratos frequentemente necessitam de dados da realidade para poderem ser cumpridos de forma adequada.

Para tornar clara a necessidade de oráculos, é possível pensar em um exemplo prático de contrato inteligente *escrow* para compra e venda de um produto físico, o que exemplifica o contexto da problemática deste trabalho.

Imagine-se um contrato para compra de uma máquina de lavar roupas. As partes optam por um contrato *escrow* para operacionalizar a transação. No contexto da elaboração do contrato, entenderam que, para tornar a transação mais segura e eficiente, seriam utilizados um sistema arbitral –adaptado a contratos inteligentes e utilizado em eventual situação litigiosa – e dispositivos capazes de informar a localização do produto em tempo real ao contrato inteligente.

Entenderam as partes, ainda, que, por razões de segurança, seriam estabelecidos alguns prazos para o processo. Um dos prazos seria o da chegada do produto. Se a mercadoria não chegasse dentro desse prazo, seria enviada automaticamente uma mensagem ao contrato – por meio dos dispositivos de localização mencionados -, ativando-se imediatamente o sistema de arbitragem constituído. Outro prazo seria constituído tanto para delimitar um período no qual o comprador, ao receber o produto, pudesse alegar eventual defeito, quanto para determinar a liberação automática do valor ao vendedor. Isso, se o comprador não se manifestasse tempestivamente acerca de possível defeito.

Definiu-se, por fim, que, em situações de litigância levadas ao árbitro, o valor poderia tanto ser transferido ao vendedor , caso se concluísse pela má-fé do comprador, quanto ser estornado em favor do comprador, na hipótese de má conduta do vendedor.

Prosseguindo com o exemplo: a máquina de lavar é despachada e, alguns dias depois, a entrega é devidamente confirmada pelos dispositivos de localização dentro do prazo estipulado. O comprador, satisfeito com a chegada do produto, procede à instalação e ao uso da máquina de lavar. No período de teste estabelecido, o comprador não identifica qualquer defeito ou

---

[21] DE FILIPPI; WRIGHT, op. cit, p. 75. Para esses autores, “Oracles can be individuals or programs that store and transmit information from the outside world, thereby providing a means for blockchain-based systems to interact with real-world persons and potentially react to external events”.

[22] Neste trabalho, serão utilizados os termos *off-chain* e *on-chain,* para significar, respectivamente, o ambiente externo à *blockchain* e o ambiente interno da *blockchain*.

[23] BREINDENBACH, Lorenz; CACHIN, Cristian; CHAN, Benedict; COVENTRY, Alex; ELLIS, Steve et al. **Chainlink 2.0:** Next Steps in the Evolution of Decentralized Oracle Networks. 2021, p. 6. Disponível em: https://chain.link/whitepaper, Acesso em 1 jun 2025.

problema com o equipamento. Decorrido o prazo, sem qualquer manifestação de sua parte sobre a identificação de vícios, o contrato inteligente executa automaticamente a liberação do valor retido em garantia, transferindo-o integralmente para o vendedor; esse recebe o pagamento sem intercorrências. A transação é concluída de forma eficiente e sem necessidade de intervenção externa, comprovando a eficácia do contrato inteligente para operações transparentes e seguras.

Em contrapartida, considere-se uma situação distinta: após a chegada da máquina de lavar, o comprador verifica que o produto apresenta um defeito grave que impede seu funcionamento. Então, notifica o contrato inteligente dentro do prazo estipulado para alegação de vícios. Automaticamente, uma mensagem é enviada ao contrato inteligente, e esse aciona, de imediato, o sistema de arbitragem previamente definido pelas partes. Um árbitro é notificado sobre a disputa e inicia o processo de análise. Durante a arbitragem, o vendedor pode argumentar que o defeito pode ter sido causado pelo comprador, mas esse apresenta um laudo técnico comprovando o vício de fabricação. Após avaliar as evidências e os argumentos das partes, o árbitro conclui que o defeito é de responsabilidade do vendedor, pois o produto foi entregue em desacordo com o ajustado. O árbitro determina que o valor retido em garantia seja estornado em favor do comprador e que o vendedor providencie a retirada do produto. A decisão arbitral é enviada ao contrato inteligente, que executa o estorno e encerra a disputa de forma justa e imparcial, protegendo os interesses do comprador ante a falha do vendedor.[24]

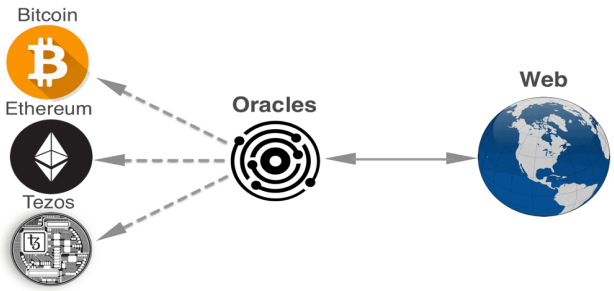
Com base na observação dos exemplos, a funcionalidade do contrato inteligente depende da **obtenção de dados externos à *blockchain***. A confirmação da entrega do produto por meio de dispositivos de localização, entre outras, é informação que, por sua natureza, não reside diretamente na rede *blockchain*. É nesse ponto que a **importância dos oráculos** se torna evidente. Foram eles, na figura dos dispositivos de localização e do sistema arbitral - atuando como fonte de informação para a decisão -, os responsáveis por alimentar o contrato inteligente com os dados *off-chain* necessários para que as cláusulas fossem devidamente executadas. Sem a capacidade de acessar e de validar essas informações do mundo real, o contrato inteligente, por si só, teria limitada sua aplicabilidade pelos eventos concretos e, consequentemente, incapaz de cumprir seu propósito de automatizar e garantir a segurança das transações.

Frente a esse panorama, é oportuno mostrar um esquema elucidativo a respeito do funcionamento de um oráculo. A figura 2 ilustra esse funcionamento,[25] tornando graficamente

[24] DE FILIPPI; WRIGHT, op. cit., p. 239. Exemplo inspirado na explicação desses autores, nota de rodapé n.º 23 do capítulo 4.
[25] THE MONEY MONGERS. **What Are Blockchain Oracles?** Disponível em: https://themoneymongers.com/ Acesso em 1 jun de 2025.

inteligível a função primordial de oráculos, de operar um intercâmbio entre o mundo externo e a *blockchain*. O exemplo é das plataformas Bitcoin, Ethereum e Tezos.

Figura 2 - Funcionamento de um oráculo



Fonte: The Money Mongers, 2023, p. 1

Extrai-se, portanto, que os **oráculos** são tecnologias essenciais para o funcionamento adequado dos ***smart contracts***, servindo como pontes entre o mundo real e as ***blockchains***. Eles consistem em indivíduos ou programas responsáveis por fornecer dados *off-chain* – informações externas à *blockchain* – que são cruciais para que os contratos inteligentes possam ser executados de forma eficaz. A necessidade desses dados se manifesta em diversas situações, como no exemplo de um contrato de compra e venda, no qual um oráculo é fundamental para verificar o estado de um produto e determinar a correta movimentação dos fundos, garantindo assim a resolução de problemas e o cumprimento preciso dos termos contratuais.

3.2 Tipos de oráculo

Dentro daquilo que representam, há oráculos de vários tipos, e conhecê-los é importante para compreender a natureza dessa ferramenta. Da grande variedade encontrada, neste trabalho serão referidos os mais citados pelos autores citados nesta pesquisa.

De início, distinguem-se "oráculos de entrada" de "oráculos de saída", sendo os termos utilizados em âmbito internacional *inbound* e *outbound oracles*.[26] Oráculos de entrada, *inbound oracles*, são aqueles que recebem dados externos e os inserem nos contratos inteligentes, cumprindo sua principal função, qual é a de "instruir" *smart contracts*, conferindo a eles

[26] BASHIR, Imran. **Mastering Blockchain:** a deep dive into distributed ledgers, consensus protocols, smart contracts, dapps, cryptocurrencies, ethereum, and more. 3rd. ed Birmingham, Reino Unido: Packt Publishing, 2020. E-book, capítulo 10, iem 5, página variável.

adequada funcionalidade e adequado cumprimento. Por seu turno, oráculos de saída, *outbound oracles*, são os que promovem o fornecimento de dados no sentido reverso, ou seja, do contrato inteligente para o mundo externo.[27]

Relativamente aos oráculos de entrada, *inbound,* sua classe é mais ampla em termos de variedade tecnológica, sendo possível estabelecer categorias distintas de oráculos com base em suas características. Nessa classe, as principais categorias são: oráculos de *software*, de *hardware,* de computação, baseados na agregação de dados, descentralizados, inteligentes e oráculos humanos.[28]

Oráculos de *software* são aqueles utilizados para adquirir dados disponíveis no âmbito da internet, tais como *Application Programming Interface* (APIs)[29], bases de dados e páginas da internet. Pela simplicidade desses tipos de oráculo - visto não ser complexa a tarefa de realizar buscas em informações contidas na internet -, eles são conhecidos por "oráculos padrão" (*standard oracles*) e por "oráculos simples" (*simple oracles*).[30]

Oráculos de *hardware* são os que obtêm informações de *hardwares*, tais como sensores que captam dados do mundo físico e sensível e dispositivos integrados à internet das coisas, *Internet of Things* (IoT).[31] Esse tipo é particularmente útil a contratos inteligentes, cujo objeto seja o serviço de seguro. Isso, porque tais contratos exigem o conhecimento de dados fáticos para se saber se a parte pode ser ressarcida ou não pelo sinistro ocorrido.[32]

Oráculos de computação, *computation oracles,* são úteis para obter resultados de cálculos complexos alheios à *blockchain*. Um aparato computacional de alta performance realiza os cálculos requeridos, e o oráculo fornece os resultados ao contrato inteligente.[33]

Os oráculos baseados na agregação de dados, como a denominação indica, colhem informações em fontes distintas e as agregam para chegar ao dado mais adequado ou mais verdadeiro. Esse tipo pode ser melhor compreendido por meio de um exemplo prático: imagine-se um contrato inteligente, que envolva muito dinheiro, necessite de um dado financeiro que possa variar entre as fontes disponíveis externas à *blockchain*. Pelo vulto do *smart contract* e

---

[27] Ibid.
[28] Ibid.
[29] ENCYCLOPEDIA BRITANNICA.A expressão designa uma tecnologia que, em suma, permite que uma comunicação entre programas de computador. Tal conceito, com maiores explicações, pode ser retirado da página da Disponível em: https://www.britannica.com/. Acesso em: 2 jun 2025.
[30] BASHIR, 2020, capítulo 10, item 5 ,número de página variável.
[31] ORACLE. **O que é IoT? "**Rede de objetos físicos incorporados a sensores, software e outras tecnologias com o objetivo de conectar e trocar dados com outros dispositivos e sistemas pela internet." Inclui desde "objetos domésticos comuns a ferramentas industriais sofisticadas". Por meio dela, pode-se" compartilhar e coletar dados com o mínimo de intervenção humana". Disponível em: https://www.oracle.com/br/ Acesso em: 16 jun 2025.
[32] Ibid.
[33] Ibid.

pela variabilidade do dado de que se necessita, não é prudente que se tome como correta a primeira informação obtida; é necessário analisar as várias informações disponíveis para se operar uma eleição ou bem, conforme a natureza do dado, uma média dos valores encontrados.[34]

Oráculos descentralizados, por sua vez, são mecanismos que realizam um intercâmbio entre os ambientes *on-chain* e *off-chain*, de modo que as informações a serem usadas na *blockchain* venham de variadas fontes, passem por um mecanismo de consenso e prescindam de uma fonte centralizada, minimizando a chance de se utilizar uma informação imprecisa. Vê-se que o conceito e a função desse tipo de oráculo são muito semelhantes às do tipo de oráculo tratado no parágrafo anterior; ambos os mecanismos retêm informações distintas e as selecionam. De fato, os mecanismos são similares, mas o conceito do tipo de oráculo aqui abordado é mais amplo, abrangendo mais possibilidades e mecanismos.

Nesse sentido, um oráculo baseado na agregação de informações é exemplo específico de oráculo descentralizado, embora haja muitos outros modelos de oráculos descentralizados. A título de exemplo, há possibilidade técnica de se obter uma informação de outra *blockchain.* Nesse caso, o dado é descentralizado, já que passou por um processo de consenso em outra *blockchain.* Mas, considerando somente a *blockchain* que se utilizará da informação, não houve captação de diversas fontes e sim, de apenas uma, isto é, a outra *blockchain*. Ou seja, nesse caso, utilizou-se um oráculo descentralizado, mas não um baseado na agregação de dados. Em síntese, um oráculo descentralizado consiste em mecanismo que obtém informação da *off-chain* por processo descentralizado, isto é, envolve variadas fontes e mecanismo de consenso ou seleção. A fonte é externa à *blockchain* do contrato, mas não é externa a tecnologia *blockchain*. Isso é fundamental para a identificação desse oráculo.[35]

Os oráculos inteligentes, *smart oracles,* têm uma característica que os torna muito eficientes e curiosos: eles não somente captam informações do meio externo para repassá-las à *blockchain,* como executam, eles mesmos, o código do contrato no ambiente externo à *blockchain*.[36]

Por fim, estudiosos do assunto, como Bashir, Narayan e Filippi e Wright, admitem os oráculos humanos, os quais, tal como o nome, consistem no acionamento da inteligência humana para que informações relevantes sejam inseridas na *blockchain,* e o contrato inteligente funcione adequadamente. A inteligência humana, em geral, é utilizada com um fim arbitral,

---

[34] Ibid.
[35] BREINDENBACH et al., op. cit., p. 7.
[36] BASHIR, 2020, capítulo 10, item 5, página variável.

dirimindo conflitos entre as partes e determinando a qual dela cabe a razão.[37] Essa classe de oráculo é bastante aplicável, dada a capacidade de uma pessoa de analisar informações sobre o cumprimento ou descumprimento de um contrato.

No que tange aos oráculos de saída, *outbounds*, sua operação consiste na transmissão de dados presentes na *blockchain* para o ambiente externo, como referido. Esse processo pode se dar, por um lado, quando a *blockchain* produz dados que são úteis a outra *blockchain*, seja qual for o motivo. Por outro, ele pode ser útil quando um dispositivo físico externo à *blockchain* necessita operar uma tarefa em resposta a uma transação ocorrida no ambiente da *blockchain*.[38]

Pelo exposto, vê-se que múltiplas são as possibilidades de se conferir adequado cumprimento e funcionamento a *smart contracts*. Com base nisso, torna-se mais viável pensar em possibilidades de solução para eventuais problemas que possam surgir.

3.3 Confiabilidade dos dados obtidos por oráculo

Os oráculos foram conceituados e foram vistos seus principais tipos, do que se depreende que, seja qual for a espécie, eles têm como principal tarefa a transmissão de dados, seja do ambiente externo para a *blockchain,* seja no sentido contrário. Nesse movimento operacional, uma indagação fundamental que se faz presente diz respeito à confiabilidade das informações obtidas por oráculos. Trata-se de uma questão pertinente, haja vista o regular funcionamento de um contrato inteligente não requerer apenas uma informação qualquer, mas um dado fidedigno ou correto.

Tratar dessa temática implica levar em conta, propedeuticamente, que a variabilidade dos tipos de oráculos faz com que sejam necessárias soluções adequadas a cada espécie; dificilmente se pode sustentar uma solução geral aplicável a todas as classes de oráculos. Nesse sentido, uma solução aplicável a oráculos de *hardware*, que recebe dados obtidos por um termômetro ambiente, não poderá ser aplicável a um oráculo simples, que obtém informações da internet, já que as fontes de informações são substancialmente distintas.

Nessa perspectiva, o presente subtópico não objetiva exaurir os vários meios de garantir a segurança de dados obtidos por oráculos - dado que tal empreendimento fugiria aos fins deste subtópico meramente introdutório à discussão central -, mas apenas apresentar algumas técnicas admitidas pela doutrina especializada e que são aplicáveis aos principais tipos de oráculos.

---

[37] DE FILIPPI; WRIGHT, op. cit., p. 239.
[38] BASHIR, 2020, capítulo 10, item 5, página variável.

Uma primeira técnica a ser considerada é a utilização de oráculo, cuja fonte seja notoriamente confiável, considerando sua projeção, sua fama ou sua história. Essa proposta é aceita com ressalvas por estudiosos como Bashir, Narayan e Filippi e Wright, já que a boa fama de uma fonte não impede erros no dado, ainda que ofereça uma boa garantia de acerto.

Outro problema que se pode assinalar nesse sentido é que a obtenção de informação é centralizada, divergindo do princípio histórico e essencial de *blockchains* e dos *smart contracts*, qual seja o da descentralização.[39] Considera-se que há centralização quando a obtenção do dado se realiza em uma fonte acessada por muitos usuários, em função da sua pressuposta confiabilidade. Essa fonte concentra muitos "consumidores", em um movimento contrário ao concebido para *blockchains*, qual seja o de descentralização de relações.[40]

De qualquer forma, ainda que não seja uma solução imune a falhas, é uma forma a ser considerada para que se garanta o bom aproveitamento do dado pelo contrato inteligente. Entretanto, não é aplicável a todos os tipos de oráculos, sendo válida para oráculos de *software* e para oráculos de computação, isto é, classes listadas neste trabalho.

Essa solução pode ser aplicada a oráculos de *software*, porque esses, como dito, acessam informações na internet, tornando aplicável eleger uma fonte presente na rede mundial de computadores que seja confiável.[41] Entende-se que pode ser aplicada a oráculos de computação, já que pressupõe a possibilidade de eleição de um sistema computacional mais confiável por seus atributos, de modo a centralizar, nele, a fonte de cálculos necessários ao *smart contract*.

A segunda técnica passível de adoção consiste na obtenção de dados de diferentes fontes, de modo que, comparando-se todos os obtidos, verifique-se qual provavelmente é o mais verdadeiro, com base na frequência com que é transmitido.[42] Exemplo: se o dado a ser obtido for a temperatura atual em determinada cidade, verificar-se-á que um determinado valor aparece mais frequentemente, ainda que poucos dados alternativos sejam reportados. Nesse caso, a comparação entre os vários resultados levaria ao juízo de que o dado mais frequente é o mais seguro e idôneo para ser utilizado no *smart contract*.

Em consonância com o descrito, essa segunda técnica não somente é viável em teoria, como é plenamente aplicável, amoldando-se aos oráculos capazes de compilar dados de diversas fontes, categoria de oráculos tratada no tópico anterior.

---

[39] DE FILIPPI; WRIGHT, op. cit., p. 20 - 29. Os autores descrevem como historicamente esteve presente o atributo da descentralização na tecnologia *blockchain*.

[40] BASHIR, 2018, p. 271. Ele entende que a busca por uma fonte reconhecidamente confiável peca pela centralização que promove.

[41] Ibid., p. 271.

[42] Ibid., p. 271.

Pode-se conceber, ainda, uma terceira técnica como forma de garantir dados mais fidedignos, sendo essa com base em oráculos descentralizados, igualmente abordada no tópico anterior. Aqui a confiabilidade do dado provém do mecanismo de consenso estabelecido entre os "nós" [43]que integram uma rede de oráculos descentralizados; uma mesma informação é buscada por oráculos de vários "nós" que integram o sistema de oráculos. As informações obtidas por todos são processadas, sendo utilizada a provável de ser correta.

Por fim, é pertinente tratar da confiabilidade de dados obtidos por oráculos humanos, já que esse tipo é aplicável à solução do problema proposto neste trabalho. Como mencionado, oráculos humanos têm como fundamento a inteligência humana e se prestam principalmente a resolver litígios contratuais que venham a surgir na condição de árbitros.[44]

A confiabilidade desse oráculo provém da vontade das partes, que consentiram em constituir um terceiro como árbitro em eventual conflito entre elas. Sob essa égide, ainda que eventualmente seja passível de erro – algo inerente à natureza humana –, a decisão tomada pelo terceiro constituído árbitro se mostra a solução mais adequada fornecida pelo oráculo, visto que o contrato estipulado é cumprido cabalmente, observando-se a vontade das partes.

Pelo exposto, é possível conceber que, dada a importância das informações obtidas para a apropriada execução de um contrato inteligente, é necessário garantir que os dados coletados sejam fidedignos e adequados. Para tal, há formas eficazes de se garantir a veracidade dos dados, como: utilização de fontes notoriamente seguras – método criticado por estudiosos do assunto; uso de oráculos capazes de captar dados de diversas fontes – analisando-se os mais provavelmente verdadeiros; uso de oráculos descentralizado – que obtêm informações de outras *blockchains*, garantindo o sistema de consenso a veracidade do dado; utilização de oráculos humanos – que se mostram idôneos pela vontade das partes do contrato inteligente.

3.4 Aplicação de oráculo humano ao problema central

Como visto, oráculos humanos são aplicáveis à solução do problema aventado, o que vai ser enfatizado, demonstrando-se que a inteligência humana é uma ferramenta muito útil à solução de problemas entre comprador e vendedor em uma transação *escrow*.

Conforme o que já se introduziu, sabe-se que o oráculo funciona como um intercâmbio entre os ambientes *on-chain* e *off-chain*, de modo que podem ser utilizados para dar

[43]DE FILIPPI; WRIGHT, op cit., p. 2. "Nó" é um computador que armazena uma cópia da *blockchain* e valida os blocos que se formam na cadeia. "Os nós armazenam cópias exatas, ou quase exatas, da *blockchain* e coordenam usando um protocolo de *software* que precisamente dita como os participantes da rede devem armazenar informação, realizar transações e executar o código de *software*" (tradução livre).
[44] DE FILIPPI; WRIGHT, op. cit., p. 76, 239.

cumprimento satisfatório a contrato inteligente a partir da obtenção de dados não presentes no ambiente interior à *blockchain*.[45] Com base nisso, é possível sustentar a aplicação da tecnologia se configurada, no caso proposto, a necessidade de obtenção de dado não presente no âmbito da *on-chain*. Levando em consideração esse argumento, será evidenciada a necessidade da inteligência humana – externa, portanto, aos meros recursos presentes na *blockchain*, que se limitam aos códigos –, comprovando-se a aplicabilidade de oráculo com base humana.

A fim de se demonstrar o que se propõe, é necessário inicialmente contextualizar a questão, o que pode ser feito por meio de um exemplo. Imagine-se que duas partes estabelecem uma avença: Maria de Fátima se compromete a comprar uma máquina de café expresso e Marina se compromete a enviar o produto mediante o pagamento do devido valor.

Tratando-se de compra e venda de produto físico, as partes, cientes do funcionamento de um contrato inteligente, entendem ser mais seguro utilizar um contrato que necessite da assinatura de, ao menos, duas pessoas. Assim, constituem José Francisco como um terceiro que servirá como um árbitro entre elas se houver eventual litígio. O valor da máquina não pertencerá a Marina, a menos que duas das três pessoas assinem o contrato nesse sentido.

Estabelecida a transação e estando ela devidamente inserida na *blockchain*, Marina, tranquila por saber que a quantia já foi estabelecida no contrato, envia a máquina a Maria de Fátima, sabendo que somente será titular do valor se a destinatária comunicar ao contrato que pode ser feita a transferência. Ao receber a máquina, no entanto, Maria de Fátima percebe que ela apresenta um defeito que não foi previamente informado ou previsto no acordo. Se Marina não reconhecer o defeito e se recusar a assinar a transação que libere o valor de volta a Maria de Fátima, será necessário que José Francisco atue no caso para resolver o litígio, já que, somente com a assinatura desse terceiro se poderá alcançar o mínimo de duas assinaturas para o valor ser destinado a uma ou outra parte. Isto é: o valor só será transferido a Marina se essa e José Francisco assinarem determinando a transferência ou a quantia somente retornará à Maria de Fátima se essa e José Francisco assinarem determinando esse retorno.

Porém, para que José Francisco decida a assinar em favor de uma ou de outra, é necessário que ambas as partes enviem provas que corroborem suas versões dos fatos. No caso da compradora, é importante que envie fotos ou vídeos que comprovem o defeito da máquina.[46] No da vendedora, ela deve enviar provas de que o produto estava em perfeito estado antes do

[45] Ibid., p. 75.

[46] Essa etapa pode ocorrer no ambiente *off-chain,* como permite inferir Primavera De Filippi e Aaron Wright na obra já mencionada neste trabalho, na página n.º 239, na nota de rodapé n.º 23. Dessa forma, as partes podem enviar o material a José por algum aplicativo de mensagem, por exemplo.

envio. Com base nas informações prestadas, José Francisco chegará a uma conclusão sobre quem tem a razão e, consequentemente, decidirá qual parte será beneficiada por sua decisão.

O mesmo raciocínio se aplica à hipótese de o produto não ser recebido por Maria de Fátima. Nesse caso, a compradora se recusaria a assinar a transação, uma vez que o produto não chegou, sendo injusto que a vendedora receba o valor. Essa, por sua vez, não seria capaz de receber o valor utilizando somente sua assinatura, necessitando que José Francisco assine o contrato de maneira favorável a ela. Nesse cenário de não envio do produto, portanto, o mesmo impasse se apresenta e torna necessária a intervenção de oráculo humano, capaz de analisar dados enviados pelas partes a fim de decidir qual das duas possui razão e, consequentemente, assinar a transação favoravelmente a uma delas.

Percebe-se, nesse contexto, que um oráculo humano é idôneo para resolver o problema proposto, tanto no caso de produto defeituoso, quanto no caso de o produto não ser entregue ao comprador. Essa adequação diz respeito à capacidade humana de analisar o estado em que foi entregue o produto e de verificar se o produto foi entregue ou não, o que permite que a assinatura faltante ao contrato se dê de forma justa.

3.5 Uso de oráculo de *hardware*

Diante do eficiente desempenho de um oráculo humano na solução dos cenários litigiosos, pode-se pensar que não há possibilidade de se empregarem outras classes de oráculos na resolução almejada. Mas essa cogitação se mostra equivocada, tendo em vista que outros oráculos podem ser empregados, para consecução do objetivo enfocado.

Uma alternativa ao oráculo humano, por exemplo, é o oráculo de *hardware*, o qual, como visto, vale-se de informações obtidas por sensores postos no mundo físico e pela internet das coisas para aplicá-las ao ambiente *on-chain*.[47] Esse cenário, conquanto pareça demasiadamente futurístico, já é realidade e é aplicado por empresas, como: VeChain (San Marino/Europa), AirDAO (Ilhas Cayman/território britânico no Caribe) e XYO Network (Califórnia/Estados Unidos da América). [48]

Nessa alternativa, sensores capazes de transmitir informações ao ambiente *on-chain* são acoplados ao produto ou mesmo ao pacote no qual será transportada a mercadoria. A depender da funcionalidade da tecnologia oferecida, tais sensores são capazes de transmitir ao *smart*

[47] BASHIR, 2020, op. cit., capítulo 10, item 5, página variável.
[48] Informações nos respectivos endereços oficiais: https://vechain.org/; https://airdao.io/; https://xyo. network/.

contract informações que denotem dano ao produto ou que informem se o produto sequer chegou ao destino, fatos que impedem que o comprador sofra prejuízo.

Sendo assim, para solucionar problemas de descumprimento de contratos inteligentes usando oráculos de *hardware*, sugere-se uma alternativa que se baseia apenas na utilização deste tipo de oráculo e que se mostra viável, ao menos se considerada a supramencionada empresa VeChain.[49] Nesse modelo, deve ser criada a transação *escrow* e, junto a ela, um contrato de seguro, que desempenhe o papel de garantir que um eventual erro por parte da transportadora não acarrete prejuízo ao vendedor.

No contrato criado, devem ficar estabelecidos local, prazo para a entrega da mercadoria e condições que garantam a integridade física do produto, de modo que, cumpridos os requisitos, o valor passe a ser titularizado pelo vendedor. Se qualquer dos requisitos não for cumprido, o contrato aciona o seguro, e esse deve ressarcir o comprador.

Os requisitos de entrega em local, prazo e condições da mercadoria específicos são possíveis de se estabelecerem graças às possibilidades vigentes no âmbito da internet das coisas. A empresa VeChain, por exemplo, permite que um vendedor anexe um módulo de IoT ao produto ou mesmo ao pacote por meio do qual é enviado.

Esse módulo contém um receptor GPS, um chip NB-IoT[50] e sensores, os quais permitem, respectivamente, identificar a localização do produto, verificar alterações físicas - como umidade, temperatura e impacto, por exemplo - no ambiente no qual está inserido e processar as informações coletadas, enviando os dados a uma torre de rádio. Nessa torre, as informações se integram à internet e alcançam o contrato inteligente.[51]

Em síntese, tais módulos averiguam o cumprimento ou não dos termos do contrato, pois verificam se o produto chegou ao local determinado, no prazo estipulado e se não sofreu alguma intempérie que pudesse alterar as condições do contrato. Se descumprido algum requisito, os sensores transmitem a informação ao contrato e, automaticamente, aciona-se o seguro.

Exposta a solução em teoria, faz-se oportuno citar um exemplo prático que ilustre o funcionamento completo desse modelo de oráculo de *hardware* em *escrow* com seguro: suponha-se que Andréa, proprietária de uma confeitaria, encomende cinquenta dúzias de ovos a Sandro, seu fornecedor habituado a despachar cargas via VeChain. No momento de formalizar a compra, ambos concordam em criar um contrato inteligente de *escrow,* cujo depósito de 3997

---

[49] VECHAIN. **Development plan and whitepaper vechain .**Disponível em:. https://www.vechain.org. Acesso em 7 jun. 2025, p. 70-71. Este processo é uma realidade e está atestado no *whitepaper* da empresa VeChain,
[50] "NB-IoT" significa *Narrowband Internet of Things,* ou Internet das Coisas em Banda Estreita.
[51] VECHAIN, op. cit., p. 70-71.

VET[52] permanece bloqueado até o cumprimento de três condições, quais sejam: entrega no local combinado (confeitaria de Andréa), no prazo de sete dias e sem qualquer dano físico às caixas de ovos. Simultaneamente, definem que 100 VET desse montante servirá como prêmio de um contrato de seguro *on-chain*, cuja função é garantir que eventuais falhas dos Correios não penalizem Sandro. Na linha de montagem, antes de fechar a embalagem, Sandro fixa em cada caixa de ovos um módulo de IoT – um dispositivo compacto, resistente à umidade, que reúne um receptor GPS, um chip NB-IoT e sensores de impacto –, certificado pela VeChain.

Conforme acordado, se qualquer pacote indicar localização distinta à da confeitaria ou se o prazo de sete dias expirar sem confirmação de chegada, o *escrow contract* entra no ramo de falha de entrega. Nesse instante, sua lógica interna provoca automaticamente o reembolso de 3997 VET a Andréa. Em seguida, o próprio *escrow* transfere os 3 897 VET que estavam bloqueados a Sandro, reconhecendo que a falha de transporte não decorreu de ação dele.

O passo a passo desse fluxo consolida-se assim: (1) depósito inicial em *escrow* com reserva do prêmio de seguro; (2) instalação do módulo IoT nas caixas de ovos; (3) verificação de prazo e localização pelo *escrow contract*; (4a) liberação de fundos ao vendedor ou (4b) acionamento do seguro e estorno ao comprador — tudo sem intervenção de árbitros externos e com garantia de que Andréa não sofrerá prejuízo nem Sandro arcará com falhas alheias.

Pelo visto, considera-se que a adoção de oráculos de *hardware* em contratos de *escrow*, aliada a um mecanismo de seguro *on-chain*, mostra-se capaz de evitar possíveis situações de descumprimento. Isso porque, ao combinar sensores físicos (GPS, NB-IoT e detectores de impacto) com o mecanismo de acionamento automático do seguro, o modelo previne que tanto o comprador como o vendedor se prejudiquem por falhas da transportadora.

3.6 Uso de oráculos descentralizados

Outra solução para o descumprimento do contrato de contratos inteligentes se vale de oráculos descentralizados. Como mencionado, esse tipo visa a garantir maior confiabilidade das informações a serem utilizadas no *smart contract* com base em um sistema de consenso, o que acaba por torná-los não somente indicáveis, para assegurar uma adequada operabilidade do contrato, mas ideologicamente alinhados aos objetivos dos primeiros desenvolvedores do sistema *blockchain;* essa tecnologia visa idealmente garantir a segurança de dados armazenados em um sistema de consenso descentralizado.[53]

---

[52] "VET", ou VeChain Token, é a criptomoeda usada na *blockchain* da empresa VeChain.
[53] DE FILIPPI; WRIGHT, op. cit., p. 20.

Antes, porém, de aplicar esse tipo de oráculo a situações-problema, convém abordar mais detidamente seu funcionamento, para posteriormente se compreender sua aplicação. Para tal, como procedido na abordagem acerca de oráculos de *hardware*, há que se basear em uma tecnologia que já esteja em operação por alguma empresa da área. Aqui, tomar-se-á como base os oráculos descentralizados, desenvolvidos pela Chainlink, grande empresa do setor.[54]

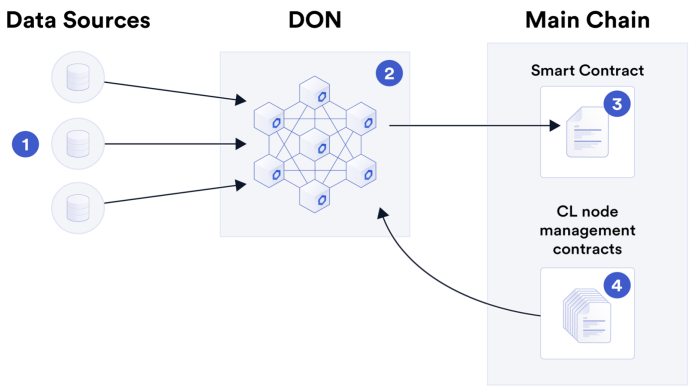
De acordo com o processo viabilizado pela empresa, a informação demandada por um contrato inteligente, tal como ocorre em outros tipos de oráculos, é obtida em ambiente externo à *blockchain.* Ocorre que, nesse modelo, não somente um nó participa do processo de busca da informação necessária, mas sim, todos os nós que compõem o sistema acessam informações por meio de seus oráculos. A informação é "deliberada" por todos antes de ser utilizada no contrato inteligente.[55]

Com isso, o sistema garante significativa segurança quanto à validade do dado com base em um duplo mecanismo de segurança: a busca de um mesmo dado por todos os nós da rede e o sistema de conferência e de seleção do dado a ser utilizado. Sabe-se que, em outros sistemas e modelos, a informação muitas vezes é obtida por um único oráculo, o que aumenta muito a chance de se utilizar uma informação inadequada em um contrato inteligente, o que prejudica as partes. No modelo ora tratado, porém, a informação a ser utilizada é produto de um trabalho realizado por muitas "frentes" e de uma "deliberação" acerca das informações obtidas por todas elas.

Para auxiliar a compreensão das ideias trazidas, considera-se pertinente colacionar esquema contido no *whitepaper* da Chainlink (figura 3). Esse esquema deixa graficamente evidente o curso do processo tratado desde a obtenção de informações pelos oráculos dos nós (1), passando pelo processamento dos vários dados obtidos (2) até que o dado selecionado seja inserido no contrato inteligente (3).[56]

[54] CHAILINK. Informações site oficial da empresa. https://chain.link/. Acesso em: 09 jun. 2025.
[55] BREIDENBACH et al., op. Cit., p. 68-69.
[56] CHALINK. **Whitepaper da Chainlink.** Disponível em: https://chain.link/whitepaper. Acesso em: 9 jun 2025.

Figura 3 – Funcionamento de uma rede de oráculos descentralizados



Fonte: BREIDENBACH et. al., op. cit., p. 66.

Uma vez abordada a essência de oráculos descentralizados nos moldes proporcionados pela Chainlink, cumpre agora averiguar como esta ferramenta é aplicável a contratos *escrow* de compra e venda de modo a garantir ao comprador que o produto será entregue e sem defeitos.

Nesse ponto, é simples aplicar a tecnologia Chainlink para garantir ao comprador que o produto seja entregue no local predeterminado. Para tal, basta constar no contrato que o valor disponibilizado pelo comprador somente será titularizado pelo vendedor a partir do momento em que for comunicado ao contrato, pelos oráculos, que o produto foi entregue no local acertado. A busca realizada pelos oráculos dos vários nós em sistemas de *Application Programming Interface* (API), Interface de Programação de Aplicações, antecede a comunicação ao contrato. Uma vez coletadas as informações e realizado o processamento dos dados, comunica-se ao contrato que o produto foi efetivamente entregue. Com essa informação, o contrato automaticamente transfere o valor disponibilizado pelo comprador ao vendedor.

Essa solução, porém, não é suficiente ao problema proposto, porque ela considera somente a garantia da entrega; não é eficaz para garantir ao comprador a entrega do produto em bom estado. Para que a tecnologia seja empregada de modo a conferir uma transação comercial completamente satisfatória, é preciso se conceber um modelo de contrato com mais cláusulas condicionantes à transferência do valor ao vendedor.

Dessa maneira, pensa-se que a melhor alternativa é elaborar um contrato com as seguintes previsões: verificação de entrega do produto no local fixado com base nas APIs de páginas da empresa transportadora; abertura de prazo para “inspeção” por parte do comprador;

possibilidade de o comprador abrir uma disputa, caso entenda que o produto foi entregue com defeitos, ou confirmar que a mercadoria satisfaz suas expectativas; disputa, caso haja, a ser resolvida com o auxílio de oráculo humano; prazo de expiração para o comprador abrir uma disputa ou confirmar a satisfação, findo o qual o valor é automaticamente transferido ao vendedor; contratação de empresa de seguro para reparar eventuais danos causados pela empresa transportadora.

Assim, criada a transferência *escrow* com os requisitos acima estabelecidos, o primeiro passo seria acompanhar possíveis sinais enviados por módulos de IoT instalados no produto ou nas caixas. Na hipótese de registro de evento prejudicial à integridade do produto, como excesso de umidade ou um impacto muito forte, pode ser acionada a seguradora automaticamente.

Não havendo qualquer notificação pelos sensores instalados, o próximo passo é a confirmação de que a mercadoria chegou ao local preestabelecido. Como já dito, é possível indicar ao contrato inteligente que a mercadoria chegou ao endereço estabelecido após conferência, por parte dos oráculos, de APIs dos correios ou da transportadora utilizada. As informações são obtidas e submetidas ao sistema de consenso, transmitindo-se ao contrato um dado com precisão.

Caso o produto não chegue ao local indicado no prazo estipulado, inicia-se um prazo para que qualquer das partes abra uma disputa. Se uma disputa for aberta, aciona-se um sistema de arbitragem disponível na internet, a exemplo o programa chamado Kleros[57]. A disputa acerca da não entrega no local acertado no prazo preestabelecido é resolvida na plataforma escolhida, e estas são as possíveis soluções: devolução do valor ao comprador, caso o vendedor sequer tenha postado a mercadoria na transportadora; pagamento ao vendedor e cobertura do valor ao comprador pela seguradora, caso a não entrega seja falha da transportadora.

Se, por outro lado, o produto for entregue no local correto, abre-se um prazo para "inspeção" por parte do comprador, no qual ele poderá verificar se a mercadoria está em bom estado ou apresenta algum defeito. Na hipótese de apresentar algum defeito, há possibilidade de se acionar novamente a plataforma de resolução de litígios. Nesse caso, deve ser verificado se verificar se o produto já apresentava defeito antes do envio ou se dano se produziu durante

[57] Kleros é um protocolo descentralizado de decisão aplicável a *smart contracts*. *Yellowpaper* do programa Kleros Disponível em: Yellow PaperKleroshttps://kleros.io › yellowpaper. Acesso em: 09 jun 2025. A página do programa está disponível em: https://kleros.io/pt-br/. Acesso em: 09 jun 2025. O programa Kleros é compatível com a Chainlink, como está previsto na página 6 de seu *Yellowpaper*: "Kleros is currently implemented on Ethereum; however, this protocol could be implemented on any blockchain with adequately expressive smart contracts". Em tradução livre: "O Kleros está atualmente implementado no Ethereum, no entanto, esse protocolo poderia ser implementado em qualquer blockchain com contratos inteligentes suficientemente expressivos."

o transporte da mercadoria. Nessa hipótese, o contrato pode se valer de oráculos de *hardware* capazes de relatar se houve alterações, no trajeto, capazes de produzir o defeito percebido.

O programa de arbitragem pode determinar o retorno do valor ao comprador, caso se verifique que o defeito já se apresentava antes mesmo do envio. Mas, se for percebido que a imperfeição se produziu durante o transporte do produto, pode ser determinado o acionamento do seguro, de modo que seja pago o valor ao vendedor e retornado o valor ao comprador.

Na situação de o produto não apresentar defeito, o comprador pode informar, dentro do prazo de "inspeção", que o valor pode ser revertido ao vendedor. De outra forma, se vencido o prazo sem manifestação do comprador, a quantia antes "imobilizada" pela transação é automaticamente transferida ao vendedor.

Imagine-se, agora, um exemplo prático, para que o modelo seja melhor compreendido. Considere-se que José Henrique quer preparar um *Magret de Canard* - prato da culinária francesa - e, para tal, deseja comprar carne de pato de boa procedência. Ao fazer uma pesquisa, identificou um produtor de patos localizado na região administrativa do Park Way, em Brasília, chamado André. Convencido de que os patos criados por André respondiam a suas expectativas, José Henrique entrou em contato com o produtor e propôs a compra e a venda por meio de um *smart contract,* com utilização da plataforma Ethereum e que os oráculos fossem operacionalizados pela empresa Chainlink.

O comprador, então, criou a transação *escrow* e dispôs que a quantia de 0,0065 ETH seria transferida a André se as carnes dos patos fossem devidamente entregues em seu endereço residencial em bom estado para consumo humano e preparo; garantido principalmente pela conservação de temperatura inferior a -12º C durante todo o percurso e no prazo de 10 dias após a criação do contrato.

Estabeleceu-se, outrossim, que seria contratada uma seguradora, a qual deveria ressarcir o comprador por falhas exclusivamente provocadas por erros da transportadora, seja a não entrega no local determinado, seja a entrega da mercadoria em condições impróprias. Uma vez que o problema não adviria do vendedor, definiu-se que o valor do produto lhe seria pago.

Para as hipóteses de constatação de não entrega do produto ou entrega com defeito, previu-se a utilização do sistema de arbitragem *online* Kleros, o qual, analisando dados fornecidos pelas partes e pela transportadora, definiria o culpado pela falha ocorrida. Sendo a culpa do vendedor, previu-se que esse não receberia a quantia relativa à venda.

Criado o contrato, André preparou as carnes, embalou-as e instalou, na caixa utilizada para o transporte, sensores capazes de verificar a temperatura ambiente e de "notificar" o contrato inteligente, caso fosse marcada temperatura superior a -12º C. Além disso, tirou

algumas fotos e gravou vídeos com o fim de produzir prova de que postou o produto em boas condições.

Após a postagem, não houve incidentes que fizessem os módulos de IoT acionarem o contrato e, transcorridos 7 dias do envio, foi notificado o contrato, por meio da rede de oráculos descentralizados da Chainlink, sobre a entrega do produto no destino. Mas José Henrique não recebeu seu pedido, o que o levou a ficar preocupado com a situação e a abrir uma disputa.

Aberta a disputa, a situação foi levada à análise de jurados do sistema Kleros, os quais conferiram as informações obtidas pelos oráculos descentralizados da Chainlink e pediram que as partes enviassem as provas que possuíam. José Henrique enviou provas de que, ao entrar em contato com a transportadora, essa verificou que seu funcionário entregou o produto em endereço diverso, fazendo com o que o sistema erroneamente indicasse o êxito da entrega. Ao apreciarem os dados, os jurados concluíram pelo erro da transportadora, determinando que o contrato automaticamente acionasse o seguro para pagamento, a José Henrique, do valor empregado na compra e que André fosse pago com a quantia disponível no contrato.

Em suma, a adoção de oráculos descentralizados, como os oferecidos pela Chainlink, indica uma solução robusta e coerente com os princípios originais da tecnologia *blockchain*, ao garantir que dados externos sejam verificados por múltiplos nós antes de acionarem cláusulas contratuais. A integração de sensores IoT, sistemas de seguro e plataformas de arbitragem online compõe um arcabouço completo para contratos *escrow* de compra e venda, assegurando tanto a entrega no local combinado, quanto a integridade do produto. O exemplo prático envolvendo José Henrique e André ilustra como, em caso de falhas — seja por erro da transportadora ou defeito pré-existente —, o mecanismo de disputas combinando oráculos descentralizados e Kleros permite uma resolução justa e automática, respeitando os direitos do comprador e do vendedor.

O modelo enfocado não apenas amplia a confiança nas transações comerciais digitais, mas também aponta caminhos para evoluções futuras, como a inclusão de novos tipos de sensores, ajustes dinâmicos de seguros e refinamento dos processos de arbitragem, consolidando os *smart contracts* como instrumentos verdadeiramente autônomos e confiáveis.

4 JUDICIALIZAÇÃO DE *SMART CONTRACTS*

Até este momento, foram abordadas formas de se garantir que um contrato inteligente de compra e venda seja exitoso ou que, ao menos, as partes não saiam prejudicadas por seu mal

funcionamento. No entanto, o que se apresentou até aqui foram aspectos preventivos, isto é, pontos que podem ser seguidos, de forma a evitar que comprador e vendedor percam produtos ou criptoativos. As soluções apresentadas não servem, porém, para dirimir litígios provenientes de um mal funcionamento de contratos inteligentes.

A respeito desses litígios, a tecnologia já não pode reverter, por exemplo, eventual injustiça cometida, tendo em vista que *smart contracts*, como amplamente abordado, são autoexecutáveis. Isto é, uma vez cumprido um comando previsto no contrato, já não é possível revertê-lo, haja vista o código não ser passível de controle algum.[58]

Uma forma de remediar esse "efeito colateral" de um contrato inteligente seria um acordo *off-chain* entre as partes. Ou seja: a título exemplificativo, se um vendedor envia frutas podres a um consumidor, e se o pagamento tiver ocorrido automaticamente, se as partes se conhecerem e agirem ambas de boa-fé, é possível acordarem para que as frutas sejam trocadas no âmbito exterior à *blockchain*.

Outro meio de resolver o litígio externamente ao contrato inteligente é o uso de arbitragem, caso haja tal previsão em contrato convencional celebrado, cujo objeto seja o mesmo do contrato inteligente. Isto é, há possibilidade de as partes pactuarem o negócio por meio de um contrato convencional e se utilizarem do *smart contract* apenas para operacionalizá-lo. Nesse perspectiva, caso haja uma cláusula, no contrato celebrado fora da *blockchain*, que permita arbitragem em eventual litígio, é possível que danos causados em decorrência do mecanismo de funcionamento do contrato inteligente sejam reparados por meio de arbitragem.[59]

Fica claro, portanto, a possibilidade de conciliação entre os dois indivíduos da relação contratual ou que o litígio se resolva por meio de um árbitro, de forma que o problema se mostra realmente pertinente se há má-fé por parte de alguma das partes. A má-fé levaria o comprador, ao tentar fazer contato com o vendedor para negociar a troca do produto, por exemplo, a ser ignorado por esse; mesmo sabendo das circunstâncias da avença, ele prefere se manter com quantia ainda que injustamente.

Nesses casos, a via mais adequada é, sem dúvida, a judicialização da contenda, visto que, agindo uma das partes com má-fé, somente a força do Estado será capaz de balancear uma relação contratual que gerou injustiça.

---

[58] SWAN, Melanie. **Blockchain: blueprint for a new economy**. Sebastopol, Califórnia: O'Reilly Media, 2015, p. 16.

[59] TALAMINI, Eduardo; CARDOSO, André Guskow. *Smart contracts*, "autotutela" e tutela jurisdicional. **Revista do Ministério Público do Estado do Rio de Janeiro** nº 89, 2023. Disponível em: https://www.mprj.mp.br/. Acesso em 13 jun 2025, p. 86.

Essa solução, no entanto, provoca dois questionamentos, tendo em vista o contexto *sui generis* em que se dá a relação contratual aqui abordada: o primeiro diz respeito à possibilidade de o Poder Judiciário julgar demandas ajuizadas que visem a reparar lesões a direitos, ocorridas em *smart contracts*, tendo em vista a não regulamentação da tecnologia no Brasil. O questionamento pode ser suscitado pela parte beneficiada pela autoexecução do *smart contract* e se fundamenta em uma visão estrita do princípio da legalidade, ou seja, que não poderia haver responsabilização por dano ocorrido mediante uso de tecnologia não regulamentada pelo Direito brasileiro, visto que a lacuna legislativa sobre a matéria inibiria a atuação do Poder Judiciário.

Uma vez identificado que o vácuo legislativo não obsta a responsabilização legal em demandas concernentes a *smart contracts*, o segundo questionamento se volta à forma como o Poder Judiciário pode dirimir tais lides. Considerada a amplitude de temas que caberiam para chegar a tal propósito, o presente trabalho se cingirá ao seguinte: discutir a contraposição entre dois princípios que podem ser alegados por partes contrárias no âmbito judicial, qual sejam, o da obrigatoriedade contratual – designado comumente pelo axioma *pacta sunt servanda* - e a teoria da onerosidade excessiva ou da imprevisão, designada pela expressão *rebus sic stantibus*.

4.1. Princípio da inafastabilidade da jurisdição

No que concerne ao primeiro questionamento, há que se analisar se o Poder Judiciário tem jurisdição sobre lides causadas em contratos inteligentes, uma vez que tal tecnologia não se encontra ainda regulada pelo ordenamento jurídico.

A questão proposta é solucionada com base no princípio da inafastabilidade da jurisdição, de acordo com o qual qualquer lesão ou ameaça de lesão a direito deve ser acolhida pelo Poder Judiciário para que esse aprecie a demanda e lhe dê um provimento justo e adequado.[60] Sob esse prisma, portanto, uma lesão a direito, cometida em contexto de *smart contract,* não pode deixar de ser apreciada pelo Poder Judiciário apenas pelo fato de a nova tecnologia não estar regulamentada no país, visto que o princípio da inafastabilidade da jurisdição impõe ao Poder Judiciário o dever de acolher petição a ele apresentada com o fim de reparar danos a direito.

[60] FUX, Luiz. **Curso de Direito Processual Civil.** 6 ed Rio de Janeiro: Forense, 2023. E-book, item 5.1, página variável. Endereço: https://integrada.minhabiblioteca.com.br/reader/books/9786559648474/ Acesso em: 14 jun. 2025.

Esse princípio tem fundamento constitucional e infraconstitucional, sendo previsto no art. 5º, inciso XXXV, da Constituição Federal de 1988, e no art. 3º, do Código de Processo Civil de 2015.

Na Constituição Federal, o art. 5º, XXXV expressa que a "lei não excluirá da apreciação do Poder Judiciário lesão ou ameaça a direito".[61] Esse dispositivo constitucional, como se nota, determina que não pode haver lei infraconstitucional que exclua da apreciação do Judiciário lesão ou ameaça de direito. Nesse sentido, o texto constitucional, em uma interpretação literal, determina que quaisquer lesões a direitos podem ser levadas ao Poder Judiciário, não se divisando qualquer limitação a tal direito.

Em interpretação ao supramencionado artigo, Alexandre de Moraes salienta que tal princípio torna obrigatória a prestação judicial, uma vez que a "toda violação de um direito responde uma ação correlativa, **independentemente de lei especial que a outorgue**".[62] Luiz Guilherme Marinoni e Daniel Mitidiero, por sua vez, afirmam que a tutela jurisdicional à luz da Constituição Federal é a mais ampla possível, abarcando, inclusive, questões políticas. Eles ressaltam que a única matéria que pode ser subtraída à apreciação pelo Poder Judiciário consiste na revisão do mérito de punições disciplinares, conforme está previsto no art. 142, § 2º, da Constituição Federal.[63]

Compreende-se, portanto, que a Constituição Federal garante um direito amplo de acesso à Justiça, desde que haja lesão ou ameaça de lesão a direito, excetuando-se dessa regra somente a revisão do mérito de punições disciplinares militares.

No Código de Processo Civil, o art. 3º, *caput* prevê: "não se excluirá da apreciação jurisdicional ameaça ou lesão a direito".[64] Trata-se, pois, de uma reprodução fidedigna do art. 5º, XXXV, da Constituição, reforçando-se, em âmbito infraconstitucional, o dever que possui o Estado de julgar lides a ele trazidas, sem haver qualquer limitação a tal dever. Ao comentar essa norma, Leonardo Carneiro da Cunha e outros asseveram que o princípio da inafastabilidade – veiculado mediante o presente artigo – impõe ao juízo encontrar técnica processual idônea à proteção de direito, caso se esteja diante de uma omissão legislativa.[65]

---

[61] CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL de 1988.
[62] MORAES, Alexandre de. **Constituição do Brasil interpretada e legislação constitucional**. São Paulo: Atlas, 2002, p. 292, realce atual.
[63] MITIDIERO, Daniel F.; MARINONI, Luiz Guilherme B.; SARLET, Ingo W. **Curso de direito constitucional**. 12. ed. Rio de Janeiro: Saraiva Jur, 2023. Item 5.3.1
[64] CÓDIGO DE PROCESSO CIVIL de 2002.
[65] CUNHA, Leonardo Carneiro da; STRECK, Lenio Luiz *et al*. **Comentários ao código de processo civil**. 2. ed. Rio de Janeiro: Saraiva Jur, 2017. E-book. Parte Geral, item 3.2. página variável.

Esses dispositivos permitem depreender, portanto, que o princípio da inafastabilidade prevê uma norma clara, qual seja, o dever do Poder Judiciário de julgar demanda que se lhe apresente, definindo-se para tal, como único requisito, que tal demanda vise a proteger direito lesado ou sob ameaça de lesão. Tal comando é previsto de forma bastante ampla e genérica, havendo ressalva somente em relação a punições disciplinares militares. Sob esse prisma, portanto, uma lesão a direito ocorrido em meio tecnológico, não compreendido pela legislação brasileira, pode ser submetida à jurisdição do Poder Judiciário. O princípio da inafastabilidade não prevê exceção a sua eficácia em função da inexistência de regulamentação da matéria tratada.

Um exemplo jurisprudencial que comprova a tese ora veiculada consiste no Conflito de Competência n.º 161.123/ SP pelo Superior Tribunal de Justiça (STJ). Trata-se de demanda levada a esse órgão, em que se discutiu se a competência para julgar condutas ilícitas no contexto de negociação de criptomoedas seria da Justiça Estadual ou da Justiça Federal. Antes de prosseguir com o relato do precedente, é oportuno colacionar a ementa do precedente:

> EMENTA: STJ. Conflito de Competência n.º 161.123/SP. Rel. Min. Sebastião Reis Júnior. Julgado em 28/11/2025. INQUÉRITO POLICIAL. JUSTIÇA ESTADUAL E JUSTIÇA FEDERAL. INVESTIGADO QUE ATUAVA COMO *TRADER* DE CRIPTOMOEDA (*BITCOIN*), OFERECENDO RENTABILIDADE FIXA AOS INVESTIDORES. INVESTIGAÇÃO INICIADA PARA APURAR OS CRIMES TIPIFICADOS NOS ARTS. 7º, II, DA LEI N. 7.492/1986, 1º DA LEI N. 9.613/1998 E 27-E DA LEI N. 6.385/1976. MINISTÉRIO PÚBLICO ESTADUAL QUE CONCLUIU PELA EXISTÊNCIA DE INDÍCIOS DE OUTROS CRIMES FEDERAIS (EVASÃO DE DIVISAS, SONEGAÇÃO FISCAL E MOVIMENTAÇÃO DE RECURSO OU VALOR PARALELAMENTE À CONTABILIDADE EXIGIDA PELA LEGISLAÇÃO). INEXISTÊNCIA. **OPERAÇÃO QUE NÃO ESTÁ REGULADA PELO ORDENAMENTO JURÍDICO PÁTRIO**. *BITCOIN* QUE NÃO TEM NATUREZA DE MOEDA NEM VALOR MOBILIÁRIO. INFORMAÇÃO DO BANCO CENTRAL DO BRASIL (BCB) E DA COMISSÃO DE VALORES MOBILIÁRIOS (CVM). INVESTIGAÇÃO QUE DEVE PROSSEGUIR, POR ORA, NA JUSTIÇA ESTADUAL, PARA APURAÇÃO DE OUTROS CRIMES, INCLUSIVE DE ESTELIONATO E CONTRA A ECONOMIA POPULAR. 1. **A operação envolvendo compra ou venda de criptomoedas não encontra regulação no ordenamento jurídico pátrio, pois as *moedas virtuais* não são tidas pelo Banco Central do Brasil (BCB) como moeda, nem são consideradas como valor mobiliário pela Comissão de Valores Mobiliários (CVM)**, não caracterizando sua negociação, por si só, os crimes tipificados nos arts. 7º, II, e 11, ambos da Lei n.7.492/1986, nem mesmo o delito previsto no art. 27-E da Lei n. 6.385/1976. 2. Não há falar em competência federal decorrente da prática de crime de sonegação de tributo federal se, nos autos, não consta evidência de constituição definitiva do crédito tributário. 3. Em relação ao crime de evasão, é possível, em tese, que a negociação de criptomoeda seja utilizada como meio para a prática desse ilícito, desde que o agente adquira a moeda virtual como forma de efetivar operação de câmbio (conversão de real

> em moeda estrangeira), não autorizada, com o fim de promover a evasão de divisas do país. No caso, os elementos dos autos, por ora, não indicam tal circunstância, sendo inviável concluir pela prática desse crime apenas com base em uma suposta inclusão de pessoa jurídica estrangeira no quadro societário da empresa investigada. 4. Quanto ao crime de lavagem de dinheiro (art. 1º da Lei n. 9.613/1998), a competência federal dependeria da prática de crime federal antecedente ou mesmo da conclusão de que a referida conduta teria atentado contra o sistema financeiro e a ordem econômico-financeira, ou em detrimento de bens, serviços ou interesses da União, ou de suas entidades autárquicas ou empresas públicas (art. 2º, III, *a* e *b*, da Lei n. 9.613/1998), circunstâncias não verificadas no caso. 5. Inexistindo indícios, por ora, da prática de crime de competência federal, **o procedimento inquisitivo deve prosseguir na Justiça estadual, a fim de que se investigue a prática de outros ilícitos, inclusive estelionato e crime contra a economia popular.** 6. **Conflito conhecido para declarar a competência do Juízo de Direito da 1ª Vara de Embu das Artes/SP, o suscitado**.[66] (g.n.)

O inquérito policial apurava a conduta de um investigado que, por meio de sua empresa, captava recursos de terceiros para especulação no mercado de Bitcoin, oferecendo uma rentabilidade fixa e expressiva. O Ministério Público Estadual, vislumbrando indícios de crimes federais — como evasão de divisas, sonegação fiscal e operação de instituição financeira sem autorização —, promoveu a remessa dos autos à Justiça Federal que, por sua vez, suscitou o conflito negativo de competência.

O STJ, para dirimir a controvérsia, fez uma análise profunda que demonstra a aplicação prática do princípio da inafastabilidade. A Corte iniciou sua fundamentação no ponto central da questão, reiterando que as operações com criptoativos carecem de regulamentação no ordenamento jurídico pátrio. Para tal, invocou, no acórdão, declarações oficiais do Banco Central do Brasil (BCB) e da Comissão de Valores Mobiliários (CVM), atestando que moeda virtual não é considerada moeda, nem valor mobiliário. Essa informação foi decisiva para afastar, de maneira fundamentada, a competência federal, uma vez que os crimes contra o Sistema Financeiro Nacional e contra o mercado de capitais pressupõem a negociação de ativos regulados.

Contudo – e aqui reside a essência da aplicação do princípio – , o Tribunal não se limitou a declarar a ausência de crime federal para extinguir a análise. Ao contrário, prosseguiu na verificação dos fatos sob a ótica de outras possíveis infrações penais. Não ignorou as circunstâncias fáticas que indicavam uma potencial lesão a direitos de particulares, como a promessa de lucros fixos e elevados em um mercado de alta volatilidade, a apreensão de vultosa quantia em espécie e a existência de bens em nome de terceiros.

---

[66] SUPERIOR TRIBUNAL DE JUSTIÇA. **Conflito de Competência nº 161.123.** DJe de 05/12/2018.

Ao reconhecer que tais elementos poderiam configurar outros delitos, a Corte explicitamente direcionou a continuidade da investigação à esfera competente, concluindo que as circunstâncias indicavam a necessidade de o procedimento prosseguir na Polícia Civil de São Paulo, para a devida apuração de outros crimes, inclusive de estelionato, e infrações contra a economia popular.

Portanto, a decisão do STJ, ao mesmo tempo em que reconheceu o vácuo regulatório, recusou-se a permitir um vácuo de jurisdição. O precedente consolida a tese de que, mesmo diante de matérias tecnologicamente novas e não regulamentadas, o Poder Judiciário tem o dever de examinar a alegação de lesão a direito. Isso, com base no arcabouço normativo geral existente, encontrando a via adequada para a persecução e o julgamento, de modo a materializar o comando constitucional da inafastabilidade da jurisdição.

Diante do exposto, torna-se claro que a ausência de legislação específica para uma nova tecnologia não representa óbice à atuação do Poder Judiciário. A análise aprofundada do princípio da inafastabilidade, sustentado tanto pela Constituição Federal quanto pela legislação processual, revela um mandamento claro: toda e qualquer alegação de lesão ou ameaça a direito deve encontrar, no Judiciário, uma via de apreciação.

O precedente do STJ no referido Conflito de Competência materializa essa doutrina, demonstrando que, mesmo em face de um vácuo regulatório sobre criptoativos, a Corte não se absteve de seu dever. Pelo contrário, analisou a situação fática e, com base nas normas gerais do ordenamento jurídico, indicou o caminho para que a persecução da justiça continuasse.

A lógica empregada pelo STJ é diretamente aplicável a lides cíveis decorrentes de *smart contracts* e de outras inovações em *blockchain*. A eventual lesão a um direito patrimonial ou moral, advinda de um contrato autoexecutável, enquadra-se perfeitamente na hipótese de "lesão a direito" que compele a intervenção judicial.

Assim, conclui-se que o arcabouço jurídico nacional, ao consagrar a inafastabilidade da jurisdição, garante que o avanço tecnológico não crie zonas de anomia ou impunidade. Cabe ao Poder Judiciário o papel fundamental de proteger os jurisdicionados e de assegurar que a justiça seja acessível e efetiva em qualquer contexto, por mais novo que ele seja.

4.2 A controvérsia judicial: força obrigatória e função social nos contratos inteligentes

Uma vez exposto que o princípio da inafastabilidade da jurisdição compele o Poder Judiciário a julgar o mérito de litígios oriundos de *smart contracts*, cabe analisar como a jurisdição pode solucionar problemas relativos a essa tecnologia que lhe sejam apresentados. Para tal, a presente análise se limitará a discutir questão jurídica que recorrentemente pode ser

suscitada em lides envolvendo contratos inteligentes de compra e venda, ou seja, um embate entre a rigidez do pacto firmado e a necessidade de uma justiça corretiva. De um lado, a parte beneficiada pela execução automatizada defenderá a aplicação estrita da força obrigatória dos contratos, comumente referenciada pelo brocardo latino *pacta sunt servanda;* de outro, a parte prejudicada invocará a aplicação da tese da onerosidade excessiva, para pleitear a revisão ou anulação do contrato.

O princípio da força obrigatória dos contratos é o pilar tradicional do direito contratual, o qual consagra a ideia de que o contrato, uma vez celebrado de forma válida, faz lei entre as partes. Embora não esteja expressamente previsto no ordenamento jurídico, seu fundamento deriva da autonomia da vontade e da necessidade de segurança jurídica, estando implícito em normas como o art. 389 do Código Civil e no art. 2º da Lei 13.874/2019.[67]

Na lição de Flávio Tartuce, tal princípio "importa em autêntica restrição da liberdade, que se tornou limitada para aqueles que contrataram a partir do momento em que vieram a formar o contrato consensualmente e dotados de vontade autônoma".[68] Essa máxima confere previsibilidade e estabilidade às relações negociais, sendo o alicerce jurídico que muito estreitamente se relaciona com os princípios regentes de *smart contracts*. Isto é, contratos inteligentes foram concebidos para ser irreversíveis, imutáveis e invioláveis, valendo completamente o que foi estipulado pelas partes no momento em que o contrato passar a valer.

Em contraposição direta a essa rigidez, encontra-se a teoria da onerosidade excessiva, segundo a qual a validade de um contrato pressupõe a inalterabilidade da situação de fato. Significa que, havendo uma situação extraordinária que torne excessivamente custoso o cumprimento do contrato, é possível que as cláusulas sejam revistas.[69] A teoria está positivada nos arts. 317, 478 e 479 do Código Civil, que assim estabelecem:

> Art. 317. Quando, por motivos imprevisíveis, sobrevier desproporção manifesta entre o valor da prestação devida e o do momento de sua execução, poderá o juiz corrigi-lo, a pedido da parte, de modo que assegure, quanto possível, o valor real da prestação.
>
> Art. 478. Nos contratos de execução continuada ou diferida, se a prestação de uma das partes se tornar excessivamente onerosa, com extrema vantagem para a outra, em virtude de acontecimentos extraordinários e imprevisíveis, poderá o devedor pedir a resolução do contrato. Os efeitos da sentença que a decretar retroagirão à data da citação.
>
> Art. 479. A resolução poderá ser evitada, oferecendo-se o réu a modificar equitativamente as condições do contrato.

---

[67] TARTUCE, Flávio. **Manual de Direito Civil.** 15. ed. Rio de Janeiro: Método, 2025. E-book. Item 5.3, páginas variáveis.
[68] Ibid.
[69] GONÇALVES, op. cit., item 6.6

O embate entre aquela rigidez e essa teoria se configura quando a parte que defende a execução literal do código argumentar que as regras programadas eram claras e válidas para ambos, constituindo lei irrevogável para aquela transação específica. Em contrapartida, a parte lesada sustentará que, por alguma razão, não tinha consciência plena de como o código agiria ou que sua execução automática violou a expectativa legítima depositada no negócio, gerando um resultado imprevisível.

Em relação à última alegação, diversas hipóteses podem levar a uma execução contrária à vontade ou à justa expectativa da parte que se sentiu prejudicada. Por exemplo: o código pode conter uma falha sutil ou uma ambiguidade que é explorada maliciosamente pela outra parte. Outra situação comum envolve a dependência de dados externos fornecidos por um oráculo que se revelam incorretos ou manipulados, levando o contrato a uma execução baseada em premissas fáticas falsas. Pode-se cogitar, ainda, a hipótese de um código intencionalmente complexo ou ofuscado, que impede a compreensão de um leigo sobre suas reais consequências, violando o dever de informação decorrente da boa-fé. Por fim, a ocorrência de um evento externo imprevisível pode tornar a obrigação programada excessivamente onerosa para uma das partes, atraindo a teoria da imprevisão.[70] Em todos esses cenários, a tarefa do Poder Judiciário é sopesar os princípios em conflito para entregar uma decisão justa.

Contudo, antes de o Poder Judiciário adentrar o mérito do sopesamento entre a força obrigatória e a onerosidade excessiva, há que se identificar se os contratos inteligentes podem ser considerados contratos à luz do Direito. Isto é, a aplicação de todo este arcabouço principiológico do direito contratual é logicamente dependente do reconhecimento de que o código computacional em litígio se enquadra como um negócio jurídico segundo o ordenamento. Desse modo, a etapa seguinte e indispensável desta análise consiste em examinar os requisitos de existência, validade e eficácia dos *smart contracts*.

4.2.1 A análise da existência, validade e eficácia do smart contract

A metodologia de análise de um negócio jurídico no direito brasileiro ocorre, de acordo com a doutrina ponteana, em três planos: existência, validade e eficácia.[71] Esses três planos, que compõem a denominada "escada ponteana"[72], constituem uma forma de se verificar se *smart contracts* podem ser considerados contratos à luz do Direito brasileiro e,

[70] BASHIR, op. cit., 2018, p. 263.
[71] TARTUCE, op. cit., item 2.6.4, página variável.
[72] TARTUCE, op. cit., item 2.5.3.1, página variável.

consequentemente, se a eles são aplicáveis os princípios contratuais do *rebus sic stantibus* e do *pacta sunt servanda*.

O plano da existência é o degrau inicial, que trata dos elementos mínimos e essenciais para que um contrato seja considerado existente no mundo jurídico. A respeito desse plano, é necessário ressaltar que não há qualquer disposição explícita no Código Civil concernente à existência de um contrato, tendo dedicado o legislador a tratar diretamente da validade.[73] Não obstante referida lacuna legislativa, o atributo contratual ora tratado encontra fundamento em significativa parcela da doutrina civilista brasileira, representada, entre outros, por Flávio Tartuce, Caio Mário da Silva Pereira e Pablo Stolze Gagliano.[74] Neste diapasão, julga-se oportuno lançar mão desse plano, haja vista sua abordagem por doutrinadores de reconhecida importância.

A existência de um contrato é aferida, consonante às doutrinas de Flávio Tartuce[75], Pablo Stolze e Rodolfo Pamplona[76], se presentes os seguintes elementos: sujeitos, objeto e forma. Aplicando essa estrutura aos *smart contracts*, verifica-se que todos os elementos estão presentes. O sujeito de direitos não é a máquina ou o protocolo, mas as partes - pessoas físicas ou jurídicas - que interagem com o sistema para se vincular. O objeto é a própria obrigação que o código executa – a transferência de um ativo, o registro de um dado, a liberação de um pagamento condicionado –e a forma é o meio pelo qual a vontade das partes se manifesta e as cláusulas são estruturadas, qual seja, a linguagem de programação e os protocolos informacionais que permitem a transação.[77]

Uma vez identificado que contratos inteligentes existem à luz do Direito brasileiro, adentra-se o plano da validade, que permite verificar se ele é válido, nulo ou anulável. Esse plano analisa se os elementos de existência possuem as qualidades exigidas pela lei - conforme o art. 104 do Código Civil -, quais sejam: agente capaz; objeto lícito, possível, determinado ou determinável e forma prescrita ou não defesa em lei.

A capacidade do agente é um ponto especialmente relevante nos contratos inteligentes, dado que mais acessíveis a incapazes, sejam absolutamente ou parcialmente, do que contratos convencionais.[78] Quanto a este requisito, o *smart contract* pode ser nulo se firmado por

---

[73] Ibid.
[74] Ibid.
[75] Ibid.
[76] GAGLIANO, Pablo Stolze; FILHO, Rodolfo Mário Veiga Pamplona. **Novo Curso de Direito Civil – vol. 4 - contratos**. 8. ed. Rio de Janeiro: Saraiva Jur, 2025. E-book. Capítulo I, Item 7.1, páginas variáveis.
[77] GOERCK, Daniella L. **Contratos eletrônicos, smart contracts e responsabilidade civil.** São Paulo: Almedina, 2023. Coleção Pinheiro Neto Advogados**.** E-book. Item 4.3, página variável.
[78] Ibid.

indivíduo absolutamente incapaz, isto é, menor de dezesseis anos. Por outro lado, se for estabelecida a avença com relativamente incapaz – pessoa entre dezesseis e dezoito anos -, faz-se possível conceber sua anulabilidade. Não havendo, no entanto, tais óbices relativos à capacidade, passa-se a verificar os demais requisitos de validade.

O segundo requisito de validade é que o objeto seja lícito, possível, determinado ou determinável. A ilicitude do objeto não se restringe à violação direta da lei, mas abrange tudo o que atenta contra a ordem pública, a moral e os bons costumes.[79] A natureza descentralizada e, por vezes, anônima dos *smart contracts* representa um risco à validade nesse ponto, pois eles podem ser utilizados para estruturar negócios com objetos manifestamente ilícitos, como esquemas de pirâmide financeira, lavagem de dinheiro ou a comercialização de produtos e serviços ilegais.[80] Um *smart contract* com objeto ilícito é nulo de pleno direito, independentemente da sofisticação de sua tecnologia.

Os demais atributos do objeto do contrato, por outro lado, aplicam-se a contratos inteligentes da mesma forma como a contratos convencionais. Assim, sob a égide deste aspecto específico, o contrato poderá ser considerado válido se seu objeto for possível, determinado ou determinável.

O terceiro requisito, a forma prescrita ou não defesa em lei, é central para a aceitação dos *smart contracts*. O ordenamento jurídico brasileiro adota, como regra geral, o princípio da liberdade das formas - art. 107 do Código Civil -, segundo o qual, não havendo exigência de solenidade, qualquer meio que expresse a vontade é válido.[81] A forma do *smart contract* em si, portanto, não é um obstáculo à sua validade. Contudo, é precisamente dentro dessa forma tecnologicamente complexa que podem surgir vícios de consentimento. A validade da manifestação de vontade pode ser maculada pela assimetria de informações, por exemplo: uma parte com conhecimento técnico superior pode, de má-fé, inserir no código uma função oculta que a beneficie indevidamente, configurando dolo. Também uma parte leiga pode concordar com a execução do código por erro ou ignorância sobre suas reais consequências. Tais vícios de consentimento são causas de anulabilidade do negócio - art. 171, II, CC - e justificam a intervenção judicial.

Por fim, há o plano da eficácia, que analisa a possibilidade de o negócio, existente e válido, produzir os efeitos desejados. Note-se que um negócio pode se tornar ineficaz de forma superveniente. É o que ocorre quando, ao longo de sua execução, ele se torna excessivamente

[79] GONÇALVES, op. cit., item *5.2,* página variável.
[80] GOERCK, op. cit.,item 4.3.2, página variável.
[81] GONÇALVES, op. cit., item 5.2*,* página variável.

oneroso para uma das partes, justificando sua resolução.[82] No caso dos *smart contracts*, os fatores de eficácia são os mesmos de outros negócios, mas sua implementação é feita por meio de código e de protocolos autoexecutáveis. É possível programar fatores de atribuição de eficácia geral, como uma condição suspensiva que só ativa o contrato após um evento específico. Pode-se também inserir fatores de atribuição da eficácia diretamente visada, como uma cláusula que subordina a transferência de um ativo à autorização de um terceiro, com um oráculo ou com o sistema de transferência *escrow*.

O grande desafio dos *smart contracts* reside precisamente neste plano: a eficácia depende da correta tradução da vontade das partes para a linguagem de programação. Se houver erro no código, os efeitos produzidos serão diferentes daqueles manifestados, e a imutabilidade da tecnologia torna a correção extremamente difícil. É crucial notar que, mesmo um magistrado, ao reconhecer um contrato como nulo, não tem capacidade técnica de impedir que o código já implementado na *blockchain* deixe de produzir os efeitos programados, criando um hiato entre a decisão jurídica e a realidade tecnológica.

Diante do exposto, conclui-se que os *smart contracts* podem percorrer com sucesso os três planos analíticos: eles existem, pois contêm os elementos mínimos de um negócio jurídico; são, em tese, válidos, desde que observadas as qualidades do agente, do objeto e da forma; são concebidos para ser eficazes, embora sua automação e imutabilidade apresentem desafios únicos para a correta produção dos efeitos desejados. Esse reconhecimento integral de sua natureza jurídica é o que legitima a aplicação de princípios próprios de direito dos contratos pelo Poder Judiciário.

4.2.2 A solução da lide pela aplicação dos princípios de ordem pública

Uma vez entendido que *smart contracts* são negócios jurídicos existentes e eficazes, sendo que, em tese, podem ser igualmente válidos, a análise judicial avança para o exame de seu conteúdo e dos efeitos de sua execução. Nessa fase, a atividade jurisdicional se depara com o sopesamento entre dois princípios fundamentais: de um lado, a força obrigatória do contrato (*pacta sunt servanda*), que preza pela segurança jurídica e pelo cumprimento do que foi programado; de outro, a onerosidade excessiva, que possibilita a revisão de cláusulas se sobrevierem eventos extraordinários. A decisão sobre a manutenção, revisão ou anulação do resultado de um *smart contract* depende de qual princípio terá maior peso no caso concreto.

[82] GOERCK, op. cit., item 4.3.3, página variável.

O princípio da força obrigatória dos contratos prevalece quando a execução automatizada do *smart contract* corresponder fielmente a um acordo hígido, ou seja, um negócio juridicamente perfeito em todos os seus aspectos. Se o código é claro, o objeto é lícito, as partes são capazes e, crucialmente, não há indícios de vício de consentimento ou de quebra da lealdade, a decisão judicial deve honrar o que foi pactuado. Nesses casos, a intervenção do Judiciário para alterar o resultado criaria insegurança jurídica e desrespeitaria a autonomia da vontade manifestada pelas partes. O Poder Judiciário não atua para proteger as partes de negócios desvantajosos que foram celebrados de forma livre e consciente, mas sim para garantir o cumprimento de acordos válidos.

Em outro ponto, a teoria da onerosidade excessiva é fator determinante para a revisão ou resolução do contrato em cenários que demonstrem a ocorrência de um evento superveniente, extraordinário e imprevisível, que rompa o equilíbrio econômico original do pacto. A intervenção judicial, nesse caso, justifica-se para restaurar a justiça comutativa, impedindo que uma das partes seja levada à ruína, enquanto a outra obtenha um lucro exorbitante por um fator alheio ao controle de ambas. Isso ocorreria, por exemplo, em contratos inteligentes de compra e venda de mercadorias em cenários como: a) fechamento inesperado de rotas marítimas essenciais devido a um conflito geopolítico súbito, que torna o custo do frete da mercadoria proibitivo e não previsto pelas partes na celebração do acordo; b) superveniência de uma pandemia que leva governos a decretarem o fechamento de fronteiras ou a requisitarem a produção da mercadoria contratada, tornando sua entrega legalmente impossível ou excessivamente custosa; c) desastre natural de proporções inéditas, como secas ou geadas históricas, que destrói a safra do produto a ser entregue, forçando o produtor a adquirir a mercadoria no mercado por um preço muito superior ao contratado. Em todas essas hipóteses, a execução literal do código resultaria em injustiça manifesta, justificando a intervenção do Judiciário para aplicar a teoria da onerosidade excessiva.

O que se afirma encontra fundamento na jurisprudência do STJ que, conquanto não possua precedente concernente a *smart contracts*, delimita de forma clara os critérios de sopesamento entre os princípios ora tratados. A título exemplificativo, no REsp n.º 1.321. 614/SP, de relatoria do Min. Paulo de Tarso Sanseverino, julgado em 16/12/2014, o voto vencedor, proferido pelo Min. Ricardo Villas Bôas Cueva, trouxe de forma evidente que o princípio da obrigatoriedade dos contratos é regra no ordenamento jurídico pátrio: “a regra é a

observância, na relação contratual, do princípio *pacta sunt servanda*", mas "desde que preservada a moral, a ordem pública e os bons costumes".[83]

Nesse precedente, levou-se ao STJ pedido de revisão de cláusulas de um contrato de compra de equipamento médico importado, o qual regrava o parcelamento do pagamento efetuado em dólar estadunidense. Alegou o recorrente que a valorização da moeda estrangeira foi imprevisível, provocou seu inadimplemento e justificava a alteração do contrato.

Ao analisar os autos, o Min. Villas Bôas Cueva ponderou a aplicação de dois grupos contrapostos de princípios: de um lado, princípios favoráveis ao autor – teoria da imprevisão e da base objetiva – e do outro, o princípio da obrigatoriedade do contrato. A título elucidativo, a teoria da base objetiva possibilita a revisão de cláusulas, mas prescinde do caráter imprevisível; foi introduzida no ordenamento jurídico no art. 6º, V do Código de Defesa do Consumidor.

O Ministro, então, ponderou os dois grupos de princípios para concluir que, no caso, deveria prevalecer a força obrigatória dos contratos. Para tal, foi considerado que a variação do valor da moeda estrangeira era matéria previsível e que, mesmo após abruptas mudanças no câmbio, as partes firmaram aditivos ao contrato, mantendo o dólar como divisa. Dessa forma, não havia possibilidade de se aplicar a onerosidade excessiva, já que a alta da moeda estadunidense não era evento extraordinário e imprevisível, devendo prevalecer o *pacta sunt servanda*.

> EMENTA- STJ. REsp 1.321.614/SP. Relator Min. Paulo de Tarso Sanseverino. Julgado em 16/12/2014. CURSO ESPECIAL. CIVIL. AÇÃO REVISIONAL DE CONTRATO DE COMPRA E VENDA. DÓLAR AMERICANO. MAXIDESVALORIZAÇÃO DO REAL. AQUISIÇÃO DE EQUIPAMENTO PARA ATIVIDADE PROFISSIONAL. AUSÊNCIA DE RELAÇÃO DE CONSUMO. TEORIAS DA IMPREVISÃO. TEORIA DA ONEROSIDADE EXCESSIVA. TEORIA DA BASE OBJETIVA. INAPLICABILIDADE.1. Ação proposta com a finalidade de, após a maxidesvalorização do real em face do dólar americano, ocorrida a partir de janeiro de 1999, modificar cláusula de contrato de compra e venda, com reserva de domínio, de equipamento médico (ultrassom), utilizado pelo autor no exercício da sua atividade profissional de médico, para que, afastada a indexação prevista, fosse observada a moeda nacional. 2. Consumidor é toda pessoa física ou jurídica que adquire ou utiliza, como destinatário final, produto ou serviço oriundo de um fornecedor. Por sua vez, destinatário final, segundo a teoria subjetiva ou finalista, adotada pela Segunda Seção desta Corte Superior, é aquele que ultima a atividade econômica, ou seja, que retira de circulação do mercado o bem ou o serviço para consumi-lo, suprindo uma necessidade ou satisfação própria, não havendo, portanto, a reutilização ou o reingresso dele no processo produtivo. Logo, a relação de consumo (consumidor final) não pode ser confundida com relação de insumo (consumidor intermediário). Inaplicabilidade das regras protetivas do Código

[83] SUPERIOR TRIBUNAL DE JUSTIÇA. **Recurso Especial Nº 1.321.614/SP.** DJe de 03 mar 2015.

> de Defesa do Consumidor. 3. A intervenção do Poder Judiciário nos contratos, à luz da teoria da imprevisão ou da teoria da onerosidade excessiva, exige a demonstração de mudanças supervenientes das circunstâncias iniciais vigentes à época da realização do negócio, oriundas de evento imprevisível (teoria da imprevisão) e de evento imprevisível e extraordinário (teoria da onerosidade excessiva), que comprometa o valor da prestação, demandando tutela jurisdicional específica. 4. O histórico inflacionário e as sucessivas modificações no padrão monetário experimentados pelo país desde longa data até julho de 1994, quando sobreveio o Plano Real, seguido de período de relativa estabilidade até a maxidesvalorização do real em face do dólar americano, ocorrida a partir de janeiro de 1999, não autorizam concluir pela imprevisibilidade desse fato nos contratos firmados com base na cotação da moeda norte-americana, em se tratando de relação contratual paritária. 5. A teoria da base objetiva, que teria sido introduzida em nosso ordenamento pelo art. 6º, inciso V, do Código de Defesa do Consumidor - CDC, difere da teoria da imprevisão por prescindir da previsibilidade de fato que determine oneração excessiva de um dos contratantes. Tem por pressuposto a premissa de que a celebração de um contrato ocorre mediante consideração de determinadas circunstâncias, as quais, se modificadas no curso da relação contratual, determinam, por sua vez, consequências diversas daquelas inicialmente estabelecidas, com repercussão direta no equilíbrio das obrigações pactuadas. Nesse contexto, a intervenção judicial se daria nos casos em que o contrato fosse atingido por fatos que comprometessem as circunstâncias intrínsecas à formulação do vínculo contratual, ou seja, sua base objetiva. 6. Em que pese sua relevante inovação, tal teoria, ao dispensar, em especial, o requisito de imprevisibilidade, foi acolhida em nosso ordenamento apenas para as relações de consumo, que demandam especial proteção. Não se admite a aplicação da teoria do diálogo das fontes para estender a todo direito das obrigações regra incidente apenas no microssistema do direito do consumidor, mormente com a finalidade de conferir amparo à revisão de contrato livremente pactuado com observância da cotação de moeda estrangeira. 7. Recurso especial não provido.[84]

Ante o exposto, portanto, depreende-se que o Poder Judiciário pode dar uma solução a problemas originados em contratos inteligentes de compra e vendas, com base no sopesamento dos princípios da onerosidade excessiva e da obrigatoriedade dos contratos. Considerando-se que, via de regra, uma das partes irá alegar que a execução do código gerou uma situação imprevisível e injusta e que, da outra parte, será alegado que aquilo que executou o código era lei para ambos os lados – não cabendo interferência do Poder Judiciário -, tal demanda deve ser resolvida de acordo com a análise de qual princípio deve prevalecer na situação específica.

[84] SUPERIOR TRIBUNAL DE JUSTIÇA. **Recurso Especial Nº 1.321.614/SP.** DJe de 03 mar 2015.

CONSIDERAÇÕES FINAIS

Os contratos inteligentes consistem em um meio eficaz, seguro e desenvolvido de se estabelecer e se executar a contratação de um negócio, sendo uma maneira ideal de estabelecer relações comerciais em um mundo cada vez mais globalizado e interligado. O grande trunfo dessa espécie de contratação são os atributos que possui: imutabilidade, autoexecutoriedade, irreversibilidade e a possibilidade de estabelecer relações de maneira descentralizada. Dessa forma, é possível asseverar que essa forma de contratação deve ganhar cada vez mais relevância e deve atingir a um número sempre crescente de usuários.

Esse tipo de contratação, no entanto, não está imune a erros e, se considerado o cenário de contratos que regulam compra e venda de produtos físicos, é perfeitamente possível que cenários indesejáveis ocorram, como o produto não ser entregue no local acordado ou que chegue com defeito. Esse tipo de erro não se dá por equívoco do código, pois esse, em condições normais, executa exatamente o que se prevê. O que pode gerar tais situações é, antes, uma programação equivocada ou a não utilização de mecanismos que aumentam a segurança da operação e minimizam as chances de erros.

Um dos mencionados mecanismos, como se identificou no trabalho, consiste nos denominados oráculos. Oráculos são meios de câmbio de dados entre os ambientes *on-chain* e *off-chain* e possibilitam que informações ausentes no âmbito da *blockchain* sejam utilizadas em um *smart contract,* de modo a dar-lhe um desejado desfecho. Variados são os tipos de oráculos, havendo desde sensores instalados no mundo físico que repassam dados concretos – como temperatura ou localização – até buscadores de dados existentes na internet. Essa variedade, como se expôs, permite inúmeras configurações de contratos inteligentes de modo a possibilitar o desfecho desejado às partes.

Outro mecanismo abordado é o tipo de contrato inteligente que se escolha utilizar, considerando aqui, como fator de diferenciação entre os tipos de contrato, a forma como a transferência é realizada. Neste trabalho, elegeu-se o tipo *escrow*, marcado pela necessidade de um número múltiplo de assinaturas para que a transferência ocorra de uma parte para outra. Nessa opção, considerou-se a segurança que esse tipo de transação oferece às partes, visto que essa configuração, entre outras funcionalidades, permite a inserção de um sistema arbitral que solucione eventual litígio e impede que a transferência se dê somente com o consentimento de uma parte.

Com base nessas ferramentas, propôs-se formas de se utilizar oráculos distintos em um contrato *escrow*, expondo-se de forma prática como alguns dos tipos de oráculos apresentados

anteriormente no texto seriam utilizados. O primeiro cenário abordado foi a utilização de um oráculo humano, cenário esse tratado por grandes autores do ramo, como Primavera De Filippi, Aaron Wright, Arvind Narayanan, entre outros. Nele, as partes elegem um terceiro de confiança de ambos, o qual serve como árbitro caso haja uma situação litigiosa. Havendo um litígio, não é possível a transferência do valor contido na conta *escrow*, já que ambas as partes precisam consentir com a movimentação. É nesse ponto que deve o terceiro intervir, analisando o caso e decidindo em favor de quem assinará o contrato para que o valor seja destinado a uma das partes.

O segundo cenário proposto exemplifica o uso de oráculo de *hardware*, concretamente sensores de localização e de impacto. Propôs-se, ademais, a contratação de uma seguradora, utilidade que garante ainda mais segurança às partes. Aqui, o contrato é programado para reagir aos estímulos vindos dos sensores instalados no produto ou na embalagem que o envolve. Assim, cumprindo-se o contrato adequadamente, ou seja, se o produto for entregue no local correto, sem impactos que poderiam acarretar dano à mercadoria e dentro do prazo, o valor é transferido automaticamente ao vendedor. Havendo, por outro lado, algum descumprimento, o seguro é acionado, sendo reembolsado o comprador e pago o vendedor.

O terceiro cenário, por fim, lança mão de oráculos descentralizados, tipo de oráculo cuja forma de obtenção de dados lhes garante maior confiabilidade. No caso proposto, foram utilizados oráculos não descentralizados igualmente, tais como: oráculo humano e sensores de localização. Além disso, estipulou-se prazo para entrega, prazo para reclamação por parte do comprador e a contratação de seguro. Com tais atributos, por um lado, o contrato garantiu que, havendo perfeito cumprimento, a importância fosse transferida ao vendedor; por outro, havendo algum descumprimento, poderia ser a situação resolvida pelo seguro.

Essas considerações, porém, prestam-se a evitar que descumprimentos ocorram em contratos inteligentes de compra e venda. Por tal motivo, a segunda parte do trabalho se voltou a identificar como o Poder Judiciário pode solucionar lides que envolvam tais contratos. Em concreto, a discussão se cingiu a averiguar como deve ser o sopesamento dos princípios do *pacta sunt servanda* e do *rebus sic stantibus*.

Antes, porém, buscou-se abordar como o Poder Judiciário tem competência para julgar tais conflitos conquanto envolvam tecnologias novas e não regulamentadas pelo Direito brasileiro. Tal competência encontra fundamento no princípio da inafastabilidade, o qual impõe o dever ao Poder Judiciário de dirimir quaisquer conflitos que lhe sejam apresentados, ainda que não haja legislação que regulamente a matéria.

Em seguida, iniciou-se a discussão, já mencionada, do sopesamento dos princípios da força obrigatória dos contratos e da onerosidade excessiva. Primeiramente, buscou-se identificar se contratos inteligentes podem ser entendidos como contratos à luz do direito brasileiro, requisito para que a eles sejam aplicados os princípios considerados.

Uma vez demonstrado que os *smart contracts* podem ser entendidos como contratos de acordo com o ordenamento jurídico, identificou-se que a aplicação dos princípios deve se guiar a partir de uma análise de cada caso. Nesse sentido, sendo o contrato válido e eficaz e não havendo nenhum evento extraordinário e imprevisível, deve prevalecer o princípio do *pacta sunt servanda*. Porém, se o contexto que envolve o contrato provocar evento imprevisível, não pode deixar o Poder Judiciário que a parte lesada fique prejudicada, valendo-se, para tanto, da teoria da onerosidade excessiva.

Por fim, conclui-se que este trabalho alcançou seus objetivos ao expor, em primeiro lugar, meios de se evitar que contratos inteligentes de compra e venda de mercadorias sejam descumpridos e ao definir, em segundo lugar, como o Poder Judiciário pode conceder uma solução a casos nos quais houve descumprimento.

REFERÊNCIAS

AirDAO. Plataforma. Disponível em: https://airdao.io. Acesso em: 6 jun 2025.

ANTONOPOULOS, Andreas M.; WOOD, Dr. Gavin. **Mastering Ethereum**. Sebastopol, California: O'Reilly Media, 2019.

BASHIR, Imran. **Mastering Blockchain:** a deep dive into distributed ledgers, consensus protocols, smart contracts, dapps, cryptocurrencies, ethereum, and more. Birmingham, Reino Unido: Packt Publishing, 2020.

BASHIR, Imran. **Mastering blockchain:** distributed ledger technology, decentralization, and smart contracts explaine**d**. 2ª ed. Birmingham, Reino Unido: Packt Publishing, 2018.

BREINDENBACH, Lorenz; CACHIN, Cristian; CHAN, Benedict; COVENTRY, Alex; ELLIS, Steve et al. **Chainlink 2.0:** Next Steps in the Evolution of Decentralized Oracle Networks. 2021. Disponível em: https://chain.link/. Acesso em 1 jun 2025.

CHAINLINK. Site oficial da empresa. Disponível em: https://chain.link. Acesso em: 7 jun. 2025.

CUNHA, Leonardo Carneiro da; STRECK, Lenio Luiz *et al*. **Comentários ao código de processo civil**. 2. ed. Rio de Janeiro: Saraiva Jur, 2017. *E-book.*

DE FILIPPI, Primavera de; WRIGHT, Aaron. **Blockchain and the law:** the rule of code. Cambridge, Massachusetts: Harvard University Press, 2019.

DRESCHER, Daniel. **Blockchain Basic**s: a Non-Technical Introduction in 25 Steps. Frankfurt am Main/Alemanha: Apress, 2017.

FUX, Luiz. **Curso de Direito Processual Civil.** 6 ed.Rio de Janeiro: Forense, 2023. E-book.

GAGLIANO, Pablo Stolze; FILHO, Rodolfo Mário Veiga Pamplona. **Novo Curso de Direito Civil – vol. 4 - contratos**. 8. ed. Rio de Janeiro: Saraiva Jur, 2025. E-book.

GOERCK, Daniella L. **Contratos eletrônicos, smart contracts e responsabilidade civil.** São Paulo: Almedina, 2023. *E-book.* (Coleção Pinheiro Neto Advogados)**.**

GONÇALVES, Carlos R. **Direito Civil Brasileiro:** contratos e atos unilaterais. 21 ed. Rio de Janeiro: Saraiva Jur, 2024. E-book.

KLEROS. Site oficial da empresa. Disponível em: https://chain.link. Acesso em: 7 jun. 2025.

LANTZ, Lorne; CAWREY, Daniel**. Mastering Blockchain:** Unlocking the Power of Cryptocurrencies, Smart Contracts, and Decentralized Applications. Sebastopol, California: O'Reilly Media, 2021.

LESAEGE, Clément; et. al. **Kleros Long Paper v2.0.2**. Júlio, 2021. Disponível em: https://kleros.io. Acesso em: 7 jun. 2025.

MORAES, Alexandre de. **Constituição do Brasil interpretada e legislação constitucional**. São Paulo: Atlas, 2002.

NARAYANAN, Arvind BONNEAU, Joseph *et al*., **Bitcoin and cryptocurrency technologies: a comprehensive introduction**. Princeton, Nova Jersey: Princeton University Press, 2016. E-book.

ORACLE. **O que é IoT?** Disponível em: https://www.oracle.com/br/ Acesso em: 16 jun 2025.

ORTOLANI, Pietro. Self-Enforcing Online Dispute Resolution: Lessons from Bitcoin. Publicação *online.* **Oxford Journal of Legal Studies**, 2015.

SWAN, Melanie. **Blockchain:** Blueprint for a New Economy. Sebastopol/Califórnia: O'Reilly Media, 2015.

TALAMINI, Eduardo; CARDOSO, André Guskow. ***Smart contracts*, "autotutela" e tutela jurisdicional**. Revista do Ministério Público do Estado do Rio de Janeiro nº 89, jul./set. 2023. Disponível em: https://www.mprj.mp.br/ Acesso em: 13 jun 2025.

TARTUCE, Flávio. **Manual de Direito Civil.**15. ed. Rio de Janeiro: Método, 2025. *E-book.* V. único.

THE MONEY MONGERS. **What are blockchain oracles?** Disponível em: https:// themoney mongers.com/blockchain-oracles.

VECHAIN. **Development Plan and Whitepaper**. Versão 1.0.0.0. 2018. Disponível em: https://www.vechain.org Acesso em: 7 jun. 2025.

XYO. Site oficial da empresa. Disponível em: https://xyo.network. Acesso em: 7 jun. 2025