VII ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS II

EDSON RICARDO SALEME

YURI NATHAN DA COSTA LANNES

RONALDO FENELON SANTOS FILHO

D597

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

Coordenadores: Edson Ricardo Saleme; Ronaldo Fenelon Santos Filho; Yuri Nathan da Costa Lannes – Florianópolis: CONPEDI, 2024.

Inclui bibliografia
ISBN: 978-85-5505-891-2
Modo de acesso: www.conpedi.org.br em publicações
Tema: A pesquisa jurídica na perspectiva da transdisciplinaridade

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito. 3. Governança e novas tecnologias. VII Encontro Virtual do CONPEDI (1: 2024 : Florianópolis, Brasil).

CDU: 34

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

VII ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS II

Apresentação

O VII ENCONTRO VIRTUAL DO CONPEDI, realizado em parceria com a Faculdade de Direito de Franca (FDF), com a Universidade UNIGRANRIO - Afya, com o Portucalense Institute For Legal Research - IJP e a Faculdad de Derecho da Universidad de la República Uruguaye, entre os dias 24 e 28 de junho de 2024, apresentou como temática central "A Pesquisa Jurídica na Perspectiva da Transdisciplinaridade". Esta questão suscitou intensos debates desde o início e, no decorrer do evento, com a apresentação dos trabalhos previamente selecionados, fóruns e painéis que no ambiente digital ocorreram.

Os trabalhos contidos nesta publicação foram apresentados como artigos no Grupo de Trabalho "DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS II", realizado no dia 27 de junho de 2024, que passaram previamente por no mínimo dupla avaliação cega por pares. Encontram-se os resultados de pesquisas desenvolvidas em diversos Programas de Pós-Graduação em Direito, que retratam parcela relevante dos estudos que têm sido produzidos na temática central do Grupo de Trabalho.

As temáticas abordadas decorrem de intensas e numerosas discussões que acontecem pelo Brasil, com temas que reforçam a diversidade cultural brasileira e as preocupações que abrangem problemas relevantes e interessantes, a exemplo do direito digital, proteção da privacidade, crise da verdade, regulamentação de tecnologias, transformação digital e Inteligência artificial, bem como políticas públicas e tecnologia.

Espera-se, então, que o leitor possa vivenciar parcela destas discussões por meio da leitura dos textos. Agradecemos a todos os pesquisadores, colaboradores e pessoas envolvidas nos debates e organização do evento pela sua inestimável contribuição e desejamos uma proveitosa leitura!

Prof. Dr. Edson Ricardo Saleme – UNISANTOS

Prof. Dr. Yuri Nathan da Costa Lannes – FDF

Prof. Dr. Ronaldo Fenelon Santos Filho

A LEGALIDADE DOS "SMART CONTRACTS" À LUZ DOS REQUISITOS DE VALIDADE DA TEORIA DO NEGÓCIO JURÍDICO

THE LEGALITY OF SMART CONTRACTS IN LIGHT OF THE VALIDITY REQUIREMENTS OF LEGAL TRANSACTION THEORY

Richard Henrique Domingos [1]
José Luiz de Moura Faleiros Júnior [2]
Luiz Felipe de Freitas Cordeiro [3]

Resumo

O presente trabalho tem como objeto de estudo os smart contracts e a tecnologia blockchain que os suporta. A pesquisa iniciará com uma análise aprofundada da rede blockchain, explorando suas características técnicas essenciais para entender como os smart contracts operam nesse ambiente. Será dada atenção especial à forma como esses contratos digitais são criados, executados e armazenados de maneira descentralizada, sem a necessidade de intermediários. A investigação segue com uma avaliação criteriosa dos requisitos de validade dos smart contracts à luz do Código Civil brasileiro. Essa análise focará em como essas ferramentas tecnológicas se encaixam nas categorias de agente capaz, objeto lícito, possível, determinado ou determinável e a forma que a lei prescreve ou não. O objetivo é esclarecer se os smart contracts podem ser considerados negócios jurídicos válidos, mesmo não se enquadrando no molde tradicional dos contratos. O trabalho também propõe um estudo sobre os desafios jurídicos e as implicações práticas da aplicação dos smart contracts, incluindo aspectos como a autonomia da vontade, a segurança jurídica e os potenciais conflitos normativos. Será adotado o método dedutivo para desenvolver a pesquisa, partindo de premissas gerais sobre a tecnologia blockchain e analisando casos específicos para verificar a aderência dessas tecnologias ao direito brasileiro. A conclusão buscará sintetizar os resultados encontrados e propor diretrizes para a integração harmoniosa entre as inovações tecnológicas dos smart contracts e o sistema jurídico brasileiro.

Palavras-chave: Smart contracts, Blockchain, Negócio jurídico, Validade, Direito civil

Abstract/Resumen/Résumé

This study focuses on smart contracts and the supporting blockchain technology. The research will begin with an in-depth analysis of the blockchain network, exploring its essential technical features to understand how smart contracts operate within this environment. Special attention will be given to how these digital contracts are created,

[1] Bacharel em Direito pela Faculdade Milton Campos. E-mail: richardtd6@gmail.com

[2] Professor da Faculdade Milton Campos. Doutor em Direito pela USP. Mestre e Bacharel em Direito pela UFU. E-mail: jose.faleiros@animaeducacao.com.br

[3] Mestrando e Bacharel em Direito pela Faculdade Milton Campos. E-mail: luiz.felipefreitasc@gmail.com

executed, and stored in a decentralized manner, without the need for intermediaries. The investigation continues with a meticulous evaluation of the validity requirements of smart contracts under Brazilian Civil Code. This analysis will focus on how these technological tools fit into the categories of capable agent, lawful object, possible, specific or determinable, and the form prescribed by law or not. The aim is to clarify whether smart contracts can be considered valid legal transactions, even though they do not fit the traditional contract model. The work also proposes a study on the legal challenges and practical implications of implementing smart contracts, including aspects such as autonomy of will, legal security, and potential normative conflicts. A deductive method will be adopted to develop the research, starting from general premises about blockchain technology and analyzing specific cases to verify the adherence of these technologies to Brazilian law. The conclusion will seek to synthesize the findings and propose guidelines for the harmonious integration between technological innovations of smart contracts and the Brazilian legal system.

Keywords/Palabras-claves/Mots-clés: Smart contracts, Blockchain, Legal transaction, Validity, Civil law

1 Introdução

Blockchain é uma tecnologia revolucionária que assegura o registro de informações de modo seguro e confiável, utilizando um sistema de armazenamento descentralizado. Esta inovação permite a codificação de dados sem a intermediação de terceiros, facilitando, assim, a interação direta entre usuários e garantindo transações transparentes e eficientes.

As contribuições da *blockchain* são vastas, englobando múltiplos setores, incluindo o desenvolvimento de *smart contracts* ("contratos inteligentes"), que não são propriamente uma nova modalidade de acordo ou contrato, mas uma nova maneira de se instrumentalizar a contratação a partir de protocolos de *software* executados automaticamente em ambientes virtuais específicos, conhecidos como Máquinas Virtuais (VM), e incorporados à rede *blockchain*.

Em síntese, *smart contracts* são desenvolvidos utilizando linguagens de programação em Ambientes de Desenvolvimento Integrado (IDEs, na sigla em inglês), assemelhando-se, em sua funcionalidade, a editores de texto. Caracterizam-se pela autoexecução, além de prover segurança, transparência, precisão e eficiência nas transações.

Este estudo visa comparar os *smart contracts* com os contratos firmados nos moldes tradicionais para destacar suas diferenças e explorar possíveis interações com esta tecnologia emergente que possam revelar sua compatibilidade com os requisitos de validade do negócio jurídico, definidos no artigo 104 do Código Civil brasileiro. Para isso, de início, serão introduzidos os conceitos fundamentais da *blockchain*, a base dos *smart contracts*, abordando sua relevância no campo da engenharia de *software* e nas redes de computadores. Em seguida, serão apresentadas a definição, as características e o funcionamento dos *smart contracts*, desde sua concepção até sua execução. Subsequentemente, se discutirá os princípios básicos da teoria do negócio jurídico, com ênfase nos requisitos de validade: agente capaz, objeto lícito, possível, determinado ou determinável e forma prevista ou não prescrita em lei.

Por opção de recorte temático, não serão analisados os pressupostos de existência e os fatores de eficácia do negócio jurídico, que eventualmente poderão ser analisados em futuros estudos. Ademais, a apresentação da base teórica que fundamenta os requisitos de validade do negócio jurídico será elucidada em comparação com os detalhamentos técnicos da rede *blockchain* com o objetivo de testar a hipótese de pesquisa, a partir da qual se defende que tais estruturas tecnológicas são válidas como mecanismo instrumental, mas não denotam novas espécies contratuais.

O método de pesquisa utilizado será o dedutivo, com base em revisão bibliográfica que conecta o direito digital ao direito civil. Por isso, far-se-á elucidação conceitual e estrutural que parte de aspectos mais gerais para a abordagem específica delimitada na hipótese de pesquisa acima mencionada. Ao final, uma conclusão será apresentada no intuito de apresentar possível solução para o tema-problema da pesquisa.

2 A *blockchain* e os *smart contracts*

2.1 Contexto histórico da tecnologia

Para iniciar qualquer abordagem relacionada aos *smart contracts*, imprescindível entender um elemento fundamental à compreensão do direito digital: onde residiria qualquer espécie de iniciativa voltada à sua regulação? Merecem expressa menção os casos em que regulação e tecnologia se relacionam por meio de incentivos, que "são aqueles em que a Administração impõe ou estimula o uso de uma determinada tecnologia" (BAPTISTA; KELLER, 2016, p. 136).

Em 2008, em busca de uma alternativa para a mitigação dos efeitos da crise econômica mundial decorrente da bolha inflacionária no mercado imobiliário dos Estados Unidos da América, foi compilado uma série de fundamentos matemáticos já existentes, a fim de criar uma moeda digital segura, descentralizada e sem a necessidade de intervenção de terceiros. Satoshi Nakamoto (pseudônimo atribuído ao seu criador), desenvolveu a primeira criptomoeda a ser mundialmente operacional (FALEIROS JÚNIOR; ROTH, 2019). O Bitcoin, como passou a ser chamado, operaria em uma rede descentralizada capaz de possibilitar as transações da referida moeda digital, valendo-se do uso de algoritmo, *hash* e criptografia. Com isso, a implementação de contratos inteligentes se torna propícia, uma vez que, sendo tão descentralizada, a rede *blockchain* possui grande confiabilidade. Para entender melhor como isto ocorre, porém, algumas considerações mais detalhadas se fazem necessárias (SWAN, 2015).

A comercialização de alta frequência (*high-frequency trading*, ou HFT) é um tipo de negociação algorítmica caracterizada por altas velocidades, altas taxas de rotatividade e altos índices de ordem para negociações baseadas na acumulação de dados financeiros de alta frequência e em ferramentas eletrônicas de negociação (MENKVELD, 2011). Embora não exista uma definição única de HFT, é certo que a "granularidade" algorítmica conduz a à

redução da volatilidade e dos riscos sistêmicos, conduzindo, ademais, à redução dos custos transacionais .

Nesse contexto, inicialmente, a *blockchain* surge como uma DLT ("*distributed ledger technology*"), ou seja, uma implementação específica da categoria mais ampla de razões compartilhadas, que são simplesmente definidas como um registro compartilhado de dados entre diferentes partes capaz de oferecer suporte distribuído confiável e seguro para realização de transações entre participantes que não necessariamente têm confiança entre si e que estão dispersos em larga escala numa rede de conexões "*peer-to-peer*".

2.2 Conceito e características estruturais

A tecnologia *blockchain* se tornou possivelmente a mais empolgante modalidade de tecnologia baseada em ledgers distribuídos no século XXI. Esse conceito, embora aparentemente complexo, tem seu funcionamento baseado em nós (*nodes*) – aqui entendidos como terminais ou computadores – que trabalham de forma coordenada pela rede para o atingimento de um resultado comum. Com mais detalhes, descreve Imran Bashir (2018, p. 12, tradução livre): "Os sistemas distribuídos são um paradigma de computação em que dois ou mais nós trabalham entre si de maneira coordenada para obter um resultado comum. Ele é modelado de forma que os usuários finais o vejam como uma única plataforma lógica (...)".

Sendo a "*blockchain*" uma rede capaz de efetuar vários registros ("*distributed ledger technology*") de forma segura, possibilitando que as pessoas se comuniquem diretamente, cria-se transparência nas informações transacionadas, sem a necessidade de uma terceira parte externa (entidades certificadoras e centralizadoras das transações de negócios, tais como bancos, governos, cartórios etc.) para a intermediação das relações entre as partes envolvidas na transação registrada.

A rede *blockchain* é resultado de uma engenhosa combinação de técnicas robustas provenientes da: (i) computação distribuída confiável; (ii) criptografia (chave assimétrica, funções "*hash*", desafios criptográficos); (iii) teoria dos jogos (mecanismo de incentivos).

Diferentemente de uma rede centralizada tradicional, que mantém e processa informações por um único servidor (com alta possibilidade de ser "hackeada"), a *blockchain* é uma rede descentralizada. Esta característica faz com que o processamento de dados se dê de maneira totalmente otimizada, proporcionando o compartilhamento de poder computacional (BUTERIN, 2017). Isto é, cada computador da rede pode exercer três funções, quais sejam, nó,

minerador ou usuário final (impossibilitando que o ataque em uma máquina macule as demais), conforme será explicado a seguir.

Além das peculiaridades mencionadas, a *blockchain* também possui algumas outras características como a comunicação direta entre as partes ("*peer-to-peer*"), registro de data e hora ("*time-stamp*") e a transparência (PEGORARO, 2022). Ainda, nesta rede ocorrerá a aplicação de conceitos como o pseudoanonimato e ampla auditabilidade.

2.2.1 Rede "*peer-to-peer*"

A arquitetura "*peer-to-peer*" (P2P) utilizada pela rede *blockchain*, nada mais é que um sistema no qual arquivos, documentos e informações podem ser compartilhados sem a necessidade de um servidor central, isto é, acontecendo de pessoa para pessoa, sem a interferência de um terceiro.

Para facilitar a compreensão de como acontece o compartilhamento destes arquivos, documentos e informações sem a interferência de um terceiro, imagine-se em uma situação em que é realizada uma transferência bancária. Neste caso, é indispensável a intermediação de um banco para efetuá-la em todos os sentidos. A *blockchain*, por sua vez, se vale da arquitetura "*peer-to-peer*" para a efetivação desta transferência (PEGORARO, 2022). Os indivíduos não dependem de um banco – servidor central – para efetuá-la, pois a própria rede, de forma descentralizada, e pela cooperação de seus participantes, provê a possibilidade de comunicação direta, dispensando a necessidade de um terceiro centralizador.

2.2.2 Função "*hash*"

A função "*hash*" é basicamente uma representação criptográfica de dados de entrada[1], isto é, uma derivação criptográfica do dado de entrada e uma representação numérica (identificada computacionalmente), figurando, então, como o identificador único dos dados lançador no livro-registro (*ledger*) da *blockchain* (NAKAMOTO, 2008). Noutros termos, trata-se de um valor alfanumérico que identifica o bloco de forma única – é entendido, nesse sentido, como uma impressão digital (*digital fingerprint*) dos elementos caracterizadores de um bloco (DE FILIPPI; WRIGHT, 2018, p. 112). O cálculo de um *hash* é feito em função de todos os elementos que compõem um bloco, como *input*. Assim, *f (block) = hash*. Ou seja, o cálculo é

[1] A entrada de dados é o processo de transcrição de informações em um meio eletrônico, como um computador ou outro dispositivo eletrônico. Pode ser executada manual ou automaticamente usando uma máquina ou computador.

feito com o uso de *index*, *timestamp*, *previous hash*, *data* e *nonce*, de forma que *f (block) = f (index + timestamp + previous hash + data + nonce) = hash*. *Previous hash*, nesse sentido, é o *hash* do bloco anterior, necessário para o cálculo do *hash* para que haja, então, o encadeamento entre os blocos. No caso de um bloco-gênese, o valor de *previous hash* é 0 (porque não há um bloco anterior). *Nonce*, por fim, é um número único, que é utilizado para o encontro de um *hash* válido, ou seja, para o encontro de um *hash* que permita o registro do bloco na cadeia de blocos, pelo consenso dos usuários. Em outras palavras, o processo de determinar esse *nonce* é a mineração, que será tratada adiante. O nonce é, então, encontrado após a seguinte questão: "quantas iterações são necessárias a fim de encontrar um novo e válido bloco?" (TAPSCOTT; TAPSCOTT, 2016)

Como se nota, a função "*hash*" tem o intuito de garantir a integridade dos arquivos transmitidos, convertendo um grupo de caracteres, também conhecido como chave, para outro valor de determinado comprimento em formato hexadecimal.

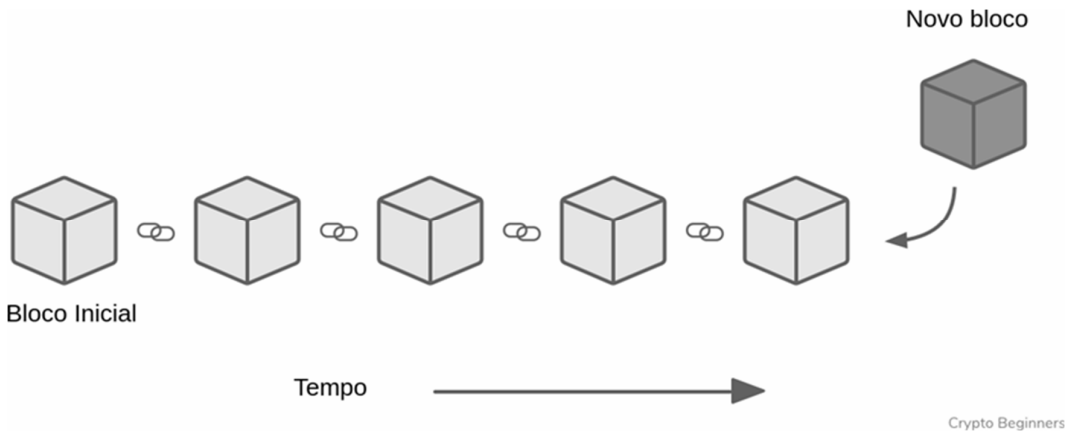
Existem diferentes tipos de funções "*hash*" criptográficas, de modo que todas elas possuem quatro propriedades em comum (RHODES, 2018): (i) são computacionalmente eficientes; (ii) são determinísticas; (iii) resistem à pré-imagem, pois, a partir da saída de uma função "*hash*", deve ser difícil encontrar o valor de entrada utilizado para gerá-la; (iv) são resistentes a colisões, uma vez que deve ser praticamente impossível encontrar "*hashes*" iguais a partir de mensagens diferentes.

O processo de validação necessita, neste ponto, do consenso entre os usuários (*peers*) quanto à validade de um bloco, que surge, em seu turno, pela necessidade do registro dos mais recentes dados (como as mais recentes transações financeiras, que, para serem validadas, necessitam ser adicionadas em um bloco da cadeia). Estes usuários formam uma rede (*peer-to-peer*) – originalmente (ou seja, na estrutura inicial da tecnologia blockchain), uma rede descentralizada (cuja validação não é feita por uma autoridade central).

2.2.3 Criação de blocos (*blocks*)

Conforme se depreende da figura abaixo, a *blockchain* é uma rede que funciona a partir de blocos encadeados seguros que sempre carregam uma informação junto a uma impressão digital (PRADO, 2017). Essa definição, embora possa ser inferida da própria tradução literal, da língua inglesa para a portuguesa, das palavras "*chain*" (corrente ou cadeia) e "*block*" (bloco), é simbolicamente relevante para que se visualize o motivo pelo qual os lançamentos registrais distribuídos se tornam confiáveis e seguros:

Figura 1 - Relação entre tempo, bloco de início e novo bloco.



Fonte: adaptado de (PRADO 2017)

Cada bloco fechado é distribuído em toda a rede, sendo que cada nó – conceito que será explicado no próximo tópico – terá uma cópia de todos os blocos registrados (PEGORARO, 2022). Cria-se, assim, um banco de dados distribuído de registros, ou razão pública, de todas as transações ou eventos digitais, que foram realizados e compartilhados entre as partes participantes, contendo cada bloco 4 tipos de informações: I - a data da transação; II - dados, armazenados em formato de texto; III – "*hash*" do bloco; IV – "*hash*" do bloco anterior (ABREU, 2020).

No caso da alteração (*hack*) de um bloco já adicionado à cadeia, por um determinado *peer*, este bloco alterado e os blocos em sua sequência serão rejeitados pelos demais *peers*, considerando-os, então, como inválidos. Este atributo traz uma das características centrais da *blockchain*: que a cadeia de blocos é quase imutável – ou seja, a sua alteração é inviável (*infeasible*), embora seja, tecnicamente, possível.

2.2.4 "Nós" (*nodes*) de uma rede

Os nós na rede *blockchain* são basicamente pontos de conexão, cuja função é figurar como local na rede onde a informação é criada, recebida e transmitida. Simplificando, os nós de uma rede *blockchain* são computadores dentro de uma rede que recebem, compartilham e validam informações (GATTESCHI, et al., 2018).

São estes computadores dentro de uma rede como a *blockchain* que recebem e compartilham informações e contribuem diretamente para o funcionamento do sistema, uma vez que sua aderência à rede possibilita o sistema descentralizado.

Como incentivo à aderência, em forma de contribuição para rede pública descentralizada, a "*blockchain*" propicia elementos como o "*Proof of Work"*, mecanismo que tem como objetivo recompensar monetariamente os que ajudam esse tipo de rede a operar.

2.2.5 Registro e criptografia

Como explicado anteriormente, a *blockchain* é uma tecnologia que permite a criação, verificação e atualização de registros de forma pública. Possui como um dos pilares do seu registro um mecanismo que permite que a informação se comunique de forma segura dentro da rede: a criptografia. Rudimentarmente, a criptografia nada mais é que a compartimentalização de informações em um universo do recipiente da mensagem. Este irá entendê-la de forma lógica e coerente, ao passo que um terceiro não destinatário daquele conteúdo terá acesso apenas a um embaralhado de letras.

Ou seja, a criptografia é a responsável pela proteção das informações contra o acesso não autorizado (PEGORARO, 2022). Criptografa-se uma mensagem enviada usando um algoritmo criptográfico com uma chave que só é conhecida pelo remetente e pelo destinatário. Um interceptador pode conseguir obter uma mensagem criptografada, mas não será capaz de decifrá-la. Na *blockchain*, a criptografia utilizada é denominada como SHA-256[2], a qual opera da seguinte maneira: qualquer informação inserida (texto, imagem, vídeo) é transformada em uma assinatura eletrônica (chamada de "*hash*"). Trata-se de mecanismo extremamente seguro.

2.2.6 Tipologia da *blockchain* (pública, privada e híbrida)

Há três classificações possíveis para a *blockchain*: pública, privada e híbrida. A rede pública (ou "não-permissionada"), como o próprio nome diz, é uma rede de acesso público, na qual é possível transacionar de forma aberta, a partir da livre e espontânea vontade de quem esteja interessado em participar (BUTERIN, 2017). O fato de a *blockchain* ser pública não ocasiona a publicidade dos dados pessoais ali armazenados, que estão criptografados. Isso significa que todos os membros da rede podem receber e enviar transações de, e para qualquer pessoa no mundo, além de poder interagir com contratos inteligentes publicados nessa rede.

[2] Diz a doutrina: "Se trata de una función hash iterativa y unidireccional que puede procesar datos de entrada, como un cadena de texto o un archivo, para producir una representación condensada de longitud fija llamada *digest*. Este algoritmo determina la integridad de los datos de entrada, es decir, cualquier cambio en los datos de entrada producirá un *digest* diferente. Esta propiedad es útil en la generación y verificación de firmas digitales y códigos de autenticación de mensajes, así como la generación de números aleatorios o *bits*". (GÓMEZ, 2018).

A rede *blockchain* privada, também denominada como “permissionada”, caracteriza-se pelo fato de somente poder participar da rede quem for autorizado por quem faz o controle dessa *blockchain*. Isso significa que, os seus nós são conhecidos, devidamente cadastrados e possuem acesso restrito (PEGORARO, 2022). Por outro lado, isso não significa que tal tipo de rede seja centralizada, porque apenas os membros da rede podem participar e interagir com ela, através de um acesso particular. Contudo, devido a essas restrições, a sua descentralização pode ser questionada, o que acaba restringindo a sua utilidade a contextos específicos.

A rede híbrida, também chamada de consórcio de *blockchains*, é uma combinação de redes públicas e privadas capaz de unir os melhores atributos das duas espécies anteriores, pois, basicamente, neste tipo de rede, os seus membros podem decidir quem pode participar da rede ou quais transações são tornadas públicas (ABREU, 2020).

2.2.7 Mineração

Mineração é o processo pelo qual um bloco é conectado em outro na rede *blockchain*. A mineração ocorre por meio do protocolo de consenso, que é o núcleo da *blockchain* que representa seu método ou o protocolo que realiza a transação, sendo, assim, um processo que disponibiliza o poder computacional para resolução de desafios criptográficos mediante incentivo financeiro.

Esse incentivo financeiro será o próprio ativo e também as taxas de transação (ABREU, 2020). O valor dessa taxa de transação é oferecido por quem está transacionando e, pode ou não, ser aceito pelo minerador que irá fazer encontrar o “*hash*” válido para que se efetue o registro.

Este processo de mineração não apenas garante a segurança e a integridade da rede *blockchain*, mas também é fundamental para a criação e a distribuição de novas unidades do criptoativo vinculado à caixa de blocos.

À medida que os mineradores solucionam complexos quebra-cabeças criptográficos para adicionar novos blocos à cadeia, eles ajudam a validar e a registrar transações de maneira descentralizada. Essa atividade, embora custosa em termos de energia e recursos computacionais, é crucial para o funcionamento autônomo da rede, eliminando a necessidade de uma autoridade central e assegurando a confiança entre os participantes desconhecidos dentro da rede.

Cumpre salientar que a emissão primária desses ativos se dá com a mineração. Baseando-se na mesma ideia do senso comum da mineração enquanto atividade extrativista,

em que o minerador está em um constante trabalho em busca da riqueza mineral, a mineração de criptoativos é uma busca. Entretanto, ocorre no ambiente digital, por tentativa e erro de achar o nó, no caso do *PoW (Proof of Work)*, e conectar um bloco a outro.

2.2.8 Mecanismos/algoritmos de consenso: *Proof of Work* (PoW) e *Proof of Stake* (PoS)

Quando se está diante de um banco de dados centralizado, a verdade dentro deste banco é aquilo que o administrador define. Ocorre que, na sistemática de banco de dados descentralizados/distribuídos, como na rede *blockchain*, é necessário que se obtenha consenso para que os participantes saibam o que é a verdade. Por esta razão, a tecnologia em comento utiliza como mecanismo específico para chegar à verdade um conjunto de regras que descreve como funciona a comunicação e registro da transmissão de dados entre dispositivos eletrônicos conhecidos como nós.

Na blockchain existem vários mecanismos de consenso, sendo os mais comuns denominados de *Proof of Work* e *Proof of Stake*.

O *Proof of Work* foi o primeiro implementado e utilizado na *blockchain* como mecanismo de consenso. Em tradução literal, a "prova de trabalho" ou *PoW* (do inglês, *Proof-of-work*), se trata de um modelo para conclusão das transações baseado em uma competição realizada entre os mineradores, que são grupos de pessoas que recebem taxas e subsídios da rede a partir da geração de novos blocos para a *blockchain* (PEGORARO, 2022).

Eles utilizam o poder computacional de suas máquinas e placas gráficas para resolver problemas matemáticos difíceis ("*hashes*") impostos pela rede para que uma transação seja efetuada. Este modelo, porém, exige grande gasto energético já que muitos validadores competem pelo mesmo problema matemático ao mesmo tempo, e a partir da resolução do problema por um deles, o trabalho realizado por todos os outros participantes é descartado e não agrega valor ao protocolo (SULTAN; RUHI; LAKHANI, 2018).

Por outro lado, o *Proof of Stake* ou *PoS*, é um algoritmo de consenso que propõe maior escalabilidade. Isso porque ele funciona a partir de validadores, nome dado àqueles que atuam na manutenção da rede, congelando seus próprios *tokens* como garantia para validarem as operações, garantindo que não haja informações erradas ou fraudulentas nos blocos (ABREU, 2020).

2.2.9 *Wallet*

Para interagir com aplicações descentralizadas e utilizar um *smart contract* é necessária uma carteira (*wallet*). A *wallet* é um local que mantém as chaves privadas protegidas e acessíveis, as quais lhe dão acesso a criptoativos, permitindo ao seu proprietário que envie e receba tais ativos, como *Bitcoin* e *Ethereum*, em transações não intermediadas.

O conceito formal de "criptoativo", aliás, foi definido, no país, pelo artigo 5º, inciso I, da Instrução Normativa nº 1.888/2019 da Receita Federal do Brasil como "a representação digital de valor denominada em sua própria unidade de conta, cujo preço pode ser expresso em moeda soberana local ou estrangeira, transacionado eletronicamente com a utilização de criptografia e de tecnologias de registros distribuídos, que pode ser utilizado como forma de investimento, instrumento de transferência de valores ou acesso a serviços, e que não constitui moeda de curso legal". São tais ativos que são adicionados às *wallets* e, por isso, elas possuem vários formatos, desde carteiras em *hardware* como a *ledger* (formato semelhante a um *pendrive* USB), a aplicativos para celular, que tornam as transações mais acessíveis às pessoas. Ao contrário de uma "carteira normal", as *wallets* também são capazes de armazenar diversos ativos digitais em formato de *tokens*, como os *non-fungible tokens* (NFT's)[3].

Será também por meio da "*wallet*", através do seu administrador, nome dado ao dono de um contrato inteligente, representado pela carteira, que se realizará o processo de implantação do contrato em uma rede *blockchain*. O dono de um contrato inteligente é o único capaz de operá-lo, salvo configuração prévia permitindo a inclusão de novos usuários, ou transferência do título de administrador para outra carteira. Um contrato inteligente também pode ser utilizado e acionado por outro contrato, na medida que um deles tenha posse do endereço do outro contrato publicado na rede *blockchain*, e estejam configurados corretamente para acionar ou receber funções um do outro (UHDRE, 2023).

Além disso, a interação entre carteiras facilita a execução de transações complexas e automatizadas, definidas pelas condições programadas nos *smart contracts*. Essa característica permite a criação de ecossistemas econômicos digitais sofisticados, nos quais transações e acordos são executados de forma transparente e sem a necessidade de intermediários

[3] Um NFT, sigla para *non-fungible token* (*token* não fungível), é um tipo de ativo digital único que representa a propriedade ou prova de autenticidade de um item específico, usando a tecnologia *blockchain* para garantir sua singularidade e propriedade. Ao contrário de criptoativos como Bitcoin ou Ethereum, que são fungíveis e podem ser trocadas por uma unidade de valor igual, cada NFT é distinto e não pode ser trocado em igualdade com outro NFT. Eles podem representar uma ampla gama de ativos tangíveis e intangíveis, como obras de arte, colecionáveis, vídeos, músicas e até mesmo ativos imobiliários virtuais, permitindo a comercialização de propriedade digital com direitos de propriedade claramente definidos (BARBOZA; FERNEDA; SASS, 2021).

tradicionais, como bancos ou agentes financeiros. Essa autonomia não apenas agiliza o processo, mas também reduz significativamente os custos associados às transações, democratizando o acesso a serviços financeiros e criando novas oportunidades de negócios.

2.3 *Smart contracts* e seu funcionamento

O surgimento da tecnologia *blockchain* tornou possível a utilização prática dos *smart contracts*, idealizado primeiramente, na década de 90, pelo jurista e programador Nick Szabo (1997). Basicamente, são programas de computador, *softwares*, que podem ser executados em uma rede *peer-to-peer* (P2P) com o objetivo de automatizar a execução daquilo que foi programado, sem a necessidade de uma autoridade externa confiável.

Diferentemente dos modos tradicionais de formalização de contratos, pela base tecnológica dos "*smart contracts*", a parte de monitoramento e execução do instrumento é transferida para a infraestrutura tecnológica e não para um terceiro interventor, trazendo, portanto, quando executados em uma rede *blockchain*, os benefícios da confiabilidade e autoexecução, independentemente de ser ter sido feito o "*deploy*" em uma *blockchain* ou não (SAVELYEV, 2017).

2.3.1 Administrador *("Wallet")* e *"Deploy"*

Conforme exposto no capítulo anterior, o usuário responsável pela inserção de um *smart contract* na *blockchain*, representado pela carteira (*wallet*), será o responsável por realizar o processo de "*deploy*[4]" do contrato. O administrador será o único capaz de operá-lo, exceto caso se parametrize previamente a permissão para inclusão de novos usuários, ou se transfira o título de administrador para outra carteira.

2.3.2 Equipamentos e *softwares* utilizados

A *Ethereum* é uma plataforma de computação distribuída pública que utiliza a rede *blockchain*, com a capacidade de desenvolver e executar *smart contracts* e aplicativos descentralizados. Possivelmente, é a mais importante rede quando o assunto envolve a utilização e aplicação dos *smart contracts*.

[4] É a implantação é a fase do ciclo de vida de um software, no contexto de um Sistema de Informação, que corresponde textualmente à passagem do software para a produção.

A plataforma é constituída por máquinas virtuais descentralizadas denominadas de *Ethereum Virtual Machines* (EVM) que executam os contratos (MASCARENHAS, VIEIRA e ZIVIANI, 2018). Um contrato é ativado quando seu endereço é chamado como destino por uma transação. A partir do seu acionamento, o contrato é executado automaticamente em cada nó da rede (CHRISTIDIS; DEVETSIKIOTIS, 2016).

A plataforma *Ethereum* foi criada por Vitalik Buterin em janeiro de 2014, marcando o início da tecnologia *blockchain* de segunda geração. Essa plataforma vai além da transferência de valores e pagamentos, com a criação da moeda digital *Ether* e a possibilidade de executar e ativar contratos inteligentes. Além disso, por ser uma plataforma programável ela torna capaz o desenvolvimento de contratos e aplicações de forma descentralizada (WOOD, 2014).

2.3.3 Linguagem "Solidity"

Solidity é uma linguagem de programação de alto nível, originalmente baseada nas linguagens *Python, Javascript e C++*. A *Solidity* foi criada com o propósito de permitir a escrita de *smart contracts* de forma simples para a rede *Ethereum*. É uma linguagem projetada para aproveitar ao máximo a Máquina Virtual *Ethereum*, permitindo a criação e desenvolvimento de contratos inteligentes que podem ser executados de forma otimizada e autônoma. Para isso, o programador pode desenvolver seus aplicativos em uma linguagem de fácil utilização, leitura e manutenção para que, ao finalizar, a *engine Solidity* converta aquele código simples para código de máquina, e assim a EVM[5] irá compilar e implantar o código na *blockchain* (SOLIDITY, 2022).

Esta abordagem facilita significativamente o desenvolvimento de aplicações descentralizadas (*dApps*) e outros tipos de *smart contracts*, abrindo um vasto campo de possibilidades para inovação e implementação de soluções na *blockchain*. Ao minimizar as barreiras técnicas e tornar o desenvolvimento de *smart contracts* mais acessível, a *Solidity* promove uma inclusão maior de desenvolvedores no ecossistema Ethereum, permitindo que uma gama diversificada de projetos beneficie-se das vantagens da tecnologia subjacente à sua operacionalização computacional. Além disso, a contínua evolução e otimização da linguagem Solidity, alinhada às atualizações da *Ethereum Virtual Machine* (EVM), asseguram que o ambiente de execução seja seguro, eficiente e compatível com os mais recentes padrões e

[5] *Ethereum Virtual Machine*.

necessidades do mercado, estimulando a inovação contínua dentro da comunidade de desenvolvedores *blockchain*.

2.3.4 "Gas" (ETH)

O termo "*gas*" é utilizado para contabilizar a taxa paga à rede *blockchain* para transações de criptomoedas e execução de contratos inteligentes. Portanto, o "*gas*" é uma unidade de medida responsável por medir e recompensar o esforço computacional para realizar as operações na *blockchain*, servindo como uma força vital para manutenção da rede.

3 Requisitos de validade da teoria do negócio jurídico e os *smart contracts*

3.1 Formas tradicionais de contratação vs. *smart contracts*

Os contratos tradicionais ocupam o primeiro lugar entre os negócios jurídicos e são, justamente, aqueles por meio dos quais os envolvidos em um acordo de vontades combinam os seus interesses, constituindo, modificando ou solvendo algum vínculo jurídico. Mais especificamente, são colocados entre os atos-negócios jurídicos bilaterais criadores de uma situação jurídica individual. (RIZZARDO, 2022). Noutros termos, pode-se dizer que "o contrato é uma espécie de negócio jurídico que se distingue na formação, por exigir a presença de pelo menos duas partes. Contrato é, portanto, negócio jurídico bilateral ou plurilateral" (FARIAS; ROSENVALD, 2017, p. 68).

Como negócio jurídico, entende-se o ato jurídico humano, onde a manifestação de vontade é relevante, com objetivo de atingir os efeitos legais pretendidos pelas partes dentro do campo da autonomia privada. Ainda, a vontade das partes, sem a presença de vícios, tem papel fundamental na produção dos seus efeitos jurídicos::

> Os elementos gerais são aqueles indispensáveis à existência de todo e qualquer negócio. Quais são eles exatamente? A rigor, tomada a palavra elemento, em seu significado já definido, somente aquilo que efetivamente constitui o negócio é que poderia ser considerado elemento, ou seja: a forma, que a declaração toma, isto é, o tipo de manifestação que veste a declaração (escrita, oral, mímica, através do silencia etc.), o objeto, isto é, o seu conteúdo (as diversas cláusulas de um contrato, as disposições testamentárias, o fim que se manifesta na própria declaração etc.) e, finalmente, as circunstâncias negociais, ou seja, o que fica da declaração de vontade, despira da forma e do objeto, isto é, aquele quid, irredutível à expressão e ao conteúdo, que faz com que uma manifestação de vontade seja vista socialmente como destinada à produção de efeitos jurídicos (AZEVEDO, 2010, p. 32).

Nesse sentido, o contrato é um instrumento jurídico que tem o objetivo de estabelecer direitos e deveres entre as partes que celebram algum tipo de negócio jurídico, tornando-se uma ferramenta para assegurar que cada parte cumprirá suas obrigações. Esse pacto é o pilar fundamental de qualquer negócio jurídico, fazendo-se presente em diversas atividades e relações humanas, com o objetivo de estabelecer as regras que devem ser cumpridas e respeitadas na vida em sociedade, caracterizando-se, assim, como garantia das regras existentes nas relações jurídicas estabelecidas em qualquer negócio.

Quando se relaciona os contratos tradicionalmente firmados aos *smart contracts*, surgem dúvidas que são rapidamente solvidas ao se perceber que a tecnologia *blockchain*, como base subjacente à perfectibilização do negócio jurídico, nada mais é que um mecanismo instrumental, pois contribui para a delimitação de nova forma de sacramentação das vontades expressadas pelos envolvidos. No mais, tal base tecnológica ainda permeia o conteúdo negocial quanto ao modo como sua estruturação é redigida: em linguagem de programação (Solidity, por exemplo), e não no vernáculo. A execução contratual, denotada a partir da automatização do *enforcement* obrigacional, é um terceiro elemento que chama a atenção, pois denota curiosa prescindibilidade dos mecanismos judiciais tradicionais.

Todavia, há de se observar que os *smart contracts* não se distanciam muito dos contratos tradicionais, uma vez que estes são compatíveis com o direito contratual brasileiro, em aspectos quanto à forma, formação e princípios como o da autonomia da vontade e função social do contrato.

Conforme prevê o art. 107 do Código Civil, os negócios jurídicos decorrem do consensualismo, ou seja, não necessitam de uma forma fixa para existirem, sendo necessário apenas o consenso das partes para se aperfeiçoar, sendo assim classificados como ‘‘não solenes’’, ou ‘‘não formais’’. Ainda, os contratos podem ser considerados como típicos, que são aqueles em que o Código Civil estabelece designação própria. Por outro lado, atípicos, aqueles criados pelas partes com base no princípio da autonomia da vontade, nos quais os contraentes preferem não utilizar os modelos legais, para pactuação de suas obrigações, conforme prevê o art. 425 do Código Civil.

Isso significa que os *smart contracts*, como quaisquer outros pactos celebrados analogicamente, são decorrentes de acordo de vontade entre as partes de uma operação econômica instrumentalizada de forma atípica, através da tecnologia, com base no princípio da autonomia da vontade. Variam, portanto, somente quanto à forma e à apresentação, mas ainda exigem agentes capazes de expressar a vontade para a conclusão do sinalagma negocial e para a conformação do vínculo obrigacional.

Quanto à formação, revisão e extinção dos contratos inteligentes, também é possível verificar que estes pontos caminham lado a lado com os princípios da autonomia da vontade e da função social do contrato, pilares essenciais para o direito contratual brasileiro, o que reforça a importância do requisito de validade previsto no artigo 104, inciso I, do Código Civil. Isso porque a autonomia da vontade está relacionada à liberdade de contratar, na seguridade das partes poderem decidirem nos ajustes do contrato, estabelecendo cláusulas conforme definirem, que se submetem, no entanto, a limites, não podendo ofender outros princípios ligados à função social do contrato (RIZZARDO, 2022).

Durante a formação de um *smart contract*, sabe-se que deve haver a concordância entre as partes sobre os termos que irão executar o programa, ao passo que as partes são livres para escolher com quem desejam firmar o *smart contract*, seu objeto e sua duração. Ou seja, o instrumento é plenamente compatível com o princípio tratado, ainda que a sua aplicação seja mais complexa durante a fase da estruturação redacional, baseada em código, e, considerando que cabe às partes a análise das particularidades de cada situação para decidirem se será mais favorável a adoção de solução registral de um *smart contract* em uma *blockchain* ou do modelo de contrato tradicional, também eventual interpretação do conteúdo textual demandará acuidade em relação às exigências derivadas da boa-fé objetiva, em particular à previsão do artigo 113, § 1º, inciso IV, do Código Civil, pelo qual a interpretação do negócio jurídico deve lhe conferir o sentido que "for mais benéfico à parte que não redigiu o dispositivo, se identificável".

Já o princípio da função social do contrato relaciona-se à limitação da autonomia das partes, vez que tem como objetivo que o instrumento entre os pactuantes deve também buscar a sua conformidade com os interesses sociais. Conforma-se com a tecnologia *blockchain*, pelo fato de existirem ferramentas e funcionalidades entrelaçadas ao contrato, pautadas na governança do contrato, capazes de modificá-lo. Isto só ocorre, contudo, desde que seja previamente estabelecido, com o objetivo de moldar o protocolo do contrato, incluir melhorias e até mesmo alterá-lo, concedendo às partes o poder de extinguir ou rever o contrato instrumentalizado por código na *blockchain*.

Nesse sentido, conclui-se que, não há incompatibilidade de tal instrumento jurídico tecnológico com o direito civil brasileiro no que diz respeito à estruturação da forma, pois esta não é vedada pela legislação, embora também não esteja textualmente prevista, o que se coaduna com o requisito de validade do artigo 104, inciso III, do Código Civil. A rigor, é inegável que o que se verifica é que a peculiaridade desta nova forma de contratação está na maneira como ocorre a sua aceitação para desencadear o posterior registro de seus termos em estruturas não escritas em linguagem natural, mas em linguagem computacional. Tal se verifica,

pois, na medida em que um *smart contract* só passa a ter forma efetiva no momento em que seu conteúdo é totalmente programado.

A mudança de perspectiva que se cria é totalmente lastreada em maneiras computacionalmente eficientes de deflagração do código, o que não sufraga, também, a obrigatoriedade de que o conteúdo contratual enderece objeto previamente determinado, pois a determinabilidade condicional se mostra impossível para o caso de conjuntos de código que devem ser previamente inseridos a ponto de viabilizar futuro *enforcement* sem o risco da editabilidade. Nesse aspecto, o requisito de validade indicado pelo legislador no artigo 104, inciso II, do Código Civil, demanda interpretação mais restritiva quanto ao objeto, que deve ser lícito e possível, mas necessariamente determinado.

3.2 Técnica jurídica, formação e conclusão do contrato

Conforme foi demonstrado no presente trabalho, os *Smart Contracts* são basicamente instrumentos contratuais eletrônicos, com a possibilidade de serem autoexecutáveis, celebrados por meio da tecnologia denominada *blockchain*. Pelo fato de essa tecnologia possuir características como da observalidade, verificabilidade e privacidade, revela-se mais acentuada a capacidade disruptiva que se extrai das possibilidades de aplicação da tecnologia *blockchain* e dos *smart contracts* aos negócios jurídicos que sejam compatíveis com a leitura restritiva que se deve fazer quanto ao objeto e à cautela com a estruturação da forma.

Nesse cenário, há de se salientar o grande potencial do uso dessa tecnologia em diversos setores e modelos de negócios. Primeiramente, a tecnologia *blockchain* contribui para que as partes possam concretizar uma transação contratual de maneira remota e segura na medida em que, somente quando satisfeitas as condições acordadas preliminarmente é que o negócio se realizará. Ademais, em especial nos setores financeiro e comercial, tal tecnologia pode ser usada para agilizar meios de pagamento, para dinamizar o despacho e a liquidação de operações em plataformas de negociação e cartas de crédito automáticas, além de propiciar operações menos burocráticas para quem deseja usufruir desta tecnologia para transferir dinheiro sem precisar de um terceiro envolvido, ou seja, um banco ou autoridade central, embora este último aspecto ainda esbarre em problemas penais, como a evasão de divisas e a lavagem de capitais, que podem afastar a licitude do objeto contratado (SILVEIRA; CAMARGO, 2021).

Acerca de todas as definições expostas neste presente trabalho, bem como em relação às formas de aplicação da tecnologia ora explanada, é possível observar que, para que seja realizada a devida análise sobre o assunto, que é repleto de peculiaridades conceituadas em

termos técnicos e tecnológicos, deve o operador do direito ser devidamente capacitado para realizar a interpretação do instrumento contratual elaborado com suporte tecnológico com o objetivo de alcançar as finalidades dadas aos meios de aplicação da tecnologia *blockchain* e aos objetivos pretendidos pelas partes.

Neste contexto, vem à tona a importância do engajamento interdisciplinar que, muitas vezes, pode estar aquém do entendimento que operadores do direito podem ter em relação à tecnologia. Isso porque, devido à grande complexibilidade do assunto, para a implantação de *smart contracts* eficientes e que respeitem os requisitos de validade estabelecidos pela legislação, será necessário que os operadores do direito se atentem às novas ferramentas de implementação da tecnologia *blockchain*, bem como às terminologias utilizadas, além de haver a necessidade de uma atuação cada vez mais próxima aos profissionais da área de tecnologia, como programadores e desenvolvedores.

4 Considerações finais

Os *smart contracts*, aliados à tecnologia *blockchain*, já demonstram seu papel fundamental no desenvolvimento de variados modelos de negócios, evidenciando o imenso potencial que esses instrumentos detêm para a inovação nas transações de diversos tipos de bens. Entretanto, tanto os *smart contracts* quanto a tecnologia *blockchain* ainda estão em processo de evolução e amadurecimento, o que exige a resolução de problemas e um acompanhamento cuidadoso de seu desenvolvimento.

Nos últimos anos, observou-se um aumento significativo na quantidade de materiais publicados sobre o tema, particularmente em português. Esse fenômeno reflete a rápida evolução dessa tecnologia, que torna a pesquisa em *blockchain* um desafio constante.

Smart contracts, ao serem executados dentro de uma rede *blockchain*, incorporam mecanismos inerentes à tecnologia, como a mineração e o uso de *nonces* (números utilizados uma única vez), para garantir segurança e quase-imutabilidade. A mineração é o processo pelo qual as transações são verificadas e adicionadas ao bloco, envolvendo a resolução de complexos problemas criptográficos. Essa atividade não apenas valida as transações e os termos do contratos, mas também assegura sua resistência a alterações, dado que qualquer tentativa de modificação exigiria a reexecução de todos os blocos subsequentes, um esforço computacionalmente inviável. O *nonce*, por sua vez, é um elemento crucial na prevenção de ataques de repetição e na garantia da ordem cronológica das transações, contribuindo para a

segurança do processo de mineração e, consequentemente, da integridade dos termos pactuados pelos contratantes.

Por outro lado, as *wallets* (carteiras digitais) desempenham um papel fundamental ao armazenar as chaves privadas dos usuários, permitindo a interação segura com os *smart contracts* na *blockchain*. A execução de um *smart contract*, especialmente na rede Ethereum, requer o pagamento de *gas*, uma taxa que cobre o custo computacional da execução do contrato. Esse mecanismo assegura que os contratos sejam executados de maneira eficiente, prevenindo a sobrecarga da rede por meio da limitação de operações que consomem muitos recursos. Assim, a combinação desses elementos – mineração, *nonce*, *wallets*, e *gas* – promove a segurança e a eficiência da rede *blockchain* e também oferece às partes contratantes uma plataforma robusta para a realização de acordos, com garantias de segurança jurídica advindas da transparência, integridade e execução automática dos termos contratados.

Enfatiza-se que os *smart contracts* podem ser considerados contratos atípicos absolutamente compatíveis com o direito brasileiro, pois não violam os requisitos de validade estabelecidos na teoria do negócio jurídico, mesmo estando estruturados em forma de código computacional. No mais, também não há óbice à sua utilização, ainda que se constate que o objeto do negócio jurídico deverá ser lícito, possível e determinado, afastando-se a determinabilidade potencial em razão da necessidade de segurança na delimitação do código no exato momento em que se formaliza o registro na *blockchain*.

Referências

ABREU, Antônio Welligton dos Santos. **Uma abordagem baseada em blockchain para armazenamento e controle de acesso aos dados de certificados de alunos do ensino superior.** 2020. 146 f. Dissertação (mestrado) – Universidade Federal do Ceará, Campus de Quixadá, Programa de Pós-Graduação em Computação, Quixadá, 2020. Disponível em: https://repositorio.ufc.br/handle/riufc/55477. Acesso em: 05 abr. 2024.

AZEVEDO, Antonio Junqueira de. **Negócio jurídico**: existência, validade e eficácia. 4. ed. 7. Tiragem. São Paulo: 2010.

BAPTISTA, Patrícia; KELLER, Clara Iglesias. Por que, quando e como regular as novas tecnologias? Os desafios trazidos pelas inovações disruptivas. **Revista de Direito Administrativo**, Rio de Janeiro, v. 273, n. 3, p. 123-163, set./dez. 2016.

BARBOZA, Hugo Leonardo; FERNEDA, Ariê Scherreier; SASS, Liz Beatriz. A garantia de autenticidade e autoria por meio de NFTs e sua (in)validade para a proteção de obras intelectuais. **Revista Internacional de Direito Digital**, Belo Horizonte, ano 2, n. 2, p. 99-117, maio/ago. 2021.

BASHIR, Imran. **Mastering blockchain**: distributed ledger technology, decentralization, and smart contracts explained. Birmingham: Packt, 2018.

BRASIL. **Código civil. Lei 10.406 de 20/11/2022**. Brasília, Diário Oficial da União, 2002.

BRASIL. **Constituição (1988). Constituição da República Federativa do Brasil. Brasília**, DF: Senado Federal: Centro Gráfico, 1988.

BUTERIN, Vitalik. **The Meaning of Decentralization**. [S.l.], 6 fev 2017. Medium: @VitalikButerin. Disponível em: https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274. Acesso em: 05 abr. 2024.

CHRISTIDIS, Konstantinos; DEVETSIKIOTIS, Michael. Blockchains and smart contracts for the internet of things. **IEEE Access**, [S.l], v. 4, p. 2292–2303, 2016.

DE FILIPPI, Primavera; WRIGHT, Aaron. **Blockchain and the Law**: The Rule of Code. Cambridge: Harvard University Press, 2018.

ETHEREUM.ORG. **Smart Contracts.** Disponível em: https://ethereum.org/en/developers/docs/smart-contracts/ Acesso em: 05 abr. 2024.

FALEIROS JÚNIOR, José Luiz de Moura; ROTH, Gabriela. Como a utilização do blockchain pode afetar institutos jurídicos tradicionais? **Atuação: Revista Jurídica do Ministério Público Catarinense**, Florianópolis, v. 14, n. 30, p. 29-59, jun./nov. 2019.

FARIAS, Cristiano Chaves de; ROSENVALD, Nelson. **Curso de Direito Civil: contratos**. Salvador, JusPODIVM, P. 68. 2017

FLORIANI, Lara Bonemer Rocha. **Smart contracts nos contratos empresariais**: um estudo sobre possibilidade e viabilidade econômica de sua utilização. Belo Horizonte: Editora Dialética, 2021.

GATTESCHI, Valentina et al. Blockchain and smart contracts for insurance: Is the technology mature enough? **Future Internet**, [S.l], v. 10, n. 2, p. 20, 2018.

GÓMEZ, Javier Domínguez. Criptografía: Función SHA-256. **Bit2Me**, [S.l], v. 1, 2018. Disponível em: https://academy.bit2me.com/wpcontent/uploads/2019/10/Criptography_SHA_256_es.pdf Acesso em: 05 abr. 2024.

MASCARENHAS, Juliana Z. G.; VIEIRA, Alex B.; ZIVIANI, Artur. Análise da rede de transações do ethereum. In: Sociedade Brasileira de Computação. **Anais do I Workshop em Blockchain: Teoria, Tecnologias e Aplicações**. [S.l.], 2018.

MENKVELD, Albert J. High-frequency trading and the new-market makers. **Tinbergen Institute**, Amsterdã, Paper n. 11-076/2/BSF21, 2011. Disponível em: http://hdl.handle.net/10419/86769. Acesso em: 05 abr. 2024.

NAKAMOTO, Satoshi. **Bitcoin**: A peer-to-peer electronic cash system. Decentralized Business Review, p. 21260, 2008. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 05 abr. 2024.

PEGORARO, Daniele Remoaldo. **Blockchain**. São Paulo: Senac, 2022.

PRADO, Jean. **O que é blockchain? [indo além do bitcoin]**. 2017. Accessed: November,2nd,2022. Disponível em: https://tecnoblog.net/responde/como-funciona-blockchain-bitcoinn

RHODES, Delton. **Cryptographic Hash Functions Explained: A Beginner's Guide**. 2018. Accessed: November, 2nd, 2022. Disponível em: https://komodoplatform.com/en/academy/cryptographic-hash-function/ Acesso em: 05 abr. 2024.

RIZZARDO, Arnaldo. **Contratos**. São Paulo: Gen, 2021. E-book.

SAVELYEV, Alexander. **Contract law 2.0: Smart Contracts as the beginning of the end of classic contract law**. Information & communications technology law, v. 26, n. 2, p. 116-134, 2017. Disponível em: https://www.tandfonline.com/doi/abs/10.1080/13600834.2017.1301036. Acesso em: 27 oct. 2022.

SILVEIRA, Renato de Mello Jorge; CAMARGO, Beatriz Corrêa. Ocultar o oculto: apontamentos sobre a lavagem de dinheiro em tempos de criptomoedas. **Revista Brasileira de Ciências Criminais**, São Paulo, v. 175, p. 145-187, jan. 2021.

SOLIDITY. 2022. **Bit2Me**, 8 set. 2022. Disponível em: https://academy.bit2me.com/pt/o-que-é-solidez-contratos-inteligentes-ethereum/ Acesso em: 05 abr. 2024.

SULTAN, Karim; RUHI, Umar; LAKHANI, Rubina. Conceptualizing Blockchains: Characteristics & Applications. **11th IADIS International Conference Information Systems**, p. 49-57, 2018. Disponível em https://arxiv.org/ftp/arxiv/papers/1806/1806.03693.pdf. Acesso em: 05 abr. 2024.

SWAN, Melanie. **Blockchain**: blueprint for a new economy. Sebastopol: O'Reilly Media, 2015.

SZABO, Nick. **The idea of smart contracts**. Nick Szabo's Papers and Concise Tutorials, 1997. Disponível em: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/index.html. Acesso em: 05 abr. 2024.

TAPSCOTT, Don; TAPSCOTT, Alex. **Blockchain revolution**. Nova York: Penguin, 2016.

UHDRE, Dayana de Carvalho. Tokenização, consumo de intangíveis e responsabilização das plataformas digitais: um novo (velho) problema? **Revista da Procuradoria-Geral do Estado do Paraná**, Curitiba, n. 14, p. 11-39, 2023.

WOOD, Gavin et al. Ethereum: A secure decentralised generalised transaction ledger. **Ethereum project yellow paper**, v. 151, n. 2014, p. 1–32, 2014.