



**Universidade de Brasília**  
**Faculdade de Direito**

**FELIPE MEE CAMPOS**

**CONTRATOS INTELIGENTES (*SMART CONTRACTS*):**  
**DESAFIOS E POTENCIALIDADES À LUZ DO DIREITO CIVIL BRASILEIRO**

**Brasília**  
**2025**

**Felipe Mee Campos**

**CONTRATOS INTELIGENTES (*SMART CONTRACTS*):  
DESAFIOS E POTENCIALIDADES À LUZ DO DIREITO CIVIL BRASILEIRO**

Trabalho de conclusão de curso apresentado 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**

#### CIP - Catalogação na Publicação

MC198c Mee Campos, Felipe.  
CONTRATOS INTELIGENTES (SMART CONTRACTS): DESAFIOS E  
POTENCIALIDADES À LUZ DO DIREITO CIVIL BRASILEIRO / Felipe  
Mee Campos;

Orientador: João Costa-Neto. Brasília, 2025.  
46 f.

Trabalho de Conclusão de Curso (Graduação - Direito)  
Universidade de Brasília, 2025.

1. Contratos inteligentes. 2. Direito Civil . 3. Smart  
Contracts. 4. Automatização contratual. 5. Legislação  
blockchain. I. Costa-Neto, João, orient. II. Título.

## **FOLHA DE APROVAÇÃO**

“Contratos Inteligentes (*Smart Contracts*): Desafios e Potencialidades à luz do Direito Civil Brasileiro” - monografia apresentada em 05/12/2025 à banca examinadora abaixo:

Prof. Dr. João Costa-Neto  
Orientador

Prof. MSc. José Humberto Pereira Muniz Filho  
Examinador

Prof. MSc. Rafael Papini Ribeiro  
Examinador

Aprovada em: **05/12/2025**

" Em virtude da modernização social, surge uma necessidade organizacional de tipo novo, que só pode ser satisfeita de modo construtivo."

(Jürgen Habermas. Direito e Democracia: entre Facticidade e Validade, v.1, 1929, p. 153 ).

## **AGRADECIMENTOS**

Agradeço a Deus, nosso grande arquiteto do universo, pela saúde, pela força e pela resiliência concedidas para superar os obstáculos ao longo desta trajetória. Sua presença constante foi a luz que me guiou em momentos de dúvida e de dificuldade, permitindo-me alcançar esta conquista com fé e gratidão.

Expresso minha profunda gratidão à minha esposa, Waleska Campos, pelo apoio incondicional, tanto emocional quanto estrutural, ao longo de toda a graduação. Sua presença, compreensão e suporte foram essenciais para que eu pudesse enfrentar os desafios acadêmicos e pessoais com determinação e equilíbrio.

Agradeço ao meu orientador Prof. Dr. João Costa-Neto, pela dedicação, paciência e valiosas contribuições intelectuais que foram fundamentais para o desenvolvimento desta pesquisa. Seu direcionamento acadêmico, com orientações precisas e incentivo constante, proporcionou a base necessária para a construção deste trabalho, guiando-me com sabedoria em cada etapa do processo.

Registro minha gratidão à Universidade de Brasília e a seus professores, pela formação acadêmica de excelência que me proporcionaram. A infraestrutura, o corpo docente qualificado e o ambiente de aprendizado da instituição foram fundamentais para meu crescimento intelectual e culminaram com a realização deste trabalho de conclusão de curso.

Por fim, aos meus amigos da Faculdade de Direito, meu sincero agradecimento pelo companheirismo, pelas discussões acadêmicas enriquecedoras, pelas revisões atentas e pelo apoio moral que me motivaram a persistir. Suas contribuições foram indispensáveis para o aprimoramento deste projeto e para tornar esta jornada mais leve e colaborativa.

## RESUMO

Este estudo investiga os contratos inteligentes (*smart contracts*) em uma perspectiva prática e teórica, à luz do Direito Civil brasileiro. O objetivo é analisar a compatibilidade dessa tecnologia com os institutos do Código Civil brasileiro, adotando uma metodologia de pesquisa bibliográfica e documental, com ênfase na análise de doutrina, da legislação e da jurisprudência. No decorrer do estudo, são apresentados criticamente os fundamentos técnicos, os desafios de aplicação e a insuficiência do marco legal vigente; são analisados o Projeto de Lei nº 954/2022 e a Lei nº 14.478/2022, bem como são propostas diretrizes legislativas concretas. A conclusão foi que a automatização contratual requer um sistema normativo específico, que incorpore critérios para validação, revisão, classificação de riscos e intervenção judicial, de modo a equilibrar inovação tecnológica e segurança jurídica.

**Palavras-chave:** Contratos inteligentes; Direito Civil brasileiro; Automatização contratual; Legislação *blockchain*.

## **ABSTRACT**

This study examines smart contracts from both practical and theoretical viewpoints under the framework of Brazilian Civil Law. Its primary goal is to assess the compatibility of this technology with the fundamental concepts of the Brazilian Civil Code. The methodology consists of bibliographic and documentary research, focusing on the analysis of legal doctrine, legislation, and judicial precedent. The study critically evaluates the technical underpinnings of smart contracts, their implementation challenges, and the shortcomings of the existing legal framework. Furthermore, it analyzes Law Propose nº 954/2022 and Law nº 14.478/2022, while also proposing concrete legislative guidelines. The study concludes that contractual automation necessitates a specific regulatory system that integrates criteria for validation, review, risk classification, and judicial oversight, thereby balancing technological innovation with legal security.

**Keywords:** Smart contracts; Brazilian Civil Law; Contractual automation; Blockchain legislation.



## LISTA DE ABREVIATURAS E SIGLAS

ANVISA	Agência Nacional de Vigilância Sanitária
API	<i>Application Programming Interface</i> (Interface de Programação de Aplicações)
BCB	Banco Central do Brasil
CC	Código Civil
CDC	Código de Defesa do Consumidor
CENAD	Central Notarial de Autenticação Digital
CNJ	Conselho Nacional de Justiça
DAO	<i>Decentralized Autonomous Organization</i> (Organização Autônoma Descentralizada)
DeFi	<i>Decentralized Finance</i> (Finanças Descentralizadas)
IA	Inteligência Artificial
ICP- Brasil	Infraestrutura de Chaves Públicas Brasileira
IoT	Internet of Things (Internet das Coisas)
KYC	<i>Know Your Customer</i>
LGPD	Lei Geral de Proteção de Dados
MAPA	Ministério da Agricultura, Pecuária e Abastecimento
MiCA	Markets in Crypto-Assets Regulation
MNE	Matrícula Notarial Eletrônica
PL	Projeto de Lei
PSAV	Prestadora de Serviços de Ativos Virtuais
STJ	Superior Tribunal de Justiça
TJSP	Tribunal de Justiça de São Paulo

## LISTA DE QUADROS

<b>Quadro 1</b> - Análise de Validade Jurídica. ....	20
<b>Quadro 2</b> - Controvérsia Doutrinária Central.....	24

## SUMÁRIO

1. INTRODUÇÃO.....	11
2. O CONTRATO INTELIGENTE E O DEBATE DOUTRINÁRIO SOBRE SUA NATUREZA JURÍDICA .....	14
2.1. Fundamentos técnicos: O que são <i>smart contracts</i> e a tecnologia <i>blockchain</i> ?.....	14
2.2. O contrato inteligente como negócio jurídico: Uma análise dos requisitos de validade.....	17
2.3. A controvérsia doutrinária: Compatibilidade versus insuficiência do Código Civil	21
3. A APLICAÇÃO DOS <i>SMART CONTRACTS</i> NA PRÁTICA: ANÁLISE JURISPRUDENCIAL E DESAFIOS CONCRETOS .....	25
3.1. Metodologia da pesquisa jurisprudencial .....	25
3.2. O diálogo dos tribunais com a tecnologia: Contratos eletrônicos e assinaturas digitais	26
3.3. A <i>blockchain</i> como meio de prova e os limites de sua imutabilidade.....	27
3.4. Padrões decisórios e a incipiência do debate sobre a autoexecutoriedade .....	30
4. UMA PROPOSTA DE REGULAMENTAÇÃO PARA OS <i>SMART CONTRACTS</i> NO BRASIL .....	32
4.1. Síntese diagnóstica: A insegurança jurídica como obstáculo à inovação.....	32
4.2. Análise das iniciativas legislativas: o marco das criptomoedas e o PL 954/2022....	33
4.3. Análise das iniciativas legislativas: o PL 954/2022 .....	34
4.4. Proposta <i>de lege ferenda</i> : diretrizes para uma legislação sobre <i>smart contracts</i> .....	35
5. CONCLUSÃO.....	39
REFERÊNCIAS .....	41

## 1. INTRODUÇÃO

A contínua transformação digital tem redefinido profundamente as interações sociais e as práticas econômicas, impulsionando a reconfiguração das relações comerciais em busca de maior eficiência, segurança e automação (Menezes; Araujo; Nishijima, 2023, p. 869–880 ). Isso gera, em consequência, novos instrumentos negociais e a necessidade de revisão das normas vigentes, quando não exige novas, visando assegurar as garantias das partes.

Nesse sentido, a trajetória evolutiva dos instrumentos negociais, que vem desde os primeiros registros em tablets cuneiformes na Mesopotâmia, passando pela sistematização do direito romano e pelas codificações modernas, chega à era digital enfrentando novos desafios de validade e de eficácia probatória (Divino, 2018, p. 2782; Giancaspro, 2017, p. 825–835).

Nesse contexto, os contratos inteligentes, *smart contracts*, emergem como o próximo passo lógico, pois representa a vanguarda da automação contratual e, por isso, exigem adaptação contínua da doutrina e da legislação para harmonizar os efeitos da inovação tecnológica com a segurança jurídica (Acre, 2025, p. 8; Silva; Coutinho, 2025, p. 2205–2211 ).

Entre as inovações disruptivas que emergem nesse contexto, os *smart contracts* figuram como uma das mais promissoras, por já estarem sendo amplamente utilizados, e cuja definição pode ser sumarizada como: protocolos de computador autoexecutáveis que utilizam a tecnologia *blockchain* para permitir a realização autônoma de acordos (Ferraz; Silva, 2019, p. 34-36; Gabardo; Dutra, 2024, p. 86-90 ).

O presente trabalho, portanto, debruça-se sobre a análise jurídica deste fenômeno, delimitando seu escopo de investigação à sua compatibilidade e aos desafios impostos sob a ótica do Direito Civil brasileiro.

A natureza tecnológica disruptiva dos *smart contracts*, fundamentada em características, como autoexecutoriedade e imutabilidade (Gobbo; Filho, 2022. p.22), suscita uma questão de pesquisa central: são estes novos instrumentos negociais compatíveis com os princípios e com os requisitos de validade do negócio jurídico, estabelecidos no Código Civil brasileiro? Daí, emerge outra questão: como o ordenamento jurídico nacional pode se adaptar para regulamentar essa nova realidade, de modo a garantir a segurança jurídica necessária às transações sem, contudo, sufocar o potencial de inovação tecnológica?

O objetivo geral deste estudo é analisar a compatibilidade dos contratos inteligentes

com o ordenamento jurídico civil brasileiro e, frente a eventuais lacunas, sugerir diretrizes para soluções que mantenham as garantias contratuais das partes.

Para alcançar tal propósito, foram elaborados os seguintes objetivos específicos, que correspondem a cada etapa do desenvolvimento: descrever os fundamentos conceituais e técnicos dos *smart contracts* e da tecnologia *blockchain*, examinando o debate doutrinário sobre sua natureza jurídica; investigar como a jurisprudência brasileira tem tratado tecnologias contratuais correlatas e identificar os desafios práticos de sua aplicação e, por fim, propor diretrizes para uma futura regulamentação no Brasil, a partir da análise de projetos de lei em tramitação.

A relevância do tema se manifesta em uma tripla dimensão, sendo categorizada da seguinte maneira: social/econômica, pela crescente adoção da tecnologia *blockchain* e dos *smart contracts* em setores vitais da economia brasileira, como o agronegócio e o mercado imobiliário, que buscam maior segurança e eficiência em suas transações; jurídica, porque essa expansão contrasta com a acentuada lacuna legislativa e com a incipiência do debate nos tribunais, gerando cenário de incerteza que afeta advogados, empresas e usuários; acadêmica, porque constitui uma oportunidade de contribuir para a construção de uma doutrina nacional sobre o tema, capaz de dialogar com a literatura existente e de propor soluções que visem à segurança jurídica e ao fomento de políticas públicas inovadoras.

Metodologicamente, o trabalho foi desenvolvido por meio de uma pesquisa bibliográfica e documental (Queiroz; Feferbaum, 2019, p. 51). Para tanto, respectivamente, fez-se uma abordagem analítica da doutrina nacional e estrangeira sobre Direito Civil, Direito Digital, *smart contracts* e *blockchain*, sendo consultadas publicações nacionais e internacionais sobre o tema; examinou-se a legislação pertinente, como o Código Civil (2002), o Marco Civil da Internet (2014) e a Lei nº 14.478/2022, o Marco Regulatório das Criptomoedas (2022b), além de projetos de lei em tramitação e da jurisprudência de tribunais superiores e estaduais sobre temas análogos.

O trabalho tem como arcabouço teórico o suporte dogmático do Direito Civil brasileiro, em especial da Teoria Geral dos Contratos e dos negócios jurídicos, como estrutura basilar para o enquadramento dos *smart contracts*. porém, insuficiente para lidar com suas especificidades. Tal cenário, análogo à insuficiência de modelos jurídicos tradicionais frente a novas dinâmicas, gera um vácuo normativo que cria insegurança jurídica e demanda uma regulamentação específica para harmonizar a tecnologia com os princípios contratuais vigentes.

O trabalho está estruturado em três capítulos. O primeiro capítulo dedica-se à

fundamentação teórica, definindo os *smart contracts* e explorando a controvérsia doutrinária sobre sua validade. O segundo volta-se à análise prática, mapeando o tratamento dado pelos tribunais a tecnologias afins e os desafios concretos. Por fim, o terceiro assume um caráter propositivo, onde se analisa as propostas legislativas em trâmite e se sugere um caminho para a regulamentação da matéria no Brasil.

## 2. O CONTRATO INTELIGENTE E O DEBATE DOUTRINÁRIO SOBRE SUA NATUREZA JURÍDICA

O presente capítulo visa descrever as bases conceituais e teóricas indispensáveis à análise jurídica dos *smart contracts*. De início, antes de discutir a aplicação da lei, é crucial compreender a tecnologia e como a doutrina jurídica tem se posicionado diante dela, firmando os pressupostos que são aplicados ao longo do estudo. Com isso, esta seção se dedica a apresentar a problemática teórica que fundamenta a pesquisa.

### 2.1. Fundamentos técnicos: O que são *smart contracts* e a tecnologia *blockchain*?

A origem do conceito de *smart contract* remonta à década de 90 (século XX), quando o jurista e cientista da computação Nick Szabo o idealizou como um protocolo de transação computadorizado que executa os termos de um contrato. Para ilustrar a ideia de autoexecutoriedade, Szabo utilizou a analogia de uma máquina de venda automática, que representa um contrato simples, no qual o cumprimento de uma condição (inserir a moeda) resulta na execução automática de uma obrigação (liberar o produto), eliminando a necessidade de um intermediário humano para garantir a performance do acordo (Cornelius, 2018; p.7-11; Gobbo; Filho, 2022, p. 27 ).

Essa concepção inicial de Szabo foi posteriormente materializada com o advento da plataforma Ethereum em 2015, que introduziu uma máquina virtual descentralizada, capaz de executar códigos arbitrários na *blockchain*, permitindo a criação de *smart contracts* mais complexos do que os simples scripts da *Bitcoin*. A linguagem de programação *Solidity* tornou-se o padrão para o desenvolvimento desses contratos, facilitando a implementação de lógicas condicionais avançadas, como *loops* e funções recursivas, embora com limitações, para evitar *loops* infinitos e garantir a determinabilidade da execução em um ambiente distribuído (Dykstra, 2023, p. 38 ; Walch, 2019, p. 39–68 ).

Tecnicamente, *smart contract* é um código de programação, ou seja, um *software*, com regras de negócio análogas às cláusulas contratuais e executado de forma automática, quando as condições predefinidas são atendidas (Santos; Pereira, 2022, p. 51). Essa operacionalidade é estruturada sob uma lógica condicional do tipo "se-então" (*if-then*), na qual a ocorrência de um evento específico ("se") dispara de maneira autônoma a consequência programada ("então") e confere ao acordo o caráter autoexecutável (De Filippi; Wright, 2018, p.6).

Além da lógica condicional básica, os *smart contracts* podem integrar mecanismos de governança descentralizada, como os *Decentralized Autonomous Organization* (DAOs), nos

quais as decisões são tomadas por votação tokenizada na *blockchain*, exemplificando como a tecnologia transcende o mero acordo bilateral para estruturas organizacionais autônomas. No contexto brasileiro, aplicações em DAOs têm sido exploradas em cooperativas agrícolas. Os produtores utilizam *smart contracts* para gerenciar distribuições de lucros baseadas em contribuições verificáveis, promovendo inclusão financeira em regiões rurais (Liu; Shang, 2022, p.8-10 ).

A tecnologia *blockchain* foi o catalisador que tornou os *smart contracts* viáveis em larga escala, por oferecer um ambiente operacional seguro para sua implementação (Ge, 2021, p.10). A *blockchain* pode ser definida como um sistema de registro distribuído que armazena informações de forma descentralizada, segura e imutável, funcionando como um livro-razão digital (Divino, 2018, p. 2775-2780; Menezes; Araujo; Nishijima, 2023, p. 873-880).

Suas principais características são: imutabilidade, assegurando que os dados não possam ser alterados retroativamente sem o consenso da rede; transparência, garantida pela verificação das transações por múltiplos participantes, e descentralização, que elimina a necessidade de uma autoridade central, tornando o sistema altamente confiável e resistente a fraudes (Divino, 2018, p. 2775-2780).

É importante distinguir entre *blockchains* que não exigem permissões, como *Ethereum*, na qual qualquer nó – computadores da rede *blockchain* que validam as transações – pode participar sem autorização prévia, daquelas que as exigem, a exemplo das *Hyperledger Fabric*. Essas exigem aprovação para entrada na rede, oferecendo maior controle e conformidade regulatória, o que pode ser mais adequado a aplicações sujeitas a normas de privacidade de dados pela Lei Geral de Proteção de Dados (LGPD). Essa distinção afeta a escalabilidade e os custos de transação, pois estas redes mais controladas reduzindo taxas e latências, mas potencialmente comprometendo a descentralização pura (Sharma; Jindal; Borah, 2024, p. 2480-2485).

Os *smart contracts*, como instrumentos jurídicos automatizados, são "hospedados" e executados diretamente na *blockchain*, uma estrutura descentralizada que armazena o código programado em linguagem específica, em endereços dedicados da rede, permitindo sua ativação automática mediante o cumprimento de condições preestabelecidas por meio de transações enviadas pelos envolvidos (Chevalier, 2021, p.571 - 576; Monteiro *et al.*, 2021, p.315 – 320).

Essa infraestrutura *blockchain* assegura a imutabilidade do código contratual após sua implementação, uma vez que as alterações demandariam o consenso de maioria dos nós da rede. Isso torna impossível modificações unilaterais e preserva a integridade do acordo original (Brito Moreira; Chaim, 2019, p, 24 - 25; Gabardo; Dutra, 2024, p. 86-90).



Ademais, a execução das obrigações é registrada de forma segura e verificável por todos os nós participantes, os quais as validam e replicam, conferindo transparência e auditabilidade, que são inerentes ao sistema *blockchain*, isto mitiga riscos de manipulação ou erro humano (De Filippi; Wright, 2018, p.6).

Como consequência, essa arquitetura elimina a necessidade de intermediários de confiança, tais como bancos, cartórios ou entidades reguladoras tradicionais, promovendo a autonomia das partes, redução de custos de intermediação e maior eficiência na concretização de obrigações contratuais, conforme destacado por Cárdenas e Molano (2022, p.7).

Para ilustrar o funcionamento prático dos *smart contracts*, considere o exemplo de um seguro de voo parametrizado na *blockchain*, no qual o contrato inteligente, ativado pela compra da apólice, monitora dados externos por meio de um oráculo – um mecanismo que consulta fontes confiáveis – como *Application Programming Interface* (API) de companhias aéreas. A indenização é liberada automaticamente para o segurado, caso o voo sofra atraso superior a determinado tempo, sem intervenção manual de ajustadores ou de burocracia. É garantido o pagamento instantâneo via transferência de criptoativos, e toda a transação é registrada de forma imutável na rede (Marriaga; Bonfante, 2023, p. 4).

Outro exemplo ilustrativo é o uso de *smart contracts* em cadeias de suprimentos, como no rastreamento de produtos agropecuários no Brasil, no qual protocolos, como o *AgriChain*, utilizam *blockchain* para registrar etapas desde a produção até a entrega; ativam pagamentos automáticos frente ao cumprimento de padrões de qualidade verificados por sensores da Internet das Coisas (IoT), reduzindo fraudes e melhorando a rastreabilidade em conformidade com normas da Agência de Vigilância Sanitária (ANVISA) e do Ministério da Agricultura, Pecuária e Abastecimento (MAPA). Esse modelo não apenas otimiza processos logísticos, mas também atende a demandas de sustentabilidade, registrando emissões de carbono de forma imutável para certificações ambientais (Bhat *et al.*, 2022, p. 20-22).

Em outro exemplo, de aluguéis residenciais, o *smart contract* pode ser programado para reter o pagamento até a confirmação do depósito via *blockchain*, momento em que libera digitalmente uma chave de acesso a uma fechadura inteligente conectada à IoT, permite a entrada do locatário e registra o evento para fins de auditoria. Com isso, evitam-se disputas sobre pagamentos ou sobre acessos indevidos e otimiza-se a gestão imobiliária (Ranchordás, 2019, p. 128; Silva; Aguiar, 2019, p. 17-20).

Esses exemplos de uso de *smart contracts* destacam a automação e a confiança distribuída proporcionadas pela tecnologia, com aplicações em setores, como seguros e logística (Marriaga; Bonfante, 2023, p. 7).

Compreendida a base tecnológica que confere aos *smart contracts* suas características de automação e de imutabilidade, bem como exemplos de sua aplicação na prática, a análise deve agora se voltar para o campo do Direito, a fim de verificar se esse artefato computacional pode ser enquadrado como negócio jurídico válido, frente aos normativos do ordenamento brasileiro. A transição do plano técnico para o jurídico é fundamental para avaliar a compatibilidade do instrumento com as normas vigentes e identificar os pontos de tensão que demandam atenção do legislador e do intérprete.

## 2.2. O contrato inteligente como negócio jurídico: uma análise dos requisitos de validade

No âmbito do ordenamento jurídico brasileiro, a validade de qualquer negócio jurídico, incluindo os inovadores contratos inteligentes (*smart contracts*), deve ser escrutinada à luz da Teoria Geral do Negócio Jurídico, como delineado no art. 104 do Código Civil (CC) de 2002.

Esse dispositivo, inalterado em sua essência desde sua promulgação (Lei nº 10.406/2002), estabelece os seguintes requisitos essenciais para validade do ato negocial: em primeiro lugar, a capacidade do agente, que pressupõe a aptidão legal para exercer direitos e para contrair obrigações sem vícios, como menoridade absoluta ou incapacidade mental; em segundo, o objeto lícito, possível, determinado ou determinável, significando que não pode contrariar a lei, a moral ou os bons costumes. Deve ser factível no mundo real e suficientemente preciso para evitar ambiguidades interpretativas; por fim, a forma prescrita ou não defesa em lei, que admite a liberdade formal para a maioria dos contratos, salvo aqueles que exigem solenidades específicas, como a escritura pública para imóveis.

Esses requisitos normativos, inspirados na tradição pandectista e adaptada ao contexto brasileiro, impõem desafios peculiares à validade dos *smart contracts*, nos quais a manifestação de vontade do assinante se materializa, como visto, por meio de códigos computacionais autoexecutáveis (Menteshashvili, 2021, p. 213–216 ; Millard, 2018, p. 843–846). Logo, esses requisitos de validade em relação aos *smart contracts* demandam uma análise criteriosa para garantir sua integração harmônica ao sistema civilista.

Quanto à **capacidade do agente**, os *smart contracts* enfrentam desafios significativos no ambiente pseudoanônimo da *blockchain*, no qual a identidade das partes é geralmente mascarada por chaves criptográficas e por *wallets* (endereço de carteiras criptografadas), dificultando a verificação de requisitos como maioridade ou ausência de interdição. Isso pode levar à nulidade absoluta nos termos do art. 166, I do CC (Gabardo; Dutra, 2024, p. 86-90)

A verificação de identidade ocorre tipicamente por meio de protocolos *Know Your Customer* (KYC), integrados a plataformas de criptoativos. Tais protocolos exigem documentos

oficiais como CPF ou RG para confirmar a capacidade legal, alinhando-se a regulamentações contra lavagem de dinheiro e contra financiamento ao terrorismo. As chaves criptográficas e assinaturas digitais atuam como vinculadores, gerando provas de autoria inegáveis via algoritmos. Porém, sem KYC prévio, um menor poderia executar uma transação irrevogável, gerando disputas judiciais sobre restituição de valores (art. 157, CC). Para superar essa vulnerabilidade, Hannan *et al.* (2023, p. 2095–2109) sugerem a obrigatoriedade de integrações KYC com verificações biométricas ou IA para plataformas *blockchain* no Brasil, garantindo capacidade prévia e evitando nulidades.

No que concerne ao **objeto**, a tecnologia dos *smart contracts* é intrinsecamente neutra, servindo tanto para fins lícitos, quanto para ilícitos. Assim, exige escrutínio para atender os critérios de liceidade, de possibilidade e de determinabilidade, sob pena de ser considerado nulo (art. 166, II, CC). Por exemplo: um *smart contract* para automatizar pagamentos em uma transação de compra e venda de bens lícitos, como criptoativos regulados, é válido, ao promover eficiência e transparência (CC, 2002).

Em outra perspectiva, um *smart contract* destinado a gerenciar esquemas de pirâmide financeira, como os casos de *Forsage* em 2022 – pirâmide financeira estruturada em *smart contracts* na *blockchain Ethereum* – é exemplo de uso indevido dessa tecnologia. O esquema demonstrou que, apesar da aparente transparência do código e do caráter imutável das transações, a lógica do contrato foi desenhada para privilegiar os organizadores e participantes iniciais, concentrando os ganhos no topo da rede. A análise do caso *Forsage* ressalta que a transparência técnica do *blockchain*, por si só, não impede fraudes; pode, paradoxalmente, ser utilizada como retórica para atrair vítimas em contextos de baixa literacia digital e financeira (Kell *et al.*, 2024, p. 241–258).

Essa dualidade, no entanto, pode ser mitigada por meio de auditorias independentes pré-lançamento e integração com oráculos regulados para validar liceidade. A propósito, propõe-se, no Capítulo 3, uma lei que classifique *smart contracts* por risco, com proibições automáticas para objetos suspeitos detectados por IA, e assim, fomentando usos legítimos sem coibir a inovação.

A **forma**, regida pelo princípio da liberdade referido no art. 107 do CC, permite que os *smart contracts* sejam reconhecidos como válidos na modalidade de código computacional. É que a lei não impõe solenidades específicas para a maioria dos atos negociais, bastando que a manifestação de vontade seja comprovável. Essa validade é reforçada pela Medida Provisória (MP) nº 2.200-2/2001 (MP, 2001), que instituiu a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). Essa estrutura equipara as assinaturas digitais qualificadas a instrumentos

públicos com presunção de veracidade, permitindo que transações em *blockchain* sejam juridicamente seguras, ao vincularem chaves privadas a identidades certificadas. Contudo, em contratos solenes, pode haver conflito entre a imutabilidade e os requisitos de publicidade, sugerindo hibridização com registros notariais digitais. Uma proposta de lei poderia atualizar a MP para incluir *smart contracts* explicitamente, com padrões mínimos de forma para maior acessibilidade e redução de litígios (Rebouças; Villas Bôas, 2012, p. 57).

No Direito Civil brasileiro, a **manifestação da vontade** é o elemento essencial do negócio jurídico (art. 104, II, do CC), devendo ela ser livre, consciente e conforme a ordem jurídica. Essa manifestação, entretanto, não é entendida apenas em seu aspecto literal, mas também interpretada segundo princípios, como o da boa-fé, o da função social e o da preservação do negócio. Enquanto no Direito Civil a vontade pode ser analisada em seu contexto e corrigida em caso de vícios ou abusos, nos *smart contracts*, a execução cega do CC tende a substituir a análise da vontade real pela lógica imutável da programação (CC, 2002).

A expressão “tirania do código”, aplicada aos *smart contracts*, refere-se à rigidez e à autoexecutabilidade desses instrumentos: uma vez programados e lançados na *blockchain*, eles tendem a ser executados de forma automática, sem espaço para flexibilização, para revisão ou para interpretação posterior. Diferentemente dos contratos tradicionais, que podem ser modulados pela hermenêutica jurídica, pela boa-fé objetiva ou mesmo pela intervenção do Judiciário, em casos de abuso ou nulidade, os *smart contracts* executam estritamente as instruções codificadas, o que pode gerar resultados injustos ou descolados da real intenção das partes. Nessa ótica, a “tirania” decorre do predomínio do código computacional sobre a autonomia privada, o qual impõe a lógica técnica em detrimento da adaptação social e jurídica (Cabral; Silva, 2022, p. 10 - 12; Lei no 10.406, de 10 de janeiro de 2002.).

Para mitigar essa problemática nos *smart contracts*, um projeto de lei poderia assegurar que a rigidez algorítmica não suprimisse o elemento volitivo essencial ao negócio jurídico. Para tanto, seria necessário: exigir que esses contratos fossem acompanhados de uma versão em linguagem clara, garantindo consentimento informado das partes; prever que, em caso de divergência entre execução automática e intenção real dos contratantes, prevalecesse a interpretação segundo a boa-fé e a função social do contrato; criar mecanismos de contestação e de revisão judicial/arbitral sempre que houvesse vícios de consentimento, mesmo após a execução. Além disso, a legislação poderia impor a obrigatoriedade de cláusulas de flexibilidade técnica, como dispositivos de suspensão ou de reversão, e atribuir, às plataformas e programadores, o dever de informar de modo compreensível os efeitos do código.

O debate em torno dessas questões não é exclusivo do Brasil: na União Europeia, o

*Markets in Crypto-Assets Regulation* (MiCA) já prevê requisitos de transparência e de proteção ao consumidor, buscando compatibilizar a automação com a autonomia da vontade. Dessa forma, a lei preservaria a manifestação da vontade como núcleo do contrato, evitando que a automatização tecnológica transformasse a autonomia privada em submissão ao algoritmo (Wronka, 2024, p. 84-93 ).

O Quadro 1 sistematiza a presente análise, confrontando os requisitos de validade do negócio jurídico com os desafios tecnológicos apresentados pelos contratos inteligentes.

**Quadro 1 - Análise de Validade Jurídica**

Requisito Legal (Art. 104, CC)	Desafio Tecnológico do Contrato Inteligente	Solução/Mitigação
I. Agente Capaz	O ambiente pseudoanônimo da <i>blockchain</i> (chaves criptográficas e <i>wallets</i> ) dificulta a verificação da capacidade jurídica (idade, sanidade mental) das partes.	Integração de protocolos de verificação de identidade ( <i>Know Your Customer</i> - KYC) que vinculam uma identidade real a um endereço digital.
II. Objeto Lícito, Possível, Determinado ou Determinável	A tecnologia é neutra e pode ser usada para fins ilícitos. A autoexecução pode concretizar um ato ilegal (ex: pirâmide financeira <i>Forsage</i> ) antes de qualquer intervenção.	Auditorias de código pré-implementação e o uso de oráculos regulados para validar a liceidade do objeto. Propostas de monitoramento por IA para detectar e proibir objetos ilícitos.
III. Forma Prescrita ou não Defesa em Lei	A forma do contrato é o próprio código computacional, uma modalidade não tradicional.	Ponto de Compatibilidade: O princípio da liberdade das formas (Art. 107, CC) e a legislação sobre documentos eletrônicos (MP nº 2.200-2/2001) dão validade à forma digital.
Elemento Transversal: Manifestação da Vontade	A "Tiranía do Código": a execução rígida e automatizada pode não corresponder à real intenção das partes, especialmente em caso de <i>bugs</i> ou mudanças de circunstâncias, desafiando o núcleo do consentimento.	Propostas legislativas que exigem sumários em linguagem natural e a incorporação de mecanismos de intervenção para garantir que a vontade prevaleça sobre a execução cega do código.

Fonte: Elaborado pelo pesquisador

A análise dos requisitos de validade, embora aponte uma compatibilidade formal dos *smart contracts* com a Teoria do Negócio Jurídico, expõe tensões substanciais, sobretudo no que se refere à garantia de um consentimento informado e à rigidez de sua execução automatizada. São precisamente esses desafios que alimentam uma grande controvérsia doutrinária sobre a suficiência do CC para regular a matéria, dividindo as opiniões sobre a real natureza e os limites desses novos instrumentos tecnológicos.

### 2.3. A controvérsia doutrinária: Compatibilidade versus insuficiência do Código Civil

Como verifica-se na seção anterior, a doutrina sobre o assunto apresenta um debate acirrado sobre a natureza jurídica dos *smart contracts*, dividindo-se entre autores que os classificam como verdadeiros contratos, capazes de gerar obrigações autônomas e vinculantes, e autores que os veem meramente como instrumentos técnicos para a execução automática de obrigações preexistentes, sem a essência negocial tradicional.

A corrente da compatibilidade, defendida por Luciano (2018, p. 911-913), postula a plena absorção dos *smart contracts* pelo Direito Positivo brasileiro, sustentando que a Teoria Geral dos Contratos, delineada no CC de 2002, revela-se flexível o suficiente para englobar tais instrumentos tecnológicos sem demandar alterações normativas substanciais. Isso, porque eles representam mera evolução na formalização e na execução de obrigações já previstas no ordenamento.

Os argumentos centrais recaem no princípio da autonomia privada, que confere, às partes, ampla discricionariedade na configuração de seus interesses jurídicos: a liberdade de contratar, positivada no art. 421 do CC, que preserva a pactuação voluntária contra intervenções estatais desproporcionais, e a validade da forma eletrônica, assegurada pela referida MP nº 2.200-2/2001 e pela Lei nº 14.063/2020, que dispõem sobre a equiparação dos códigos programados a documentos tradicionais para fins probatórios e executórios.

Nessa visão, o *smart contract* não constitui inovação disruptiva, mas sim, uma nova modalidade de concretização automatizada do que já era juridicamente possível, modalidade essa que otimiza a eficiência transacional e que preserva a essência consensual do contrato como manifestação de vontade.

Da mesma maneira, outros defensores dessa ideia, como Cárdenas e Molano (2022, p. 7), argumentam que os *smart contracts* constituem negócios jurídicos plenos, materializadores da autonomia da vontade por meio de códigos autoexecutáveis que atendem aos elementos de validade do art. 104 do CC, promovendo eficiência e segurança em transações.

Essa corrente sustenta ainda que a Teoria Geral dos Contratos é suficientemente flexível para acomodar esses instrumentos tecnológicos, sem necessidade de reformas legislativas significativas. Assim, os *smart contracts* não representam uma ruptura jurídica, mas apenas uma nova forma de executar obrigações contratuais já previstas com eficiência, por meio da automação, sem alterar a essência do acordo de vontades.

Aprofundando essa perspectiva, a corrente da compatibilidade defende ainda que os princípios basilares do Direito Contratual brasileiro, como boa-fé objetiva (art. 422 do CC) e

função social do contrato (art. 421 do CC), são plenamente aplicáveis e servem de ferramentas hermenêuticas para interpretar e, se necessário, corrigir os efeitos de um *smart contract*. Sob essa ótica, mesmo um contrato automatizado está sujeito ao controle de legalidade e aos deveres anexos de lealdade, de informação e de cooperação, não suplantando a teoria geral dos contratos, mas sim, submetendo-se a ela (Cardoso; Marino, 2022, p. 206; Lei no 10.406/2002)

Se, por um lado, a boa-fé objetiva impõe deveres de lealdade, de transparência e de cooperação, permitindo que o julgador analise o código programado para mitigar interpretações que gerem desequilíbrio ou injustiça – como a execução automática de cláusulas abusivas –, por outro lado, a função social do contrato subordina a autonomia privada ao interesse coletivo, possibilitando a revisão judicial de resultados automatizados que violem normas de ordem pública ou comprometa o equilíbrio socioeconômico (Marriaga; Bonfante, 2023, p.5).

Assim, mesmo automatizados, os *smart contracts* devem permanecer sujeitos ao controle de legalidade e aos deveres contratuais, de modo a garantir que a tecnologia da *blockchain* respeite os fundamentos éticos e jurídicos do sistema contratual brasileiro.

Em contrapartida, críticos, como Divino (2018, p. 2794), destacam as limitações desses tipos de contratos, afirmando que se trata de ferramentas programáticas dependentes de acordos prévios; que não há flexibilidade para incorporar elementos humanos, como boa-fé ou revisão; que são apenas mecanismos de automação sem status contratual independente. É uma visão doutrinária oposta que aponta profundas incompatibilidades entre a tecnologia e a dogmática civilista.

O principal argumento dessa corrente é que a autoexecutoriedade e a imutabilidade da *blockchain* colidem frontalmente com institutos fundamentais do Direito Civil, como a possibilidade de revisão contratual por onerosidade excessiva (arts. 478-480 do CC) ou a anulação de um negócio por vício de consentimento. Gera-se, então, o questionamento central sobre como "desfazer" ou como revisar uma transação já executada e registrada de forma imutável em uma rede descentralizada (Gomes; Matias, 2022, p. 46. Lei no 10.406/ 2002).

Detalhando esses desafios, a questão da responsabilidade por erros de código (*bugs*) é uma das mais complexas: se uma falha na programação levar a um resultado injusto, sobre quem recai a responsabilidade? Ao programador, às partes que aderiram ao código ou à plataforma? De acordo com análises doutrinárias, a responsabilidade pode ser atribuída ao desenvolvedor por falhas na codificação, especialmente se houver negligência na verificação de vulnerabilidades; é o caso de *hacks* em plataformas descentralizadas. No entanto, as partes contratantes também assumem riscos ao aceitar o código "*as is*", enquanto as plataformas de *blockchain* podem ser responsabilizadas por fornecer infraestrutura defeituosa, conforme

princípios de responsabilidade civil objetiva (arts. 186 e 927 do CC). Essa “distribuição” de responsabilidade exige definições claras de deveres, como auditorias prévias obrigatórias para mitigar *bugs*, evitando-se a aplicação estrita da Teoria do Risco Integral, que poderia sobrecarregar inovadores (CC, 2002; Dykstra; Moraes; Moraes, 2023, p. 41-42).

Ademais, a impossibilidade de revisão contratual se torna evidente diante de eventos supervenientes, pois um código que se executa automaticamente é, por natureza, insensível a alterações fáticas. Isso torna a aplicação da Teoria da Imprevisão um obstáculo quase intransponível. No Direito brasileiro, essa teoria (art. 478 do CC) permite a revisão ou a resolução de contratos por onerosidade excessiva, decorrente de eventos imprevisíveis. Porém, a imutabilidade da *blockchain* impede adaptações dinâmicas, como ajustes por força maior ou por mudanças econômicas. As soluções propostas incluem a incorporação de oráculos externos<sup>1</sup> para *inputs* variáveis ou cláusulas de *escape hatches*<sup>2</sup>, que permitam pausas condicionadas, integrando flexibilidade sem comprometer a automação (CC, 2002; Dykstra; Moraes; Moraes, 2023, p. 41-42).

Com isso, a própria intervenção judicial é posta em xeque, quando se questiona como um magistrado poderia ordenar a suspensão ou alteração de um contrato que opera de forma descentralizada e autônoma? A descentralização da *blockchain* dificulta a execução de decisões judiciais, pois não há uma autoridade central para interromper transações. No contexto brasileiro, tribunais podem recorrer a indenizações ou a bloqueios de *wallets*, mas enfrentam barreiras técnicas, como a necessidade de *hard forks*<sup>3</sup> (alteração no protocolo de uma *blockchain* com as versões anteriores) para reversões coletivas. Tal recurso demanda expertise judicial em tecnologia e legislação específica para habilitar intervenções híbridas, de modo a

---

<sup>1</sup> Na lógica dos smart contracts, os oráculos funcionam como “pontes” entre a *blockchain* (que só reconhece dados internos à rede) e o mundo externo (off-chain). Eles fornecem informações externas confiáveis — como índices econômicos, taxas de câmbio, indicadores climáticos ou eventos jurídicos — que podem ser usados para condicionar a execução contratual. Assim, em um cenário de aplicação da Teoria da Imprevisão, oráculos externos permitiriam que o contrato reconhecesse alterações imprevisíveis de contexto, como uma hiperinflação ou um desastre natural, e ajustasse automaticamente suas cláusulas. Em outras palavras, são mecanismos técnicos para introduzir variáveis dinâmicas no contrato, evitando que a rigidez da *blockchain* impeça a adaptação às circunstâncias

<sup>2</sup> *Escape hatches* são comandos internos no próprio código que permitem interromper, pausar ou mesmo reverter a execução automática do contrato em situações excepcionais. Funcionam como válvula de segurança, acionada manualmente por uma parte, por ambas, ou por uma autoridade designada (como um árbitro ou tribunal). Ao prever *escape hatches*, o contrato inteligente mantém sua automação, mas com margens de flexibilidade, permitindo que eventos extraordinários sejam tratados sem necessidade de criar um contrato. No contexto jurídico, equivalem a cláusulas que permitem adaptação por força maior, caso fortuito ou onerosidade excessiva.

<sup>3</sup> *Hard fork* é uma alteração estrutural em uma *blockchain* que modifica de maneira incompatível as regras de validação de blocos e transações, de modo que os nós que adotam a nova versão do protocolo deixam de reconhecer como válidas as transações da versão antiga, e vice-versa. Em termos práticos, o *hard fork* cria uma divisão permanente na rede: uma parte dos usuários e mineradores pode permanecer na cadeia original, enquanto outra passa a seguir a nova versão, resultando na coexistência de duas *blockchains* independentes a partir de um mesmo histórico até o ponto de bifurcação.



equilibrar soberania judicial com inovação (Efing; Santos, 2018, p. 57-60).

Embora a corrente que reconhece os *smart contracts* como contratos verdadeiros acerte, quando enfatiza sua compatibilidade com o ordenamento jurídico, evitando um vácuo regulatório e promovendo a inovação, a corrente que os considera meros instrumentos destaca limitações incontornáveis de ordem prática, como a rigidez tecnológica que conflita com a flexibilidade civilista.

O Quadro 2 resume, comparativamente, o debate acadêmico sobre o tema, destacando uma síntese dos argumentos das duas principais correntes de pensamento sobre a natureza jurídica dos *smart contract*.

**Quadro 2 - Controvérsia Doutrinária Central**

<b>Critério de Análise</b>	<b>Corrente da Compatibilidade</b>	<b>Corrente da Insuficiência</b>
<b>Tese Central</b>	O Código Civil é flexível o suficiente para absorver os <i>smart contracts</i> como uma nova forma de execução contratual.	A rigidez, imutabilidade e autoexecutoriedade são incompatíveis com institutos essenciais do Direito Civil.
<b>Fundamentos Jurídicos</b>	Autonomia Privada, Liberdade de Contratar (art. 421, CC), Liberdade das Formas (art. 107, CC), Boa-Fé Objetiva (art. 422, CC).	Revisão Contratual (Teoria da Imprevisão, arts. 478-480, CC), Anulação por Vício de Consentimento, Função Social do Contrato.
<b>Visão da Tecnologia</b>	O <i>smart contract</i> é uma ferramenta para executar um acordo jurídico tradicional de forma mais eficiente.	O código se torna a própria lei do contrato ("Tiranía do Código"), suplantando a interpretação e os remédios jurídicos.
<b>Papel do Judiciário</b>	Os tribunais podem e devem intervir para interpretar o código e corrigir resultados injustos com base em princípios gerais do Direito.	A intervenção judicial é tecnicamente difícil ou impossível. Como um juiz pode alterar um registro imutável e descentralizado?
<b>Desafios Práticos</b>	Foco na adaptação dos princípios existentes.	Responsabilidade por <i>bugs</i> no código, impossibilidade de revisão por eventos supervenientes, dificuldade de reverter transações.

Fonte: Elaborado pelo pesquisador

Essa dicotomia revela que a aplicação analógica do CC de 2002 representa uma solução paliativa, insuficiente para abarcar peculiaridades dos *smart contracts*, como autoexecutoriedade e imutabilidade. A abordagem do tema demanda uma evolução hermenêutica e legislativa que integre mecanismos específicos para harmonizar a dogmática tradicional com a disrupção digital, conforme será aprofundado nos capítulos subsequentes sobre desafios práticos e propostas regulatórias.

### 3. A APLICAÇÃO DOS *SMART CONTRACTS* NA PRÁTICA: ANÁLISE JURISPRUDENCIAL E DESAFIOS CONCRETOS

Superado o debate teórico, este capítulo passa para uma análise prática, investigando como os *smart contracts* são aplicados e interpretados no cenário jurídico concreto. Dada a incipiência de uma jurisprudência consolidada especificamente sobre esses contratos no Brasil, a análise se voltará para o tratamento que os tribunais têm conferido a tecnologias análogas, como contratos eletrônicos e uso da *blockchain* como meio de prova. Este exame permitirá mapear as tendências decisórias e identificar os desafios práticos que a autoexecutoriedade e a imutabilidade impõem ao Poder Judiciário.

#### 3.1. Metodologia da pesquisa jurisprudencial

Para a realização da pesquisa jurisprudencial, foram adotados critérios metodológicos precisos e sistemáticos, visando capturar decisões judiciais relevantes sobre temas análogos aos *smart contracts*, como contratos eletrônicos e tecnologias digitais, dado o ainda incipiente tratamento direto do tema nos tribunais brasileiros.

No que concerne aos tribunais, o foco principal foi o Superior Tribunal de Justiça (STJ), em razão de sua competência constitucional para uniformizar a interpretação da lei federal (art. 105, III, CF/1988), especialmente em matéria de Direito Civil envolvendo validade contratual e provas digitais. Em complemento, vieram tribunais estaduais com alto volume de casos empresariais, como o Tribunal de Justiça de São Paulo (TJSP), que lida frequentemente com litígios envolvendo comércio eletrônico, *fintechs* e criptoativos, refletindo a concentração econômica da região.

Quanto ao período, fez-se um recorte dos últimos 10 anos (2015 a 2025), a fim de abarcar decisões mais recentes que incorporam avanços tecnológicos pós-Lei nº 12.965/2014 e Lei nº 14.063/2020 (assinaturas eletrônicas), capturando evoluções jurisprudenciais em um contexto de crescente digitalização (Marco Civil da Internet, 2014; Lei nº 14.063/2020).

As palavras-chave empregadas nas buscas em bases como o Sistema de Automação da Justiça (SAJ) do TJSP, o portal de jurisprudência do STJ e plataformas como Jusbrasil incluíram os termos: "contrato eletrônico", "assinatura digital", "validade negócio jurídico eletrônico", "*blockchain* como prova", "criptoativos", "transação digital autoexecutável", "prova eletrônica em contrato" e "vício de consentimento digital", combinados com operadores booleanos (e.g., "contrato eletrônico" e "validade") para refinar os resultados e identificar analogias aplicáveis aos *smart contracts*.

A análise dos dados jurisprudenciais transcende a mera transcrição de ementas ou acórdãos, concentrando-se na identificação da *ratio decidendi* de cada julgado, ou seja, nos fundamentos jurídicos essenciais que embasam a decisão e que podem ser extrapolados para casos semelhantes, conforme metodologia qualitativa inspirada em autores como Dworkin (1999, p. 55 ) sobre integridade interpretativa.

Os casos selecionados foram agrupados tematicamente em categorias – "validade da manifestação de vontade digital", "prova e exequibilidade eletrônica" ou "responsabilidade em transações automatizadas" — para detectar: padrões (e.g., tendência à validação de contratos eletrônicos com base na boa-fé); tendências evolutivas (e.g., crescente aceitação de *blockchain* como meio de prova pós-2020) ou contradições (e.g., divergências entre instâncias sobre anonimato e capacidade), de modo a permitir uma síntese crítica que contribua para a hipótese do trabalho sobre a necessidade de adaptações legislativas.

### **3.2. O diálogo dos tribunais com a tecnologia: Contratos eletrônicos e assinaturas digitais**

A análise da jurisprudência pátria revela uma progressiva e já consolidada aceitação dos contratos eletrônicos, com o STJ pacificando o entendimento de que a forma eletrônica, por si só, não invalida o negócio jurídico. Essa postura, alinhada ao princípio da liberdade das formas, demonstra que o Judiciário superou a desconfiança inicial com o meio digital, estabelecendo diretrizes para a eficácia, eficiência comercial e confiabilidade desses negócios jurídicos online (Menezes; Dias, 2023, p. 102-105).

Esse entendimento pacificou-se ao longo dos últimos anos, como evidenciado em julgados que enfatizam a autenticidade e a integridade conferidas por tecnologias que dispensam formalismos excessivos, promovendo eficiência no ambiente virtual sem comprometer a segurança jurídica.

Um julgado paradigmático que ilustra essa tendência é o REsp. 1.495.920/DF (2014/0295300-9), Rel. Min. Paulo de Tarso Sanseverino, 3ª Turma, julgado em 15 de maio de 2018, no qual a controvérsia central residia em definir se um contrato eletrônico de mútuo, assinado digitalmente, mas sem a presença das duas testemunhas exigidas pelo Código de Processo Civil, possuiria força de título executivo extrajudicial (STJ, 2018b)

Na decisão, essa Corte defendeu a executividade do documento, em uma importante exceção à regra formal em vigor, que não previa a validade da assinatura. A *ratio decidendi* do acórdão foi a de que a assinatura digital, quando certificada por autoridade confiável, dentro da ICP-Brasil, confere autenticidade e integridade ao documento. Com isso, cumpre a mesma

tarefa de verificação exercida por testemunhas, garantindo a força executiva do título.

Transportando essa lógica para o universo dos *smart contracts*, pode-se argumentar que a assinatura de uma transação, via chave criptográfica na *blockchain*, cumpre uma função análoga, garantindo autoria e integridade ao registro de forma ainda mais robusta, o que reforça a tese de sua validade e eficácia.

A discussão sobre a validade da manifestação de vontade eletrônica se expande para além do padrão ICP-Brasil, abrangendo outras formas de consentimento digital. A jurisprudência do STJ tem evoluído no sentido de validar assinaturas eletrônicas certificadas por entidades privadas não credenciadas na ICP-Brasil, desde que as partes admitam o método como válido e que a autenticidade e a integridade do documento possam ser verificadas.

Em decisões recentes, como os REsp nº 2.150.278/ PR (2024/0212892-1), (STJ, 2024a), e o REsp nº 2.159.442/PR (2024/0267355-0), ambos julgados em 24 de setembro de 2024 (STJ, 2024b), Rel. Min. Nancy Andrighi, 3ª Turma, a Corte tem afastado o "formalismo excessivo", valorizando a intenção das partes e a existência de um acordo, independentemente da tecnologia empregada. Isso inclui aceite por e-mail, confirmação via aplicativos de mensagens ou clique em botão "aceito" em um site. Afirmou a Ministra:

Negar validade jurídica a um título de crédito, emitido e assinado de forma eletrônica, simplesmente pelo fato de a autenticação da assinatura e da integridade documental ter sido feita por uma entidade sem credenciamento no sistema ICP-Brasil seria o mesmo que negar validade jurídica a um cheque emitido pelo portador e cuja firma não foi reconhecida em cartório por autenticidade, evidenciando um excessivo formalismo diante da nova realidade do mundo virtual (STJ, 2024b).

Essa tendência do Tribunal Superior em focar na substância do acordo, que reflete a manifestação da vontade entre as partes, em detrimento do formalismo tecnológico, é um indicador positivo para a futura aceitação pelo judiciário, de formas não típicas de celebração de contratos, como é o caso dos *smart contracts* (Menezes; Dias, 2023, p. 109 ).

### **3.3. A *blockchain* como meio de prova e os limites de sua imutabilidade**

O Provimento nº 100/2020, editado pelo Conselho Nacional de Justiça (CNJ) (CNJ, 2020b), representa um marco na modernização dos serviços notariais brasileiros, ao regulamentar a prática de atos notariais eletrônicos por meio do sistema e-Notariado. A norma estabelece diretrizes para a realização de escrituras, de procurações, de autenticações e de outros atos em ambiente digital, garantindo segurança jurídica, autenticidade e fé pública aos documentos produzidos remotamente.

Entre os principais avanços trazidos pelo provimento, destacam-se a obrigatoriedade da

videoconferência notarial para captação da manifestação de vontade das partes e o uso de assinaturas digitais vinculadas à ICP-Brasil. O sistema e-Notariado oferece funcionalidades como a Matrícula Notarial Eletrônica (MNE), que assegura a rastreabilidade dos atos, e a Central Notarial de Autenticação Digital (CENAD), responsável pela validação de documentos digitalizados.

A tecnologia *blockchain* transcendeu o universo das criptomoedas e tem sido progressivamente introduzida no contexto probatório do Direito brasileiro. Sua arquitetura tem sido utilizada para a criação de provas digitais robustas, especialmente por meio de plataformas que registram os documentos e seu conteúdo em um determinado momento, uma funcionalidade conhecida como *timestamping*<sup>4</sup>. Esse carimbo de tempo digital, registrado de forma imutável na cadeia de blocos, oferece uma prova de anterioridade com validade jurídica, sendo uma ferramenta reconhecida legalmente no Brasil para comprovar a data e a hora de uma transação ou registro (Hepp *et al.*, 2018, p. 273-281).

O fato acima é referendado em diversos julgados, a exemplo do acórdão nos autos de Apelação Cível nº 1001795-79.2024.8.26.0035/SP, julgada em 30 de julho de 2025, de relatoria da Desembargadora Léa Duarte (TJSP, 2025). A apelante, aposentada, alegou descontos indevidos em seu benefício previdenciário, a título de contribuição associativa sem autorização ou filiação prévia, e requereu a declaração de inexistência de relação jurídica, a cessação dos descontos, a restituição em dobro dos valores debitados e uma indenização moral. A sentença de primeira instância julgou improcedente o pedido com base em contrato eletrônico apresentado pela ré, e a apelação visou reformá-la, impugnando a validade do documento por ausência de autenticação segura, nos termos do art. 42 do Código de Defesa do Consumidor (CDC) (CDC, 1990). O colegiado deu provimento ao recurso por unanimidade, reformando a sentença para declarar a inexistência de relação jurídica.

A fundamentação do acórdão enfatizou a vulnerabilidade de contratos eletrônicos sem mecanismos de autenticação e imutabilidade, destacando fraudes comuns, com dados pessoais obtidos ilegalmente na *deep web*, e a insuficiência de elementos como selfies, geolocalização ou dados básicos para comprovar a autoria, contrariando requisitos de integridade e não repúdio.

A relatora ressaltou a necessidade de registro em plataformas neutras e imparciais, como

---

<sup>4</sup> *Timestamping* (ou carimbo de tempo) é o processo de registrar data e hora exatas em que um determinado evento ocorreu. Esse registro é geralmente feito de forma automática e segura, para que possa ser utilizado como prova de quando algo aconteceu, especialmente em contextos onde a integridade e a autenticidade das informações são importantes.

cartórios de registro ou *blockchain*, para garantir a inalterabilidade do documento após assinatura. Citou doutrina sobre a tecnologia *blockchain* como meio seguro de prova em processos digitais, alinhando-se à evolução do direito probatório eletrônico e à proteção ao consumidor vulnerável.

O Agravo de Instrumento nº 2237253-77.2018.8.26.0000/SP, de relatoria da Desembargadora Fernanda Gomes Camargo, julgado em 19 de dezembro de 2018 (TJSP, 2018), envolveu o pedido de remoção de publicações ofensivas feitas em redes sociais. O agravante, político de projeção nacional, alegando conteúdos inverídicos, ofensivos e ameaçadores em páginas das redes sociais, os quais violavam sua honra e sua imagem, requereu tutela de urgência para citada remoção, fornecimento de dados dos usuários responsáveis e abstenção de comunicação a terceiros. A decisão de primeira instância indeferiu o pedido, e o agravo visava reformá-la, sustentado no *fumus boni iuris e periculum in mora*, nos termos do art. 300 do Código de Processo Civil (CPC) de 2015 e do art. 22 da Lei nº 12.965/2014.

No entanto, o colegiado, por unanimidade, negou provimento ao recurso e manteve o indeferimento, ao entender que a análise da veracidade dos conteúdos e de eventuais excessos demandava dilação probatória sob contraditório, sem elementos suficientes em cognição sumária para justificar a medida cautelar.

A fundamentação do acórdão enfatizou o equilíbrio entre liberdade de expressão, assegurada pelos arts. 5º, IV, IX, V e X, e 220 da CF/88, e proteção à honra e à imagem, destacando que o controle judicial sobre manifestações do pensamento deve ser excepcional para evitar censura prévia. A relatora ressaltou a necessidade de demonstração inequívoca da falsidade das informações para intervenção judicial, com base em precedentes do STJ, e rejeitou o pedido de fornecimento de dados dos usuários por ausência de fundados indícios de ilícito e por justificativa motivada.

Inovadoramente, o julgado reconheceu a validade da preservação de provas digitais via *blockchain*, utilizada pelo agravante por meio da plataforma *OriginalMY*<sup>5</sup>, para registrar o conteúdo ofensivo e sua integridade. Esse reconhecimento configurou uma das primeiras decisões judiciais brasileiras a admitir essa tecnologia como meio idôneo de comprovação em processos cíveis; alinhou-se à evolução do Direito Digital e à segurança proporcionada pela imutabilidade dos registros em cadeia de blocos.

---

<sup>5</sup> OriginalMy é uma plataforma brasileira que oferece soluções de autenticação, assinatura digital e registro de informações com garantia de integridade por meio da tecnologia *blockchain*. Fundada em 2015, a empresa tem como principal objetivo promover a governança digital, reduzir a burocracia e aumentar a transparência em processos que envolvem documentos, identidades e comprovações de autoria.

No processo, ficou entendido ainda que, para a assinatura eletrônica ser válida, é imprescindível se contar com mecanismos robustos para verificação da autenticidade do signatário, além do registro imediato do documento em banco público de dados de terceiros, garantindo sua imutabilidade para ambas as partes. Exemplos comuns desse registro incluem Cartórios de Registro de Títulos e Documentos e uso de tecnologias como a *blockchain*.

O tribunal, contudo, destacou que a tecnologia apenas assegura o registro e integridade de um dado em determinado momento, mas não garante que o conteúdo registrado seja verdadeiro. Por isso, não estavam presentes os requisitos do art. 300 do CPC (2015) para a concessão da tutela de urgência.

A decisão reforçou que a liberdade de expressão só pode ser limitada em situações excepcionais, pois a remoção imediata, sem prova cabal da falsidade, configuraria censura prévia. O caso ilustra os limites da *blockchain* como meio de prova, ou seja, ela atesta que algo foi registrado, mas não sua veracidade. Esse ponto é crucial também para o debate sobre *smart contracts*, que dependem de dados externos e que, sem oráculos confiáveis, podem executar automaticamente resultados baseados em informações falsas.

A distinção entre imutabilidade técnica e veracidade fática é essencial para *smart contracts* que dependem de oráculos, como os contratos de seguros paramétricos. Em cenários hipotéticos, no Brasil, falhas nos *feeds* de dados poderiam resultar em execuções injustas. Tal condição torna clara a necessidade de uma jurisprudência que incorpore auditorias independentes para validar *inputs* externos, seguindo orientações da doutrina mais recente.

### **3.4. Padrões decisórios e incipiência do debate sobre a autoexecutoriedade**

A análise da jurisprudência evidencia que o Judiciário brasileiro tem se mostrado receptivo à modernização das relações contratuais e à incorporação de novas tecnologias no processo probatório. O STJ já consolidou entendimento de que a forma eletrônica não compromete a validade de um negócio jurídico, valorizando a manifestação de vontade das partes e a boa-fé, ainda que os instrumentos não atendam a formalismos tradicionais, como a assinatura de testemunhas. Essa postura demonstra a superação da antiga desconfiança em relação ao meio digital e a adoção de critérios de autenticidade e de integridade como fundamentos suficientes para assegurar a eficácia contratual.

No campo probatório, decisões como a que envolveu o uso da *blockchain* para registro de conteúdos reforçam a distinção entre a imutabilidade tecnológica e a veracidade do conteúdo. Mostram que os tribunais reconhecem o potencial probatório da tecnologia, mas de forma crítica e equilibrada, preservando garantias constitucionais como o contraditório e a liberdade

de expressão.

Em conjunto, esses precedentes revelam um terreno fértil para a futura aceitação dos *smart contracts*, cuja lógica de autoexecutoriedade e de registro criptográfico encontra respaldo na tendência jurisprudencial de prestigiar a eficiência, a autenticidade e a confiança nas transações digitais.

Apesar da receptividade demonstrada pela jurisprudência, quanto à validade de contratos eletrônicos e ao uso da *blockchain* como meio de prova, permanece uma lacuna central: os tribunais ainda não enfrentaram o aspecto mais disruptivo dos *smart contracts*, que é, justamente, a comentada autoexecutoriedade e a consequente ausência de um intermediário humano, capaz de interromper ou reverter a execução. As decisões analisadas continuam partindo do pressuposto de que o Judiciário pode intervir para forçar o cumprimento ou anular cláusulas, o que pressupõe uma reversibilidade que, na lógica de um contrato inteligente puro, pode simplesmente não existir.

Nesse sentido, vê-se que não há, até o momento, precedentes consolidados que tratem diretamente da execução irreversível de um *smart contract*. A jurisprudência tem enfrentado questões de validade formal, de autoria, de integridade de registros e de meios de prova digitais; ainda não se deparou com litígios que envolvam efeitos autoexecutados e imutáveis.

Esse vazio evidencia a necessidade de construção doutrinária e legislativa, seja para estabelecer mecanismos de intervenção (como cláusulas de escape ou arbitragem especializada), seja para regulamentar a atuação de oráculos confiáveis. Assim, embora haja uma base favorável à aceitação dos *smart contracts*, o desafio concreto de lidar com sua execução automática permanece em aberto.

Conclui-se, portanto, que a análise jurisprudencial revela um Judiciário aberto à incorporação de tecnologias, validando contratos eletrônicos, reconhecendo a força probatória de registros digitais e sinalizando confiança na autenticidade e integridade de meios inovadores como a *blockchain*. Contudo, ao mesmo tempo, a jurisprudência permanece ancorada em modelos tradicionais de controle e de execução contratual, com a possibilidade de intervenção judicial para corrigir abusos, forçar cumprimento ou anular cláusulas.

Essa posição, embora ofereça uma base de segurança jurídica ao resguardar valores constitucionais, como a ampla defesa e o contraditório, deixa evidente a necessidade de um marco legal específico que oriente a atuação judicial diante dos desafios trazidos pela automação e pela descentralização próprias dos *smart contracts*.

Somente com diretrizes normativas claras, assunto abordado a seguir, será possível preencher o vácuo deixado pela doutrina e pela prática, garantindo equilíbrio entre inovação



tecnológica, segurança jurídica e efetividade da tutela jurisdicional.

#### **4. UMA PROPOSTA DE REGULAMENTAÇÃO PARA OS *SMART CONTRACTS* NO BRASIL**

Este capítulo final assume um caráter propositivo, construído sobre os alicerces estabelecidos anteriormente. A jornada investigativa partiu do Capítulo 1, que estabeleceu o problema teórico ao evidenciar a tensão entre a tecnologia disruptiva dos *smart contracts* e a dogmática civilista tradicional. Em seguida, o Capítulo 2 apresentou um diagnóstico prático, revelando uma jurisprudência receptiva a inovações digitais, mas ainda despreparada para lidar com as especificidades da autoexecutoriedade e da imutabilidade. Com base nesse panorama, no presente capítulo, será feita uma elucidação sobre o tema, analisando-se as propostas legislativas e oferecendo diretrizes para uma regulamentação eficaz que promova a segurança jurídica sem inibir o avanço tecnológico.

##### **4.1. Síntese diagnóstica: A insegurança jurídica como obstáculo à inovação**

A ausência de um marco legal claro para os *smart contracts* no Brasil cria um ambiente de acentuada insegurança jurídica, que se reflete no problema central desta pesquisa. Para as empresas e desenvolvedores, essa lacuna legislativa representa o risco de que seus contratos, nos quais investiram recursos e tecnologia, sejam considerados inválidos ou inexecutáveis perante o Judiciário. Para os usuários, a incerteza é igualmente prejudicial, pois, em caso de falhas de código ou de resultados manifestamente injustos, há o risco de não terem a quem recorrer, tornando a resolução de conflitos um desafio complexo e de difícil solução (Silva; Coutinho, 2025, p. 2213–2215 ).

Essa insegurança jurídica transcende o risco contratual individual e funciona como um freio sistêmico ao desenvolvimento e à adoção da tecnologia no país. A ausência de uma legislação específica, apontada como a principal barreira para a implementação generalizada dos *smart contracts*, gera incertezas que desestimulam a adoção de soluções tecnológicas mais avançadas e inovadoras (Kaczmarek-Templin, 2023, p. 65–75; Monteiro *et al.*, 2021, p.315 - 320 ).

A literatura especializada sobre o tema corrobora amplamente a tese de que um ambiente regulatório estável, claro e previsível é um pré-requisito essencial para atrair investimentos e para fomentar o desenvolvimento de novas tecnologias. A previsibilidade normativa permite que investidores e empresas possam planejar suas ações com segurança e reduz incertezas quanto à aplicação das regras e à interpretação das leis ao longo do tempo.

Em contrapartida, a instabilidade ou a ambiguidade regulatória eleva o risco jurídico, tornando o ambiente de negócios mais volátil e, muitas vezes, inóspito à inovação. Sem uma base regulatória sólida, os custos associados à insegurança jurídica podem se sobrepor aos potenciais ganhos de eficiência e desestimular iniciativas empreendedoras e a adoção de soluções tecnológicas mais avançadas. Portanto, a construção e a manutenção de um marco regulatório confiável são elementos estratégicos para impulsionar a competitividade econômica e promover o progresso tecnológico sustentável (Giancaspro, 2017, p.830; Kuznetsova, 2022, p.134–149).

#### **4.2. Análise das iniciativas legislativas: o marco das criptomoedas e o Projeto de Lei 954/2022**

A Lei nº 14.478, de 21 de dezembro de 2022, conhecida como Marco Legal dos Criptoativos, insere-se no ordenamento jurídico brasileiro como um instrumento pivotal para a regulação do mercado de ativos virtuais. Ancora-se na Teoria Geral dos Contratos do CC (2002), que preconiza a autonomia privada e a liberdade contratual (arts. 421 e 422) como pilares para a validade de pactuações eletrônicas e automatizadas, sem prejuízo da boa-fé e da função social.

Seu escopo principal reside na regulamentação das Prestadoras de Serviços de Ativos Virtuais (PSAV), definidas como entidades autorizadas a realizar atividades de troca, de transferência, de custódia e de administração de ativos virtuais — representações digitais de valor registradas eletronicamente e utilizáveis para pagamentos ou investimentos, excluindo moedas fiduciárias ou ativos financeiros tradicionais (art. 3º). Tudo com exigência de autorização prévia de órgãos federais, como o Banco Central do Brasil (BCB), e observância de princípios, como transparência, segurança cibernética, proteção ao consumidor e prevenção à lavagem de dinheiro (arts. 2º, 4º e 5º) (CC, 2002).

Essa estrutura normativa impõe sanções administrativas e penais, incluindo a tipificação de fraudes com ativos virtuais (art. 10 do Código Penal (CP) (1940) e a inclusão das PSAV nas obrigações de combate a ilícitos financeiros (alterações nas Leis nº 7.492/1986 (CDC, 1986a) e nº 9.613/1998, fomentando um ambiente de supervisão que mitiga riscos sistêmicos sem proibir inovações tecnológicas.

Embora a Lei nº 14.478/2022 não aborde diretamente os *smart contract* — cuja imutabilidade e automação desafiam interpretações tradicionais da vontade contratual sob o Código Civil —, sua relevância para o ecossistema *blockchain* é inegável. Ela representa a primeira legislação brasileira de envergadura a legitimar o uso de tecnologias distribuídas de

registro, ao reconhecer ativos virtuais como instrumentos jurídicos válidos e atribuir competências explícitas ao BCB e a outros órgãos federais para autorizações, fiscalização e aplicação de medidas disciplinares (arts. 6º a 8º). Preenche, assim, lacunas regulatórias anteriores e sinaliza maturidade institucional.

Essa abordagem indireta, ao enquadrar serviços de custódia e de transferência em PSAV, sem menção específica a Protocolos de Finanças Descentralizadas (DeFi)<sup>6</sup> ou *smart contracts*, cria um arcabouço propício a futuras normatizações. Exemplo disso são as resoluções do BCB sobre inovação financeira, promovendo segurança jurídica e incentivando investimentos em *blockchain*, conforme análises econômicas que destacam sua função em estabilizar o mercado sem asfixiar a inovação.

#### 4.3. Análise das iniciativas legislativas: o PL 954/2022

A discussão teórica sobre os *smart contracts* ganha contornos práticos com a análise do Projeto de Lei (PL) 954/2022 (CD, 2022a), a principal iniciativa legislativa no Brasil para endereçar o tema. Proposto pelo Deputado Luizão Goulart (Solidariedade/PR), o projeto tem uma abordagem minimalista, mas com implicações profundas para o futuro das relações contratuais digitais no país.

O cerne desse PL é a adição de um parágrafo único ao artigo 425 do CC. O referido artigo estabelece a licitude dos contratos atípicos, ou seja, aqueles que não possuem uma forma específica prevista em lei, desde que observadas as normas gerais fixadas no Código. A redação proposta é a seguinte:

Art. 425 [...]

Parágrafo único. O disposto no caput aplica-se inclusive a contratos estruturados sob definições para sua execução, no todo ou em parte, de modo automatizado e mediante emprego de plataformas eletrônicas e soluções tecnológicas que assegurem autonomia, descentralização e autossuficiência, dispensando intermediários para a implementação do acordo entre os contratantes ou garantir a autenticidade (NR) (CD, 2022a, p. 1)

A estratégia legislativa é clara: em vez de criar um regime jurídico específico e detalhado para os *smart contracts*, opta-se por enquadrá-los na categoria aberta e flexível dos contratos atípicos. Com isso, busca-se conferir a eles validade jurídica de forma ampla, submetendo-os aos princípios gerais do Direito Contratual sem, contudo, regulamentar suas

---

<sup>6</sup> Os protocolos de Finanças Descentralizadas, conhecidos pela sigla DeFi (Decentralized Finance), representam um conjunto de aplicações e contratos inteligentes que operam sobre redes *blockchain* públicas, como a Ethereum, visando a execução de serviços financeiros sem a necessidade de intermediários tradicionais, tais como bancos e corretoras

peculiaridades técnicas e operacionais.

O percurso do PL 954/2022 na Câmara dos Deputados revela uma estratégia de tramitação célere. Ele está sujeito ao regime de Apreciação Conclusiva pelas Comissões, conforme o Art. 24, II, do Regimento Interno da Câmara dos Deputados (CD, 2000). Isso significa que, se aprovado pela Comissão de Constituição e Justiça e de Cidadania (CCJC), ele não precisa ser votado pelo Plenário da Casa, seguindo diretamente para o Senado Federal, a menos que haja recurso. Atualmente, o projeto encontra-se no estágio de "Aguardando Parecer do(a) Relator(a)", função designada à Deputada Caroline de Toni (PL-SC).

As iniciativas legislativas, representadas pela Lei nº 14.478/2022 e pelo PL 954/2022 (CD, 2022a) constituem avanços significativos para o reconhecimento do ecossistema *blockchain* no Direito brasileiro. É que, ao legitimar ativos virtuais e enquadrar *smart contracts* como contratos atípicos sob o art. 425 do CC (Brasil, 2002), promove a segurança jurídica inicial e incentiva a inovação tecnológica em um ambiente regulado pelo BCB e por princípios contratuais tradicionais, como autonomia privada e boa-fé objetiva.

No entanto, essas medidas revelam-se passos preliminares, insuficientes para endereçar as questões mais espinhosas, tais como a tensão entre a imutabilidade do código dos *smart contracts* e a possibilidade de revisão judicial por vícios de consentimento ou erro (arts. 138-165 do CC (2002); a responsabilidade civil por falhas em oráculos externos que alimentam a automação ou os desafios processuais para execução forçada e para a produção de provas em redes descentralizadas e transfronteiriças; nessas, a ausência de intermediários complica a aplicação de normas imperativas e a proteção ao consumidor.

A abordagem minimalista do PL 954/2022 (CD, 2022a), limitada a uma inserção definicional no CC, carece de regras materiais substantivas, a exemplo de critérios para interpretação do código como manifestação de vontade ou mecanismos para correção de desigualdades contratuais. Necessita também de normas processuais adequadas, como procedimentos específicos para auditoria de *blockchain* em juízo ou integração com o Marco Civil da Internet (Lei nº 12.965/2014) para questões de jurisdição digital. A abordagem minimalista traz o risco de gerar lacunas que perpetuem inseguranças jurídicas em aplicações práticas, como DeFi, conforme criticado por análises doutrinárias que enfatizam a necessidade de um regime híbrido que concilie rigidez tecnológica com flexibilidade normativa.

#### **4.4. Proposta de *lege ferenda*: diretrizes para uma legislação sobre *smart contracts***

Com base na pesquisa desenvolvida, que evidenciou a insuficiência das propostas legislativas atuais para endereçar as complexidades dos *smart contracts*, propõe-se um conjunto

de diretrizes para a elaboração de uma legislação mais efetiva. O objetivo não é redigir artigos de lei, mas sim, apontar temas cruciais que uma regulamentação mais eficiente precisa obrigatoriamente enfrentar para harmonizar a inovação tecnológica com a segurança jurídica, superando a abordagem meramente definicional e enfrentando os desafios práticos da autoexecutoriedade e da imutabilidade

Na diretriz concernente à forma e ao consentimento nos *smart contracts*, uma legislação mais efetiva deve priorizar a acessibilidade e a transparência para mitigar assimetrias informacionais e estabelecer padrões mínimos de clareza para o código programado.

Isso incluiria a obrigatoriedade de um "sumário" em linguagem natural, redigido em português claro e acessível, que delineasse as principais cláusulas contratuais, as condições de execução automática e os riscos potenciais envolvidos, como falhas em oráculos ou volatilidade de ativos virtuais. Tal medida não apenas reforçaria o princípio da boa-fé objetiva (art. 422 do CC de 2002), ao promover um consentimento mais informado e voluntário, mas também se alinharia à proteção ao consumidor prevista no CDC (1990). Evitar-se-ia que a complexidade técnica do código obscurecesse a verdadeira manifestação de vontade das partes e se reduzissem litígios decorrentes de mal-entendidos. A diretriz relativa a mecanismos de intervenção buscaria equilibrar a rigidez inerente aos *smart contracts* com a necessidade de flexibilidade em situações excepcionais, propondo a criação de ferramentas que permitissem pausas ou reversões mediante decisões judiciais ou arbitrais.

Pesquisas recentes indicam que já existem soluções técnicas, que podem tornar-se legislativas, implementadas em protocolos *blockchain*, com o objetivo de mitigar riscos operacionais e de preservar a segurança dos usuários, mesmo em ambientes de governança minimamente centralizada.

Entre essas soluções, destacam-se os chamados *escape hatches*, “cláusulas de escape”, mecanismos de emergência que podem ser acionados por gatilhos específicos, como a inatividade de operadores ou o descumprimento de obrigações por parte dos *sequencers*. Esses dispositivos funcionam como salvaguardas contratuais automatizadas e permitem que os usuários recuperem seus ativos diante de falhas operacionais graves, sem comprometer os princípios de descentralização (Gorzny; Po-An; Derka, 2022, p. 7-12).

Tais mecanismos são particularmente relevantes no contexto dos *rollups*, soluções de segunda camada (Layer 2) que executam transações fora da *blockchain* principal (Layer 1), mas ainda dependem dela para garantir segurança e verificabilidade. Nessa arquitetura, os *sequencers* exercem a função de ordenar e de publicar transações com alta performance e baixo custo. Porém, a atuação centralizada do *sequencer* pode representar um ponto de falha,

especialmente em casos de censura ou de paralisação (Gorzny; Po-An; Derka, 2022, p. 7-12).

Para assegurar que os usuários possam exercer seu direito de retirada (*exit rights*) de forma segura e autônoma, muitos *rollups* utilizam *Merkle proofs*, estruturas criptográficas que permitem comprovar, com eficiência e integridade, que uma transação ou saldo faz parte do estado registrado na *blockchain* principal.

Em conjunto com contratos inteligentes resolutores, essas provas viabilizam saídas seguras diretamente na camada base, mesmo sem cooperação do *sequencer*, reforçando a confiança e a robustez jurídica desses sistemas. Assim, os *escape hatches*, os *Merkle proofs* e os contratos programáveis compõem um arcabouço técnico-jurídico que visa equilibrar inovação, segurança operacional e garantias legais mínimas no uso de tecnologias descentralizadas (Chen *et al.*, 2021, p.4; Chevalier, 2021, p. 571 - 576 ).

A futura legislação deve incentivar ou tornar obrigatório o emprego desses mecanismos em contratos de consumo ou de longa duração, integrando-os ao ordenamento brasileiro para alinhar com normas imperativas e preservar a função social do contrato (art. 421 do CC (2002), promovendo, assim, uma governança híbrida que mitigue riscos sistêmicos sem inibir a inovação.

Uma diretriz central para a nova legislação seria a criação de um sistema de classificação de risco para os *smart contracts*, o qual poderia ser combinado com o uso de Inteligência Artificial (IA) para monitoramento e fiscalização. Embora um sistema regulatório estatal, que utilize Inteligência Artificial (IA) para proibições automáticas, ainda seja uma proposta em desenvolvimento, a abordagem baseada em risco é um modelo já adotado em outras áreas, como no *AI Act*, da União Europeia, que classifica as aplicações de IA em categorias de risco inaceitável, alto e baixo. A tecnologia para tal monitoramento também avança no setor privado, onde ferramentas de IA são empregadas para auditar códigos e para detectar vulnerabilidades e anomalias em tempo real. A implementação de um sistema similar no Brasil, ao identificar um objeto de alto risco ou ilegal, poderia acionar proibições automáticas ou suspender a execução do contrato, mitigando danos potenciais antes de se tornarem irreversíveis e fomentando um ecossistema de usos legítimos da tecnologia sem coibir a inovação (Gabardo; Dutra, 2024, p. 86-90 ; Laux; Wachter; Mittelstadt, 2024, p.2).

Quanto à diretriz de responsabilidade civil, a regulamentação deve delinear critérios claros para estabelecê-la entre os atores envolvidos, conforme as respectivas obrigações: os desenvolvedores, responsáveis pela integridade do código; as plataformas de hospedagem, pela segurança operacional; os auditores independentes, pela verificação prévia de vulnerabilidades e os provedores de oráculos, pela precisão de dados externos.

Essa definição hierárquica de responsabilidades, inspirada na Teoria da Culpa Contratual (art. 389 do CC) (2002) e na responsabilidade objetiva, em certos casos (art. 927, parágrafo único), incentivaria práticas de auditorias regulares, elevando a confiança dos usuários e reduzindo danos decorrentes de falhas técnicas ou maliciosas. Ao estabelecer sanções proporcionais e mecanismos de reparação, a lei fomentaria um ecossistema mais seguro, alinhado à Lei nº 14.478/2022, sem sobrecarregar a inovação com burocracia.

A regulamentação dos *smart contracts* no ordenamento jurídico brasileiro não deve buscar restringir ou limitar a inovação tecnológica, mas sim, estabelecer um "porto seguro" jurídico, que garanta confiança a todos os envolvidos. Uma legislação cuidadosamente estruturada, que contemple padrões mínimos de clareza (como sumários em linguagem natural), mecanismos de intervenção (como cláusulas de emergência) e alocação clara de responsabilidades civis, deve harmonizar-se com os princípios da autonomia privada, com a boa-fé objetiva e com a função social do contrato, bem como com o arcabouço do Marco Legal dos Criptoativos.

Essa abordagem permitiria, ao Estado brasileiro, explorar o potencial transformador dos *smart contracts* em áreas apontadas por Dixit et al (2022, p.10-11), como finanças, logística e gestão contratual, promovendo eficiência e redução de custos, enquanto protege consumidores e assegura a conformidade com normas imperativas, como asseguram Ordoñez; Niviayo; Molano (2019, p.504). Assim, o país poderá consolidar-se como um ambiente propício à inovação *blockchain*, incentivando investimentos e aplicações práticas com segurança jurídica e eficiência.

## 5. CONCLUSÃO

Este trabalho se propôs a investigar a complexa relação entre os contratos inteligentes, uma tecnologia de vanguarda, e as estruturas seculares do Direito Civil brasileiro, buscando caminhos para uma coexistência harmônica e segura. A pesquisa partiu da necessidade de compreender como um instrumento autoexecutável e imutável, que opera com base em uma lógica de código, poderia ser integrado a um ordenamento jurídico pautado pela flexibilidade, pela interpretação da vontade humana e pela possibilidade de revisão judicial, pilares fundamentais da justiça contratual.

A análise demonstrou que, no plano teórico (Capítulo 1), os *smart contracts* desafiam dogmas contratuais clássicos, especialmente no que tange à manifestação de vontade, que se torna opaca pela "tirania do código", e à possibilidade de revisão, que colide frontalmente com a imutabilidade da *blockchain*. No plano prático (Capítulo 2), a jurisprudência, embora demonstre uma postura favorável a contratos eletrônicos em geral, ainda não desenvolveu ferramentas para lidar com a autoexecutoriedade e a irreversibilidade dos *smart contracts*, mantendo-se apegada a um modelo de controle judicial *a posteriori*, que a tecnologia visa, em essência, contornar. Esse diagnóstico levou à compreensão, no Capítulo 3, de que as soluções legislativas atuais, como o PL 954/2022, são tímidas e que uma regulamentação eficaz deve ir além do mero reconhecimento, devendo focar mecanismos de transparência, de intervenção e de responsabilização.

Diante do exposto, conclui-se que o ordenamento jurídico brasileiro, em seu estado atual, não está plenamente apto a regular os *smart contracts*, confirmando-se a hipótese inicial. A aplicação analógica do Código Civil, embora seja o caminho inicial, é uma medida paliativa que não resolve as tensões fundamentais entre a rigidez do código computacional e a flexibilidade exigida pelo Direito para garantir a justiça contratual.

A segurança jurídica e o fomento à inovação dependem, portanto, da criação de um microsistema legal específico para essa nova realidade, que estabeleça diretrizes claras para a validade, para a interpretação e, crucialmente, para a possibilidade de controle e de correção dos efeitos desses novos instrumentos, evitando que a automação resulte em injustiça.

Ressalta-se que este estudo se ateve a uma análise dogmática e jurisprudencial do cenário brasileiro neste momento e que se reconhecem suas limitações. Pesquisas futuras poderiam enriquecer o debate por meio de estudos de Direito Comparado, analisando como jurisdições mais avançadas na matéria, como a Suíça ou alguns estados norte-americanos, estão regulamentando o tema e quais lições podem ser aprendidas.



Adicionalmente, são necessárias pesquisas empíricas que investiguem os tipos de conflitos que vêm surgindo na prática entre usuários de plataformas de *smart contracts* no Brasil, a fim de subsidiar o legislador com dados concretos sobre as vulnerabilidades desse tipo de contratação e as necessidades do mercado, garantindo que a futura legislação seja não apenas teoricamente sólida, mas também pragmaticamente eficaz.

## REFERÊNCIAS

ACRE. **Reconhecimento da força probatória dos contratos digitais: elementos de validação e compatibilidade com o CPC**. Rio Branco: Tribunal de Justiça, 2025.

BHAT, Showkat Ahmad *et al.* Agriculture-Food Supply Chain Management Based on Blockchain and IoT: A Narrative on Enterprise Blockchain Interoperability. **Agriculture (Switzerland)**, v. 12, n.1, p. 1–40, 2022.

BRASIL. Câmara dos Deputados. **Regimento Interno da Câmara dos Deputados**: Brasília/DF, 5º ed., 2000. Disponível em: <https://www2.camara.leg.br/atividade-legislativa/legislacao/regimento-interno-da-camara-dos-deputados>. Acesso em: 1 ago. 2025.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 954, Dep. Luizão Goulart**: Câmara dos Deputados, Brasília/DF, 19/04/2022, 2022a. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2320041>. Acesso em: 31 jul. 2025.

BRASIL. Constituição da República Federativa do Brasil, de 05 de outubro de 1988. **Diário Oficial da União**: p. 1, 5 out. 1988. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/constituicao/constituicao.htm](https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm). Acesso em: 18 set. 2025.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. **Diário Oficial da União**: Brasília, DF, Seção 1, p. 1, 31 dez. 1940. Disponível em: <https://www2.camara.leg.br/legin/fed/declei/1940-1949/decreto-lei-2848-7-dezembro-1940-412868-norma-pe.html>. Acesso em: 1 ago. 2025.

BRASIL. Lei nº 7.492, de 16 de junho de 1986. Código de Defesa do Consumidor. **Diário Oficial da União**: Brasília, DF, Seção 1, p. 1, 18 jun. 1986a. Disponível em: <https://www2.camara.leg.br/legin/fed/lei/1980-1987/lei-7492-16-junho-1986-367988-norma-pl.html>. Acesso em: 31 jul. 2025.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Código de Defesa do Consumidor. **Diário Oficial da União**: Brasília, DF, Seção 1, p. 1, 12 set. 1990. Disponível em: <https://www2.camara.leg.br/legin/fed/lei/1990/lei-8078-11-setembro-1990-365086-norma-pl.html>. Acesso em: 1 ago. 2025.

BRASIL. Lei nº 9.613, de 3 de março de 1998. Dispõe sobre os crimes de “lavagem” ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselho de Controle de Atividades Financeiras - COAF, e dá outras providências. **Diário Oficial da União**: Brasília, DF, Seção 1, p. 1, 4 mar. 1986b. Disponível em: <https://www2.camara.leg.br/legin/fed/lei/1998/lei-9613-3-marco-1998-372359-norma-pl.html>. Acesso em: 9 set. 2025.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. **Diário Oficial da União**: Brasília-DF, p. 1–74, 10 jan. 2002. Disponível em: [https://www.camara.leg.br/proposicoesWeb/prop\\_mostrarintegra?codteor=247357&filename](https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=247357&filename). Acesso em: 18 set. 2025.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet. Estabelece

princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da União**: Brasília, DF, 24 abr. 2014. Disponível em: <https://www2.camara.leg.br/legin/fed/lei/2014/lei-12965-23-abril-2014-778630-norma-pl.html>. Acesso em: 9 set. 2025.

BRASIL. Lei No 13.105, de 16 de março de 2015. Código de Processo Civil (CPC). **Diário Oficial da União**: Brasília, DF, seção 1, p. 1, 17 mar. 2015. Disponível em: <https://www2.camara.leg.br/legin/fed/lei/2015/lei-13105-16-marco-2015-780273-norma-pl.html>. Acesso em: 4 set. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**: Brasília, DF, seção 1, p. 59, 15 ago. 2018a. Disponível em: <https://www2.camara.leg.br/legin/fed/lei/2018/lei-13709-14-agosto-2018-787077-publicacaooriginal-156212-pl.html>. Acesso em: 11 set. 2025.

BRASIL. Lei nº 14.063, de 23 de setembro de 2020. Dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos, em atos e em processos administrativos. **Diário Oficial da União**: Brasília, DF, seção 1, p. 4, 24 set. 2020a. Disponível em: <https://www2.camara.leg.br/legin/fed/lei/2020/lei-14063-23-setembro-2020-790659-norma-pl.html>. Acesso em: 31 ago. 2025.

BRASIL. Lei nº 14.478, de 21 de dezembro de 2022. Dispõe sobre diretrizes a serem observadas na prestação de serviços de ativos virtuais e na regulamentação das prestadoras de serviços de ativos virtuais (Marco das Criptomoedas). **Diário Oficial da União**: Brasília, DF, Seção 1, p. 3, 22 dez. 2022b. Disponível em: <https://www2.camara.leg.br/legin/fed/lei/2022/lei-14478-21-dezembro-2022-793516-norma-pl.html>. Acesso em: 1 set. 2025.

BRASIL. Medida Provisória nº 2.200-2, de 24 de agosto de 2001. Institui a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, e dá outras providências. **Diário Oficial da União**: Brasília-DF, p. 94, 27 ago. 2001.

BRASIL. **Provimento nº 100, de 26 de maio de 2020**. Conselho Nacional de Justiça: Brasília/DF, 2020b. Disponível em: <https://atos.cnj.jus.br/files/original222651202006025ed6d22b74c75.pdf>. Acesso em: 4 set. 2025.

BRASIL. **Recurso Especial nº 1.495.920/DF (2014/0295300-9)**. Brasília - DF : Superior Tribunal de Justiça, Relator: Ministra Paulo de Tarso Sanseverino, 3ª Turma, DJe. 07/06/2018, 2018b. Disponível em: <https://stj.jus.br/websecstj/cgi/revista/REJ.cgi/ATC?seq=78697787&tipo=51&nreg=201402953009&dt=20180607&formato=PDF&salvar=false>. Acesso em: 14 set. 2025.

BRASIL. **Recurso Especial nº 2.150.278/PR (2024/0212892-1)**. Brasília - DF : Superior Tribunal de Justiça, Relator: Ministra Nancy Andrichi, 3ª Turma, DJe. 27/09/2024, 2024a. Disponível em: [https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num\\_registro=202402128921&dt\\_publicacao=27/09/2024](https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202402128921&dt_publicacao=27/09/2024). Acesso em: 9 set. 2025.

BRASIL. **Recurso Especial nº 2.159.442/PR (2024/0267355-0)**. Brasília - DF : Superior

Tribunal de Justiça, Relator: Ministra Nancy Andrighi, 3ª Turma, DJe. 27/09/2024, 2024b.

Disponível em:

[https://processo.stj.jus.br/processo/julgamento/eletronico/documento/mediado/?documento\\_tipo=5&documento\\_sequencial=272898917&registro\\_numero=202402673550&peticao\\_numero=&publicacao\\_data=20240927&formato=PDF](https://processo.stj.jus.br/processo/julgamento/eletronico/documento/mediado/?documento_tipo=5&documento_sequencial=272898917&registro_numero=202402673550&peticao_numero=&publicacao_data=20240927&formato=PDF). Acesso em: 20 set. 2025.

BRITO MOREIRA, Kleber; CHAIM, Ricardo Matos. **Blockchain - Tecnologia, Arquitetura e Aplicações**. 2019. 1–85 f. Monografia (Graduação) - Universidade de Brasília, Brasília, 2019.

CABRAL, Natan Souza; SILVA, Leandro Barbosa. **Smart Contracts e os Princípios de Validade do Negócio Jurídico na Teoria da Escada Pontean**. 2022. Monografia (Graduação em Direito) - Faculdade Santo Agostinho de Sete Lagoas, Sete Lagoas, 2022.

CÁRDENAS, Erick Rincón; MOLANO, Valeria Martínez. Smart Contracts and Automation as Applied Developments of Legaltech in Colombia. **Revista Direito GV**, v. 18, n. 1, p. 1–22, 2022.

CARDOSO, Stephanie Trindade; MARINO, Francisco Paulo de Crescenzo. **Smart Contracts: Caracterização e aplicação no direito contratual brasileiro**. 2022. Dissertação (Mestrado em Direito) - Universidade de São Paulo, São Paulo, 2022.

CHEN, Chin Ling *et al.* A traceable online will system based on blockchain and smart contract technology. **Symmetry**, v. 13, n. 3, p.1-19, 2021.

CHEVALIER, Maxime. From Smart Contract Litigation to Blockchain Arbitration, a New Decentralized Approach Leading Towards the Blockchain Arbitral Order. **Journal of International Dispute Settlement**, v. 12, n.4, p. 558–584, 2021.

CORNELIUS, Kristin B. Standard form contracts and a smart contract future. **Internet Policy Review**, v 7, n.2, 2018.

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

DIVINO, Sthéfano Bruno Santos. Smart Contracts: Conceitos, Limitações, Aplicabilidade e Desafios. **RJLB**, v. 4, p.2771–2808, 2018.

DIXIT, Abhishek *et al.* **Towards user-centered and legally relevant smart-contract development: A systematic literature review**. [S. l.]: Elsevier B.V., 2022.

DWORKIN, Ronald. **O império do direito**. tradução: Jefferson Luiz Camargo. São Paulo: Martins Fontes, 1999.

DYKSTRA, Mayna Marchiori; MORAES, Michele Hertz Marchiori; MORAES, Rodrigo Marchiori de. Smart Contracts: os desafios à adoção dos contratos inteligentes pelo ordenamento jurídico brasileiro. **Revista Eletrônica do TRT-PR**, v. 12, n. 118, 2023.

EFING, Antonio Carlos; SANTOS, Adrielly Pinho dos. Análise dos Smart Contracts à luz do Princípio da Função Social dos Contratos no Direito Brasileiro. **Direito e Desenvolvimento**,

v. 9, n. 2, p. 50–64, 2018.

FERRAZ, Robertson Novellino; SILVA, Artur Stamford da. **As tecnologias envolvendo os contratos inteligentes (Smart Contracts) e alguns dos impactos nos contratos**. 2019. 1–68 f. Monografia (Graduação em Direito) - Universidade Federal de Pernambuco, Recife, 2019.

GABARDO, Emerson; DUTRA, Gustavo Ferreira de Souza. Smart contracts: blockchain e a ressignificação do pacta sunt servanda. **International Journal of Digital Law**, v. 5, n. 1, p. 79–102, 2024.

GE, Xianyun. Smart Payment Contract Mechanism Based on Blockchain Smart Contract Mechanism. **Scientific Programming**, v.1, p. 1-12, 2021.

GIANCASPRO, Mark. Is a ‘smart contract’ really a smart idea? Insights from a legal perspective. **Computer Law and Security Review**, v. 33, n. 6, p. 825–835, 2017.

GOBBO, Leandro Oliveira; FILHO, Roberto Freitas. **Smart Contracts e o Direito Contratual Brasileiro**. 2022. Tese (Doutorado em Direito Constitucional) - Instituto Brasiliense de Direito Público, Brasília, 2022.

GOMES, Letícia Beatriz Arruda; MATIAS, João Luís Nogueira. **A eficácia da cláusula arbitral nos Smart Contracts**. 2022. Monografia (Graduação em Direito) - Universidade Federal do Ceará, Fortaleza, 2022.

GORZNY, Jan; PO-AN, Lin; DERKA, Martin. Ideal properties of rollup escape hatches. **DICG 2022 - Proceedings of the 3rd International Workshop on Distributed Infrastructure for the Common Good, Part of Middleware**, v.1, p.7-12, 2022.

HANNAN, Md Abdul *et al.* A systematic literature review of blockchain-based e-KYC systems. **Computing**, v. 105, n. 10, p. 2089–2118, 2023.

HEPP, Thomas *et al.* OriginStamp: A blockchain-backed system for decentralized trusted timestamping. **IT - Information Technology**, v. 60, n. 5–6, p. 273-281, 2018.

KACZMAREK-TEMPLIN, Berenika. The Smart Contract – problems with taking evidence in Polish Civil proceedings in the light of European regulations. **Bratislava Law Review**, v. 7, n. 1, p. 65–75, 2023.

KELL, Tyler *et al.* Forsage: Anatomy of a Smart-Contract Pyramid Scheme. 2024. **Lecture Notes in Computer Science**, vol 13951, p.241–258, 2024.

KUZNETSOVA, S. S. Topical issues of the realization and protection of human rights in the practice of smart contract technology application. **Law Enforcement Review**, v. 6, n.1, p. 134–149, 2022.

LAUX, Johann; WACHTER, Sandra; MITTELSTADT, Brent. Trustworthy artificial intelligence and the European Union AI act: On the conflation of trustworthiness and acceptability of risk. **Regulation and Governance**, v. 18, n. 1, p.3-32, 2024.

LIU, Yan; SHANG, Chao. Application of Blockchain Technology in Agricultural Water Rights

Trade Management. **Sustainability (Switzerland)**, v. 14, n.12, 2022.

LUCIANO, Romulo Benites de Souza. Aplicação da Smart Contract nos Contratos de Gás Natural: Uma Análise Exploratória. **Revista de Administração Contemporânea**, v. 22, n. 6, p. 903–921, 2018.

MARRIAGA, Cielo Ester; BONFANTE, Maria Claudia. Blockchain: Application in International Trade and Supply Chain Management. **TransInformação**, v. 35, n.1, 2023.

MENEZES, Leonardo Dias; ARAUJO, Luciano Vieira; NISHIJIMA, Marislei. Blockchain and smart contract architecture for notaries services under civil law: a Brazilian experience. **International Journal of Information Security**, v. 22, n. 4, p. 869–880, 2023.

MENEZES, Dionnísio Matheus Reis; DIAS, Jean Carlos. Os Requisitos de Validade do Negócio Jurídico nos Contratos Eletrônicos: Uma Análise a partir da Jurisprudência do Superior Tribunal de Justiça. **Revista Jurídica do CESUPA**, v. 1, n. 1, p. 92–115, 2023.

MENTESHASHVILI, Tamar. Blockchain, Law and Governance. **Chinese Journal of International Law**, v. 20, n. 1, p. 213–216, 2021. Disponível em: <https://doi.org/10.1093/chinesejil/jmab006>.

MILLARD, Christopher. Blockchain and law: Incompatible codes?. **Computer Law and Security Review**, v. 34, n. 4, p. 843–846, 2018.

MONTEIRO, Emiliano *et al.* Combining Natural Language Processing and Blockchain for Smart Contract Generation in the Accounting and Legal Field. 2021, Cham. (Madhusudan Singh et al., Orgs.) **Intelligent Human Computer Interaction**. Cham: Springer International Publishing, 2021. p. 307–321.

ORDOÑEZ, Luz Angélica Téllez; NIVIAYO, Evelyn Juliana Ruíz; MOLANO, José Ignacio Rodríguez. Approach to Blockchain and Smart Contract in Latin America: Application in Colombia. 2019, Cham. (Juan Carlos Figueroa-García et al., Orgs.) **Applied Computer Sciences in Engineering**. Cham: Springer International Publishing, 2019. p. 500–510.

QUEIROZ, Rafael Mafei Rabelo; FEFERBAUM, Marina. **Metodologia da Pesquisa em Direito: técnicas e abordagens para elaboração de monografias, dissertações e teses**. 2 ed. São Paulo: Saraiva, 2019.

RANCHORDÁS, Sofia. **Editorial: Blockchain, Public Trust, Law and Governance**. Groningen: Brill Nijhoff, 2019.

REBOUÇAS, Rodrigo Fernandes; VILLAS BÔAS, Regina Vera. **Contrato Eletrônico: Considerações sob a ótica do plano de validade do negócio jurídico na formação do contrato**. 2012. Dissertação (Mestrado em Direito das Relações Sociais) - Pontifícia Universidade Católica de São Paulo, São Paulo, 2012.

SANTOS, Gabriel Gonçalves; PEREIRA, Fábio Queiroz. **Smart Contracts: Conceitos, limitações e potencialidades**. 2022. 1–139 f. Dissertação (Mestrado em Direito) - Universidade Federal de Minas Gerais, Belo Horizonte, 2022.

SÃO PAULO. TRIBUNAL REGIONAL DE SÃO PAULO. **Agravo de Instrumento nº 2237253-77.2018.8.26.0000**. Tribunal de Justiça do Estado de São Paulo, Relatora: Fernanda Gomes Camacho, 2018.

SÃO PAULO. **Apelação Cível 1001795-79.2024.8.26.0035**. Tribunal de Justiça do Estado de São Paulo, Relatora: Léa Duarte, 2025.

SHARMA, Pratima; JINDAL, Rajni; BORAH, Malaya Dutta. Blockchain-based distributed application for multimedia system using Hyperledger Fabric. **Multimedia Tools and Applications**, v. 83, n.1, p. 2473–2499, 2024.

SILVA, Davi Antônio Araújo; AGUIAR, Alexandre Kehrig Veronese. **Blockchain, Confiança e Direito: um pouco além do alarde**. 2019. Monografia (Graduação em Direito) - Universidade de Brasília, Brasília, 2019.

SILVA, Jonas Gabriel Borges da; COUTINHO, Diógenes José Gusmão. Smart Contracts: o potencial para reduzir a litigiosidade e a burocracia no Brasil. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, v. 11, n.3, p. 2205–2221, 2025.

WALCH, Angela. Deconstructing “Decentralization”. In: CRYPTOASSETS. Oxford: Oxford University Press New York, 2019. p. 39–68. Disponível em: <https://academic.oup.com/book/35207/chapter/299660206>.

WRONKA, Christoph. Crypto-asset activities and markets in the European Union: issues, challenges and considerations for regulation, supervision and oversight. **Journal of Banking Regulation**, v. 25, n. 1, p.84-93, 2024.