


## DESAFIOS DOS *SMART CONTRACTS* NA ERA DA COMPUTAÇÃO QUÂNTICA: UMA ANÁLISE SOBRE A SEGURANÇA DO BLOCKCHAIN

 <https://doi.org/10.56238/sevened2024.037-018>

**Luani Maria de Albuquerque Macário**

Doutora em Ciências Sociais e Jurídicas pela Universidade Del Museo Argentino, 2019; Pós-graduação em EAD pela Faculdade de Jacarepaguá/RJ; DOCÊNCIA: Faculdade Raimundo Marinho, Faculdade Mauricio de Nassau, Faculdade Fama, Período: 2007 a 2017; POLÍCIA Militar de Alagoas, Bombeiros de Alagoas, Período de 2007 a 2022; Ministério da Ciência e Tecnologia. Coordenação de Bens Sensíveis; Trabalho com a ONU Segurança Antiterrorismo. Armas-químicas, Biológicas, Nuclear; Direito Internacional, braço da Casa Civil. Trabalho Considerado Paramilitar, Período: 2001 a 2006.

**Marielli Melo Soares de Morais**

Editora-chefe da Revista de Legal Design & Visual Law; Consultora de Compliance em Privacidade e Proteção de Dados; Membro da Associação Nacional de Compliance (ANACO) e do Comitê de Privacidade e Proteção de Dados; Engenheira de Prompt para Cibersegurança pelo IBSEC; Integrante dos Laboratórios: Comunidade de Estudos LGPD (Facilitadora) e Pesquisadora em Legal Design do Laboratório de Direitos Digitais da Universidade Federal da Bahia (LabiD<sup>2</sup>-UFBA); Pesquisadora do Grupo de Tecnologia e de pesquisa em Inteligência Artificial e Direito da Comissão de Tecnologia, Inovação e Proteção de Dados (CITPD) e da OAB/AL em parceria com a Escola Superior de Advocacia de Alagoas (ESA/AL); Mestranda Profissional em Direito, Justiça e Desenvolvimento pelo Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP-BSB); Pós-Graduada em Direito Internacional (CEDIN/ Milton Campos/BH-MG); Pós-Graduada em Direito Constitucional (IDP/UNISUL/LFG);  
E-mail: [mariellimelo@infodireitodigital.com.br](mailto:mariellimelo@infodireitodigital.com.br)  
LATTES: <http://lattes.cnpq.br/0389416055398926>  
ORCID: <https://orcid.org/0000-0002-4894-6642>

---

### RESUMO

Este estudo explora a interação entre contratos inteligentes e computação quântica, mapeando as principais vantagens, riscos e vulnerabilidades envolvidos, além de analisar destacar os benefícios da tecnologia *blockchain* e sua inserção no mundo jurídico brasileiro. Os contratos inteligentes são contratos programados em uma estrutura de *blockchain*, que não dependem de ações humanas para serem cumpridos. A utilização da *blockchain* no Direito possibilita o armazenamento de dados criptografados, dificultando a violação e alteração de informações. No entanto, a legislação brasileira ainda não normatizou o uso dessas técnicas. O artigo aborda as principais vantagens dos *smart contracts*, como a autonomia negocial, segurança de dados privados, eliminação de manipulação de dados, confiabilidade e agilidade. Propõe medidas para garantir a robustez dos contratos inteligentes e da *blockchain* diante do avanço iminente da computação quântica. A metodologia utilizada foi uma análise crítica, na qual objetiva-se propor medidas que assegurem a robustez dos contratos inteligentes e do *blockchain* frente à realidade iminente da computação quântica, por meio de uma revisão bibliográfica. A relevância desse trabalho está na necessidade de antecipar e mitigar potenciais ameaças, garantindo que essas inovações tecnológicas cumpram sua promessa de segurança e confiabilidade em uma sociedade cada vez mais digitalizada. Compreende-se que os *smart contracts* representam uma evolução na automatização dos contratos, com potencial para alterar a forma como as relações contratuais ocorrem no ordenamento jurídico, trazendo novos parâmetros para o direito.



**Palavras-chave:** Smart Contracts. Blockchain. Tecnologia. Computação Quântica. Ordenamento Jurídico.

## 1 INTRODUÇÃO

A contemporaneidade é caracterizada por uma profunda imersão tecnológica, onde avanços digitais permeiam e redefinem múltiplas esferas de nossa existência. Dentre esses avanços, os contratos inteligentes e a tecnologia *blockchain* destacam-se, prometendo transformações significativas em diversos setores, dada sua capacidade de proporcionar eficiência, transparência e segurança sem paralelo (BARON, Guilherme; HOPPE, Aurélio, 2018). Contudo, a evolução da computação quântica apresenta-se como um potencial desafio à integridade dessas tecnologias.

A literatura recente tem evidenciado a promissora sinergia entre contratos inteligentes e *blockchain*, ressaltando sua capacidade de automatizar e validar acordos de forma descentralizada. No entanto, a emergente computação quântica, com seu poder computacional superior, coloca em xeque a segurança dessas inovações (MACÁRIO, L. M. A., MORAIS, M. M. S. de, SILVA, M. A. X. da., 2022). Diante deste cenário, a presente pesquisa emerge como uma tentativa de compreender e antecipar os desafios inerentes a essa intersecção.

O propósito central deste estudo, é explorar a interação entre contratos inteligentes e computação quântica, mapeando os riscos e vulnerabilidades inerentes, além de analisar a tecnologia *Blockchain* e de qual forma ela está e pode ser inserida no mundo jurídico no âmbito brasileiro. Inicialmente, a tecnologia é conceituada e explicada de forma a qual venha a facilitar a compreensão de todo o estudo em torno da mesma. A *blockchain* é uma ferramenta poderosa a qual vem ganhando cada vez mais visibilidade, consiste em uma cadeia de blocos praticamente inalterável, onde registram-se diversas informações, armazenadas em cada um desses blocos e por todos os computadores que a ele acessam.

Os *smart contracts* (contratos inteligentes) são contratos com cláusulas programadas previamente em uma estrutura de *blockchain* que, uma vez pactuados, caracterizam-se por independem de ações humanas para serem cumpridos, gerando praticidade, transparência e confiança na celebração e na execução das avenças. O trabalho busca analisar a forma de recepção dos *smart contracts* pelo direito brasileiro, por meio da discussão travada na doutrina e jurisprudência acerca da natureza jurídica, da legislação aplicável e da casuística, com o intuito de apresentar e defender potenciais benefícios além de descrever riscos na adoção desse modelo.

O tema é importante e merece ser investigado, pois a *blockchain* possibilita o armazenamento de dados criptografados de modo a dificultar as possibilidades de violação e alteração de dados. Nesse sentido, notou-se a possibilidade da utilização da ferramenta no Direito, o que impulsionou o desenvolvimento de diversas iniciativas na área, como os *smart contracts*.

O conceito dos *smart contracts* foi originalmente pensado por Nick Szabo em 1996 que idealizou um protocolo de internet que ajudaria as partes a realizar contratos de maneira mais eficiente, a fim de impedir a não conformidade e tornar as possíveis violações contratuais autoexecutáveis.

Ao descompasso da tecnologia está a legislação brasileira, que deixou de acompanhar tal avanço e, até o presente momento, não normatizou a utilização dessas novas técnicas. Isto, contudo, não as impediu de serem utilizadas. Nesse contexto, vê-se a necessidade de adaptação dos operadores do direito a tais tecnologias, bem como a regulamentação dos smart contracts no Brasil.

Por isso, o artigo pretende abordar as principais vantagens da tecnologia dos smart contracts, utilizando-se de tecnologias de *Blockchain* e, incluindo, mas não se limitando a autonomia negocial sem intervenção de terceiros, e, conseqüentemente segurança de dados privados e a eliminação de uma possível manipulação de dados; confiabilidade, pois os documentos estão sob uma linguagem computacional que confere certeza e segurança; agilidade, devido a autoexecutibilidade dos *smart contracts*; economia, permitindo e facilitando uma maior liberdade negocial, uma vez que minimiza a insegurança jurídica devido a autoexecutibilidade por meio da computação quântica.

Através de uma análise crítica, objetiva-se propor medidas que assegurem a robustez dos contratos inteligentes e do blockchain frente à realidade iminente da computação quântica, por meio de uma revisão bibliográfica. A relevância deste trabalho reside na imperativa necessidade de antecipar e mitigar potenciais ameaças, garantindo que tais inovações tecnológicas mantenham sua promessa de segurança e confiabilidade em uma sociedade cada vez mais digitalizada (FEDOROV, A. K.; KIKTENKO, E. O.; LVOVSKY, A. I., 2018).

## **2 BLOCKCHAIN E SMART CONTRACTS**

Entende-se que o *blockchain* e os *Smart Contracts* têm uma grande importância no campo do direito. Essas tecnologias visam oferecer uma série de benefícios, como transparência, segurança e automatização de processos, que podem ser aplicados em diversas áreas do direito.

No ramo do direito, a utilização de contratos inteligentes baseados em *blockchain* permite a execução automática e imutável de acordos, eliminando a necessidade de intermediários e reduzindo o risco de fraudes ou disputas. Isso traz maior segurança jurídica e eficiência para as transações.

Compreende-se a *blockchain* também pode ser utilizada para registrar e autenticar documentos, garantindo sua integridade e autenticidade. Isso é especialmente notório em áreas como propriedade intelectual, registros públicos e contratos comerciais.

No campo da governança e *compliance*, a *blockchain* pode ser utilizada para criar registros imutáveis de transações, garantindo a transparência e a rastreabilidade de atividades. Isso é particularmente útil em setores regulados, como financeiro e saúde, onde é necessário comprovar a conformidade com normas e regulamentos.

A *blockchain* e os contratos inteligentes têm um papel preciso no direito, proporcionando maior segurança, eficiência e transparência para as transações e processos legais. Sua adoção está cada vez mais presente e promete transformar a forma como lidamos com questões jurídicas.

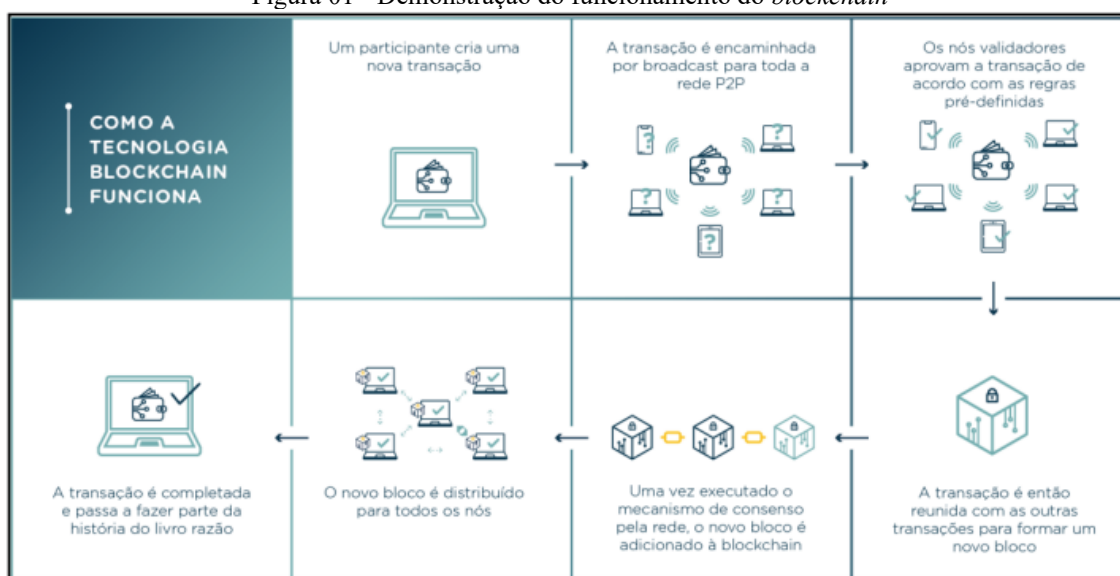
## 2.1 BLOCKCHAIN

A origem da *blockchain* está no protocolo do Bitcoin, descrito em um artigo publicado por Satoshi Nakamoto (Nakamoto, 2008), que entrou em operação em 2009. Conforme menciona Bashir (2017), esse artigo propôs uma nova inovação de rede ponto a ponto (P2P) em que um servidor, conhecido como minerador, recebe transações com a moeda digital bitcoin e, por meio de um protocolo de consenso bizantino baseado em desafios criptográficos, determina a ordem das transações.

A *blockchain* é uma tecnologia da informação emergente e revolucionária que oferece suporte distribuído, confiável, descentralizado e seguro para transações entre participantes de uma rede, com base no consenso entre eles e assegurado por um algoritmo de prova de trabalho (*Proof-of-work*), cujo objetivo principal é prevenir ataques à rede (CHICARINO, JESUS, ALBUQUERQUE e ROCHA, 2017). Compreende-se que a cadeia de nós pode ser atualizada por qualquer participante da rede ponto a ponto (P2P).

A capacidade da *blockchain* de criar registros confiáveis e imutáveis a torna notória e adequada para áreas que exigem alta segurança e integridade dos dados. Isso é possível graças ao uso de criptografia, permitindo que cada participante processe com segurança o livro-razão ou registro digital de informações, conhecido como *ledger*. Uma vez que um bloco de dados é adicionado à *blockchain*, é praticamente impossível alterá-lo ou excluí-lo. Com isso, cada transação é registrada em blocos interligados, formando uma cadeia de blocos (*blockchain*) que pode ser visualizada por todos os participantes da rede. Por meio desse sistema as transações são visíveis e acessíveis a qualquer pessoa autorizada, promovendo um alto nível de transparência e prestação de contas (ABIJAUDE, GREVE e SOBEIRA, 2021).

Figura 01 - Demonstração do funcionamento do *blockchain*



Fonte: Brasil (2020).

Conforme é demonstrado na figura 01, todos os participantes da rede podem concordar sobre o conjunto e a ordem de execução das transações por meio do consenso bizantino, que permite a ação contra nós maliciosos que poderiam danificar o sistema. O consenso é um elemento essencial para o desenvolvimento de um sistema confiável e seguro, pois permite que os participantes concordem sobre as operações a serem realizadas para manter a consistência do sistema e torná-lo contínuo (ALCHIERI, TOMALIN, BESSANI e FRAGA, 2011).

Além disso, a segurança e a privacidade dos dados são questões importantes que precisam ser abordadas para garantir a confiança do usuário e a conformidade regulatória (ALECRIM, 2019). A evolução do projeto da blockchain pode ser dividida em três fases, conforme destacado por Swan (2015, citado por BASHIR, 2017):

*A Blockchain 1.0, que envolveu o lançamento do Bitcoin em 2008, com as primeiras implementações de criptomoedas e um ecossistema de aplicações e pagamentos com ativos digitais; a Blockchain 2.0, que começou com a proposta inovadora dos contratos inteligentes em 2013, após a criação do projeto Ethereum, idealizado por Vitalik Buterin, e as diversas aplicações financeiras possíveis; e a Blockchain 3.0, que caracteriza a adoção da tecnologia blockchain em benefício de aplicações em diversas áreas além da financeira, como governo, comércio, artes, saúde, cidades digitais (BASHIR, 2017).*

A criptografia é usada para garantir a autorização, autenticidade, integridade da transação e requisitos de segurança de todo o sistema. É possível realizar transações financeiras sem a necessidade de intermediários, como bancos, de forma rápida, segura e sem fronteiras. A descentralização da *blockchain* permite que os usuários tenham controle total sobre suas transações e dados financeiros, promovendo a inclusão financeira e a autonomia individual. Essas transações são executadas e armazenadas permanentemente em uma cadeia de blocos (*blockchain*) e replicadas em cada servidor (CHICARINO, JESUS, ALBUQUERQUE e ROCHA, 2017).

## 2.2 SMART CONTRACTS

De acordo com Savelyev (2017), o termo “*Smart Contracts*” ou contratos inteligentes foi mencionado pela primeira vez no ano de 1995, por Nick Szabo, que é um pesquisador e jurídico na área da criptografia, como princípio a ideia central era contribuir na implementação de práticas de contrato jurista e de comércio na internet. Segundo o autor, embora o termo tenha sido definido em teoria, não havia uma infraestrutura computacional que pudesse ser utilizada para realizar o seu desenvolvimento (SAVELYEV, 2017).

De acordo com Alecrim (2019), os contratos inteligentes são constituídos em programas computacionais autônomos que controlam e executam de modo automático ações quando certas condições predefinidas são atendidas. Desse modo, os smart contracts foram projetados para conceber a facilitação, verificação e cumprir de modo satisfatório a negociação ou negociação de acordos entre partes sem a necessidade de intermediários tradicionais, diante desse cenário são considerados uma

inovação dos contratos tradicionais, incorporando a lógica computacional e a automação para que se tenha a execução confiável e imparcialidade das cláusulas acordadas (ALECRIM, 2019).

Compreende-se que os *Smart Contracts* são sistemas que movem ativos digitais de modo automático com regras pré-especificadas, assim esses contratos são desenvolvidos e escritos em linguagem de alto nível, o contrato será executado somente quando uma transação for acionada, na qual um contrato pode acionar outro e assim sucessivamente, até certo ponto de acordo com o que foi pré-definido, onde o primeiro contrato dessa cadeia de execução será chamado pela transação de um usuário (Ølnes et al., 2017).

Outro aspecto que cabe destacar é a segurança e transparência dos smart contracts é que além da imutabilidade e automatização, a segurança é uma característica fundamental dos smart contracts, pois são protegidos por criptografia avançada e incorporam mecanismos para garantir a autenticidade e a integridade das transações. Linguagens de programação como a já falada anteriormente, a Solidity, são uma das utilizadas na criação dos contratos inteligentes

Abijaude, Greve e Sobeira (2021) destacaram outro aspecto importante dos smart contracts, na qual a segurança e transparência são características precisas. Além da imutabilidade e automatização, a segurança é uma característica fundamental dos smart contracts, protegidos por criptografia avançada e incorporando mecanismos para garantir a autenticidade e integridade das transações, as linguagens de programação como a *Solidity* são amplamente utilizadas na criação dos contratos inteligentes.

### 2.3 A INTERSEÇÃO ENTRE *SMART CONTRACTS* E *BLOCKCHAIN*

Compreende-se que a interseção entre *Smart Contracts* e *Blockchain* traz consigo importantes implicações para o campo jurídico. Os *Smart Contracts*, que são contratos digitais autoexecutáveis baseados em código, oferecem a oportunidade de automatizar e agilizar processos legais, eliminando intermediários e reduzindo custos. Por sua vez, a tecnologia *Blockchain* assegura a segurança, transparência e imutabilidade das transações, o que pode ser especialmente relevante em questões contratuais.

A tecnologia *blockchain* e os contratos inteligentes são duas inovações revolucionárias que estão transformando a maneira como as transações são realizadas. *Blockchain* e os contratos inteligentes formam a base de muitos projetos de criptomoedas, bem como de várias outras aplicações em setores como finanças, imóveis, saúde e governança e jurídico. É importante ressaltar que os contratos inteligentes não se limitam apenas a documentos legais, mas abrangem o conceito de contrato de modo holístico, conforme ensinado por Tartuce (2020):

Os contratos são, em resumo todos os tipos de acordos ou estipulações que podem ser criados por meio do acordo de vontades e outros fatores acessórios. Em uma visão clássica ou moderna, o

contrato pode ser definido como um negócio jurídico bilateral ou plurilateral que visa criar, modificar ou extinguir direitos e deveres de natureza patrimonial (TARTUCE, 2020).

De acordo com Soares (2022), essa tecnologia tem sido amplamente utilizada na criação dos mencionados contratos inteligentes, que são contratos digitais autoexecutáveis que usam programação pré-definida para automatizar a execução de termos e condições acordados entre as partes envolvidas em uma transação. A *blockchain* oferece um ambiente seguro, transparente e descentralizado para a criação e execução desses contratos inteligentes.

Uma das maiores vantagens dos contratos inteligentes é a automação da execução de um acordo sem a intervenção humana. Isso traz benefícios como redução de custos, aumento da segurança e confiança para as partes envolvidas e para o mercado, além de diminuir as chances de fraudes decorrentes do comportamento humano (SOARES, 2022).

Fachini (2023), menciona que além de serem autoexecutáveis e permitirem a autogestão de suas cláusulas de forma automática, sem a necessidade de terceiros, esses contratos podem ser usados para automatizar a execução de termos e condições acordados entre as partes envolvidas em uma transação.

Na prática, quando corretamente codificado, o programa que serve de base para o contrato inteligente tem a capacidade de tomar ações e executar as cláusulas do contrato. Isso é chamado de inteligência de programação. Destaca-se que a execução dessas cláusulas pode não ser imediata. Em muitos casos, o contrato inteligente é reativo, ou seja, o ser humano precisa solicitar a execução de uma cláusula específica. No entanto, isso não diminui a "inteligência" do contrato inteligente, uma vez que a execução automatizada respeita as condições estabelecidas no contrato. Diante disso, o programa só executa a ação se todas as condições previstas estiverem completamente satisfeitas (FACHINI, 2023).

Por ser um contrato armazenado em um bloco de código na *blockchain*, como mencionado anteriormente, os códigos armazenados nos blocos dessa tecnologia, que funcionam como um livro-razão, são praticamente impossíveis de serem alterados. Portanto, o contrato inteligente não pode ser alterado sem o consentimento mútuo das partes envolvidas.

Um exemplo de contrato inteligente, relatado pela Equipe TD (2023), é quando uma empresa faz um pedido de material a um fornecedor e formaliza a relação com um contrato inteligente. Quando os produtos são entregues, o contrato recebe essa informação e libera automaticamente o pagamento, sem a necessidade de envio de fatura ou envolvimento de profissionais do setor financeiro. Os contratos inteligentes permitem que as partes tenham total liberdade para negociar e concordar com seus próprios termos, criando cláusulas que protegem seus interesses (EQUIPE TD, 2023).

Os contratos inteligentes podem ser usados em uma ampla variedade de aplicações, como no ramo jurídico, gestão de identidade, gestão de propriedades, permitindo que as partes envolvidas em





uma transação estabeleçam acordos de forma confiável e transparente, sem a necessidade de intermediários ou custos adicionais. Embora ainda não sejam amplamente utilizados, os contratos inteligentes são considerados grandes impulsionadores no avanço da tecnologia *blockchain*, que está ganhando cada vez mais espaço em diversos países. Espera-se, portanto, um aumento significativo no uso dessa ferramenta, especialmente no Brasil.

A utilização dos contratos inteligentes traz benefícios significativos para as partes envolvidas em uma transação. Além da automação e da redução de custos, eles proporcionam maior segurança e confiança, uma vez que todas as cláusulas e condições são programadas e executadas de forma imparcial e transparente. Isso elimina a necessidade de intermediários e reduz os riscos de fraude ou manipulação.

Outra vantagem dos contratos inteligentes é a flexibilidade que eles oferecem. As partes têm total liberdade para negociar e estabelecer seus próprios termos, criando cláusulas personalizadas que atendam aos seus interesses específicos. Isso permite uma maior agilidade e eficiência nas transações, eliminando a necessidade de longos processos burocráticos e negociações complexas.

No entanto, é importante destacar que, apesar de todas as vantagens, os contratos inteligentes também apresentam desafios e limitações. A programação e a codificação corretas são fundamentais para garantir a eficácia e a segurança desses contratos. Além disso, a adoção em larga escala ainda enfrenta obstáculos regulatórios e de aceitação por parte das instituições e do mercado.

Desse modo, os contratos inteligentes são uma inovação promissora que está transformando a forma como as transações são realizadas. Com a combinação da tecnologia *blockchain* e da automação programada, eles oferecem segurança, transparência e eficiência para as partes envolvidas. Embora ainda haja desafios a serem superados, espera-se que o uso dos contratos inteligentes se torne cada vez mais comum, impulsionando o avanço da *blockchain* e trazendo benefícios significativos para diversos setores como no ramo jurídico.

No entanto, a aplicação dos *Smart Contracts* e da *Blockchain* no âmbito jurídico também apresenta desafios, como a necessidade de adaptar a legislação existente, garantir a validade jurídica dos contratos digitais e lidar com questões relacionadas à privacidade e proteção de dados. Diante desse contexto, é essencial que os profissionais do direito compreendam as implicações dessa convergência e estejam preparados para enfrentar as mudanças e aproveitar as oportunidades que surgem com essa tecnologia emergente.

### **3 A ERA DA COMPUTAÇÃO QUÂNTICA**

#### **3.1 VISÃO GERAL DA COMPUTAÇÃO QUÂNTICA**

Compreende-se que as primeiras ideias para um computador baseado em princípios da mecânica quântica surgiram nos anos 80, e desde então a pesquisa na área da computação quântica tem

se intensificado, atraindo cada vez mais a atenção do setor tecnológico e industrial. Os computadores quânticos se diferenciam da computação convencional ao aplicarem conceitos da Matemática, Física e computação na prática (NICOLAU, 2010).

De acordo com Mattiello, Silva, Amorim e Silva (2012, p.1), o campo da computação e informação quântica tem sido revolucionário ao considerar que avanços na mecânica quântica e na Ciência da Computação têm modificado o estilo de vida moderno em diversos aspectos. A computação clássica já evoluiu o suficiente para mostrar a quão significativa foi sua influência na sociedade atual. É de se esperar que a comercialização em larga escala de computadores quânticos traga ainda mais revoluções, juntamente com as descobertas que surgirão das novas pesquisas utilizando essa tecnologia que lida com problemas em escala atômica.

Mello (2018), menciona que o aprimoramento dos sistemas quânticos poderá transformar outras áreas de pesquisa, pois possibilita a resolução de operações altamente complexas, como interações moleculares e químicas, resultando na descoberta de novas estruturas para auxiliar na criação de novos materiais e medicamentos. Além disso, permitiria cadeias de logística e abastecimento extremamente eficientes, ajudando a encontrar novas maneiras de modelar dados financeiros e isolar os principais fatores de risco para realizar investimentos melhores.

Segundo Jack D. Hidary (2021), os avanços recentes nas tecnologias quânticas possibilitaram o uso de computadores quânticos, sensores quânticos e redes específicas, como a Distribuição de Chaves Quânticas (QKD - Quantum Key Distribution). De acordo com Hidary (2021, p.15), a computação quântica começou a se destacar como um campo de estudo próprio por volta de 1979.

### 3.2 A REVOLUÇÃO TECNOLÓGICA DA COMPUTAÇÃO QUÂNTICA

Em um artigo publicado por Mozelli (2023), é apresentado que físicos deram o primeiro passo em direção à construção de computadores quânticos a partir de moléculas individuais presas a dispositivos a laser chamados pinças ópticas.

De acordo com Mozelli (2023), segundo a *Nature*, dois grupos de cientistas relataram seus resultados na Science em 07 de dezembro de 2023, em ambos os casos fazendo pares de moléculas de monofluoreto de cálcio interagirem de forma que ficassem entrelaçada, efeito fundamental para a computação quântica. Diante desses fatores, essas descobertas são consideradas marco importante, pois abrem caminho para aproveitar estados entrelaçados e melhorar as aplicações potenciais de matrizes de pinças moleculares. Essa abordagem utiliza moléculas como qubits, unidades fundamentais da informação quântica, em vez de átomos ou íons como em outras plataformas de computação quântica.

Conforme menciona Mozelli (2023), os experimentos envolveram o uso de pinças ópticas para prender moléculas de monofluoreto de cálcio individualmente em cada unidade de pinça. As moléculas



foram resfriadas a temperaturas próximas do zero absoluto, fazendo com que ficassem praticamente imóveis. Esta técnica permitiu aos cientistas manipular o estado de rotação dessas moléculas para representar os estados “0” e “1” dos qubits.

Esses avanços também podem contribuir para o uso de moléculas presas para medidas de alta precisão que poderiam revelar a existência de novas partículas elementares. Os pesquisadores destacam a rapidez com que o campo da computação quântica tem avançado e afirmam que as moléculas serão base de plataforma competitiva capaz de realizar simulações quânticas. Essas descobertas representam avanço significativo na construção de computadores quânticos utilizando moléculas individuais presas a pinças ópticas (MOZELLI, 2023).

Além de abrir caminho para nova abordagem na computação quântica, esses estudos possibilitam a manipulação de informações quânticas utilizando “qutrits” e oferecem oportunidade de simular materiais complexos e forças fundamentais da física de forma mais precisa. Com novas possibilidades de medir partículas elementares, espera-se que essa tecnologia revolucione a ciência e a computação no futuro próximo (MOZELLI, 2023).

Ao unir a ciência da computação e a física quântica, esse campo busca desenvolver sistemas computacionais extremamente sofisticados, que vão além dos modelos atualmente estabelecidos e amplamente utilizados. Esses sistemas, que são consideravelmente mais eficientes do que os computadores clássicos que usam bits “0” e “1”, marcam uma revolução no processamento e gerenciamento de informações, introduzindo uma nova era na computação (HIDARY, 2021).

### 3.3 COMPUTAÇÃO QUÂNTICA X SEGURANÇA DIGITAL

Os computadores quânticos estão presentes em universidades de pesquisa, órgãos governamentais e empresas científicas líderes e, em geral, estão fora do alcance de indivíduos mal-intencionados. No entanto, essa nem sempre é a realidade (HATTAR, 2023).

À medida que a pesquisa sobre computação quântica continua avançando, surge uma preocupação crescente de que esses computadores possam, em breve, quebrar a criptografia moderna. Isso tornaria obsoletos todos os métodos atuais de criptografia de dados e exigiria o desenvolvimento de novos métodos de criptografia para proteção contra essas máquinas poderosas (HATTAR, 2023).

Embora o conceito de computadores quânticos não seja novo, o debate em torno deles aumentou nos últimos meses, graças às ações governamentais contínuas. Em maio de 2022, o presidente Biden divulgou um memorando de segurança nacional que delineava os esforços do governo para antecipar as preocupações de segurança relacionadas à computação quântica (HATTAR, 2023). Em junho, a Câmara dos Representantes dos EUA aprovou a Lei de Preparação para Segurança Cibernética de Computação Quântica, exigindo que as agências federais migrassem seus sistemas de tecnologia da informação para criptografia pós-quântica.



Essa legislação que ainda precisa ser aprovada pelo Senado dos EUA, baseia-se nos esforços contínuos do Instituto Nacional de Padrões e Tecnologia (NIST) para desenvolver padrões de criptografia pós-quântica. Em julho de 2022, o NIST lançou seus primeiros quatro algoritmos à prova de ataques quânticos. Pouco tempo depois, o algoritmo de criptografia de chave pública e encapsulamento de chave CRYSTALS-Kyber, recomendado pelo NIST, foi quebrado usando inteligência artificial combinada com ataques de canal lateral.

Mesmo os computadores mais rápidos de hoje têm dificuldade em quebrar as chaves de segurança devido à sua complexidade. Levaria anos para um sistema conseguir quebrar as chaves padrão, mesmo nas melhores circunstâncias. É isso que torna a criptografia uma defesa de segurança tão valiosa (HATTAR, 2023).

A computação quântica parece mudar drasticamente esse cenário, reduzindo o tempo necessário de anos para algumas horas. Embora a situação possa se complicar rapidamente, especialistas acreditam que muitos métodos populares de criptografia de chave pública hoje, como RSA, Diffie-Hellman e curva elíptica, poderão ser relativamente fáceis de serem resolvidos por computadores quânticos no futuro (HATTAR, 2023).

Embora os ataques baseados em computação quântica ainda estejam no futuro, as organizações devem pensar em como proteger os dados em trânsito quando a criptografia não for mais eficaz. As melhores práticas incluem a segmentação de redes, o aproveitamento de redes privadas 5G e a adoção de arquiteturas de confiança zero (HATTAR, 2023).

A preocupação crescente com ataques cibernéticos relacionados à tecnologia quântica pode não ser iminente, mas também não é infundada. Os profissionais de segurança cibernética devem permanecer ágeis diante de novas ameaças e mudanças de paradigma. À medida que avançamos para esse próximo desafio, devemos nos manter em uma base sólida.

A autora menciona que estamos caminhando em direção a um futuro com computação quântica, portanto, é importante preparar sua organização agora para essa ameaça emergente, além de lidar com outras ameaças que afetam sua empresa atualmente. Uma abordagem de defesa profunda atua como uma proteção contra diferentes vetores de ataque. Ela fornece às organizações uma cobertura abrangente e uma defesa robusta contra vários tipos de ataques (HATTAR, 2023).

## **4 DESAFIOS PARA CONTRATOS INTELIGENTES NA ERA DA COMPUTAÇÃO QUÂNTICA**

### **4.1 VANTAGENS RISCOS E VULNERABILIDADES DOS *SMART CONTRACTS***

De acordo com Cavalcanti (2020), os *smart contracts* são considerados um instrumento contratual relativamente novo no sistema jurídico, e todas as suas possíveis aplicações ainda estão longe de serem totalmente reveladas, principalmente porque a tecnologia blockchain está em constante

evolução. Com essa tecnologia, há um potencial de ganho de velocidade, praticidade, segurança e efetividade no cotidiano jurídico, pois os smart contracts permitem a execução automática de acordos judiciais e sentenças.

Pereira (2014), menciona que um contrato é uma transação jurídica bilateral que requer consentimento. Ele deve estar em conformidade com os requisitos legais e, como um ato negociável, tem como objetivo alcançar objetivos específicos. Segundo o autor, um contrato é "um acordo de vontades, em conformidade com a lei, com o propósito de adquirir, proteger, transferir, preservar, modificar ou extinguir direitos" ou, em outras palavras, "um acordo de vontades com o propósito de produzir efeitos jurídicos".

Diniz (2014), por sua vez, afirma que um contrato é "um acordo entre duas ou mais vontades, em conformidade com a ordem jurídica, com o objetivo de estabelecer uma regulamentação de interesses entre as partes, com o propósito de adquirir, modificar ou extinguir relações jurídicas de natureza patrimonial".

De acordo com Coelho (2016), um contrato é definido como uma transação jurídica bilateral ou multilateral que gera obrigações para uma ou todas as partes envolvidas, correspondendo a direitos detidos por elas ou por terceiros. Portanto, não há contrato sem a intenção característica das transações jurídicas, pois a conduta humana intencional contida no contrato é a declaração de uma vontade.

Em geral, a legislação brasileira não impõe uma forma específica para a celebração de acordos. Surge da teoria geral dos contratos e do artigo 107 do Código Civil que só haverá uma forma específica para um contrato quando a lei expressamente o prever. Assim, desde que haja acordo mútuo e não viole a ordem pública, as partes têm liberdade para elaborar contratos, inclusive utilizando linguagem de programação (USTER, 2021).

Por sua vez, os tribunais brasileiros reconhecem a importância dos contratos eletrônicos e, em particular, dos smart contracts, como pode ser observado em uma decisão recente do Tribunal de Justiça do Estado de São Paulo:

É importante ressaltar que as tecnologias que envolvem os smart contracts e os contratos eletrônicos, apesar da modernidade que trazem e da necessidade de uma nova interpretação dessas relações jurídicas a cada dia, não implicam em um afastamento dos conceitos fundamentais do Direito Privado. Questões atuais, que estão cada vez mais transformadas devido à Sociedade da Comunicação, são os desafios que o Direito e a Jurisprudência precisam superar para não ficarem para trás (TRT-9ª Região).

Por essas razões, é possível reconhecer a aceitação dos smart contracts pelo ordenamento jurídico brasileiro como uma nova forma de realizar uma transação jurídica bilateral, sempre em conformidade com a teoria geral dos contratos e as normas reguladoras.

Portanto, existem pontos positivos e negativos na adoção dos *smart contracts* que contribuem para o debate e evolução do tema. Entre os atrativos significativos estão a eficiência gerada pela

conclusão e execução instantânea do contrato sem a necessidade de intervenção estatal; a garantia de cumprimento representada pela impossibilidade de uma das partes deixar de cumprir suas obrigações; a redução de disputas devido à queda na inadimplência; a facilitação do comércio eletrônico pela eliminação do terceiro de confiança na cadeia de negócios; a segurança proporcionada pelo alto grau de precisão em relação à identidade do contratante à distância (preservando o anonimato); e o potencial dos smart contracts e da blockchain para revolucionar a Internet das Coisas.

Por outro lado, entre os desafios e riscos da adoção dos *smart contracts* estão a integração de toda a sociedade no ambiente digital; a possibilidade de falha no algoritmo de codificação (embora mínima); a impossibilidade de prever todas as circunstâncias possíveis, o que pode levar à execução contrária à vontade das partes; a má-fé na elaboração do script de programação; a execução diferida ou contínua de um *smart contract* pode ser afetada por alterações factuais ou legislativas; a impossibilidade, por meio da tecnologia atual, de resolver questões subjetivas que afetam a execução do contrato; estar sujeito aos mesmos defeitos de consentimento ou problemas de capacidade dos contratos tradicionais; restrição da atuação do Poder Judiciário e de seus órgãos auxiliares, resultando na perda do poder de tutela preventiva e na redução do poder de tutela reparatória (*status quo ante*).

#### 4.2 ESTRATÉGIAS DE MITIGAÇÃO

O ordenamento jurídico brasileiro pode adotar diversas estratégias de mitigação para lidar com os desafios e riscos associados aos *smart contracts*. Essas estratégias visam garantir a segurança jurídica e a efetividade desses contratos no contexto brasileiro.

Uma das estratégias é a atualização legislativa. O legislador pode promover a atualização das leis existentes para abordar especificamente os *smart contracts*, estabelecendo regras claras e adequadas para sua utilização. Isso pode incluir a definição legal de smart contracts, a determinação dos requisitos formais para sua validade e a regulamentação de questões específicas relacionadas à execução e resolução de disputas (Cavalcanti, 2020).

Além disso, os tribunais podem adotar uma interpretação flexível das leis existentes para acomodar os smart contracts. Isso implica em uma interpretação ampla dos conceitos legais existentes, de modo a abranger os smart contracts, bem como a aplicação de princípios gerais do direito para resolver questões específicas relacionadas a esses contratos (TRT-9ª Região).

O desenvolvimento de mecanismos alternativos de resolução de disputas específicos para os *smart contracts*. Considerando a natureza automatizada e autônoma desses contratos, pode ser necessário criar mecanismos de arbitragem ou mediação eletrônica, bem como tribunais especializados ou câmaras de resolução de disputas dedicadas aos smart contracts (Cavalcanti, 2020).

Cabe destacar que a cooperação internacional é fundamental. Dado que os *smart contracts* são uma tecnologia global, é importante promover a cooperação internacional para desenvolver padrões e



diretrizes comuns para sua utilização. Isso pode envolver a participação em fóruns internacionais, a troca de informações e experiências com outros países e a adoção de convenções ou tratados internacionais que abordem os smart contracts (Cavalcanti, 2020).

Essas estratégias, quando adotadas em conjunto, podem contribuir para mitigar os desafios e riscos associados aos *smart contracts* no ordenamento jurídico brasileiro. É importante ressaltar que a evolução tecnológica é constante, e o sistema jurídico deve estar preparado para se adaptar e acompanhar essas mudanças (Cavalcanti, 2020).

## 5 SEGURANÇA DO BLOCKCHAIN NA ERA DA COMPUTAÇÃO QUÂNTICA

### 5.1 A IMPORTÂNCIA DA SEGURANÇA DO BLOCKCHAIN

Compreende-se que a importância da utilização da *blockchain* no judiciário brasileiro ainda é limitada e está em fase experimental, não sendo adotada de forma ampla (ANDRIGHI, 2018). No entanto, já existem algumas iniciativas em andamento. Em 2018, o Tribunal de Justiça do Distrito Federal e Territórios (TJDFT) realizou um teste de registro de informações processuais em uma *blockchain* privada, visando verificar a eficácia da tecnologia nos processos judiciais e garantir a autenticidade das informações (ANDRIGHI, 2018).

No ano de 2022, o Tribunal de Justiça de Santa Catarina (TJSC) desenvolveu o aplicativo *LGPD JUS*, que utiliza a tecnologia *blockchain* para garantir a segurança das solicitações dos usuários ao validarem suas contas (PORTO, LIMA JÚNIOR e SILVA, 2019). Outro ponto que cabe destacar é que o Tribunal do Trabalho da 3ª Região (TRT-3) recomendou o uso da tecnologia *blockchain* para o registro de provas em um processo, e o TRT-2 reconheceu o registro de uma prova na *blockchain* como válido (GUSSON, 2020).

O Conselho Nacional de Justiça (CNJ) também lançou a plataforma "Justiça 4.0" em 2020, que permite o registro e a consulta descentralizada e segura de dados processuais. A plataforma está em fase de testes e será expandida para outros tribunais no futuro (ANDRIGHI, 2018).

No setor privado, o Cartório Azevedo Bastos, em parceria com a start-up *OriginalMy*, oferece o serviço de autenticação digital para pessoas jurídicas por meio de uma rede *blockchain* (PORTO, LIMA JÚNIOR e SILVA, 2019).

Apesar dessas iniciativas, ainda há muito a ser explorado em termos de potencial e impacto da tecnologia *blockchain* no setor jurídico brasileiro. É necessário investimento, desenvolvimento e compreensão do tema para que a *blockchain* possa ser amplamente adotada e utilizada como prova no judiciário brasileiro (BURATTO, 2022).



## 5.2 VULNERABILIDADES POTENCIAIS DE BLOCKCHAIN E ABORDAGENS PARA FORTALECER A SEGURANÇA NO JUDICIÁRIO

Quanto a vulnerabilidades potenciais de *Blockchain* e abordagens para fortalecer uma das principais vantagens é a maior possibilidade de intervenção do sistema judiciário para manter o equilíbrio dos contratos. Com a aplicação dos princípios modernos nos contratos, é necessário humanizar as relações contratuais e superar ideias ultrapassadas baseadas em convicções liberais, trazendo o interesse do Estado Social na regulamentação dos contratos. Isso envolve uma ponderação dos princípios, onde a intervenção estatal (função social do contrato) prevalece sobre a liberdade contratual (autonomia da vontade).

Diante das inúmeras demandas enfrentadas pelo Poder Judiciário, especialmente no Brasil, onde há uma grande demanda judicial, é válido considerar a implementação de tecnologias que possibilitem um melhor funcionamento do sistema judiciário, com foco na celeridade e no reforço dos princípios constitucionais relacionados, como a duração razoável do processo e a celeridade.

O Decreto nº 10.332 instituiu a Estratégia de Governança Digital, que é organizada por princípios, objetivos e iniciativas, e uma dessas iniciativas é o *blockchain*. O fato de o Governo Federal reconhecer a importância e os benefícios dessa tecnologia, planejando sua criação e implementação o mais rápido possível, demonstra sua relevância.

No mundo jurídico, não será diferente. O mencionado decreto, em seu Objetivo 8, que trata dos serviços públicos do futuro e das tecnologias emergentes, na iniciativa 8.3, prevê que o governo federal planeja disponibilizar conjuntos de dados por meio de soluções de *blockchain* na administração pública federal até 2022. Já na iniciativa 8.4 do mesmo objetivo, sobre a implementação de recursos para a criação de uma rede *blockchain* do Governo Federal que seja interoperável, com uso de identificação confiável e algoritmos seguros.

O Conselho Nacional de Justiça (CNJ) emitiu a Resolução nº 75/2009, que versa sobre concursos públicos para ingresso na magistratura. Em seu Anexo VI, letra F, aborda o Direito Digital, destacando a necessidade de noções gerais de contratos inteligentes, *blockchain* e algoritmos. Isso é apenas mais uma demonstração da relevância do *blockchain* nos tempos atuais e, conseqüentemente, no Direito. Dado o seu comprovado valor e as diversas áreas em que pode ser utilizada e aplicada, é necessário analisar sua aplicação de forma a incorporá-la em diferentes ramos do Direito, buscando viabilizá-la por meio de sua implementação.

## 5.3 CRESCIMENTO DAS INOVAÇÕES EM COMPUTAÇÃO QUÂNTICA, BLOCKCHAIN E CONTRATOS INTELIGENTES: UMA ANÁLISE BASEADA NAS DESCOBERTAS DE BARON E HOPPE (2018)

Cabe ressaltar que ao mergulharmos na intrincada relação entre computação quântica,



blockchain e contratos inteligentes, a análise no estudo revela implicações profundas dessas inovações. Apoiados nas descobertas de Baron e Hoppe (2018), destacou-se como os contratos inteligentes e a *blockchain* reformularam as práticas nas operações online, estabelecendo um novo paradigma para transações seguras e descentralizadas.

No entanto, ao investigarmos mais a fundo a computação quântica, torna-se evidente a emergência de desafios significativos que ameaçam a segurança dessas infraestruturas pioneiras (Kappert, Karger e Kureljusic, 2020). A rápida evolução da computação quântica representa uma ameaça concreta, exigindo respostas ágeis e proativas.

Nesse cenário, a criptografia quântica surge como uma nova ferramenta, propondo uma abordagem revolucionária para combater os riscos impostos pela computação quântica (Ilie, Knottenbelt e Stewart, 2020). Portanto, os métodos avançados oferecem uma camada extra de proteção, tornando-se indispensável à medida que nos aproximamos da era quântica.

Assim, as conclusões de nosso estudo (Macário, Morais e Silva, 2022) acendem um alerta sobre os desafios iminentes e a urgência de estratégias de segurança aprimoradas. O futuro das operações online reserva inúmeras possibilidades, mas é vital estarmos equipados para preservar a integridade dessas inovações frente às incertezas que se aproximam. Compreender o contexto atual e as alternativas disponíveis é fundamental para assegurar que os méritos da *blockchain* e dos contratos inteligentes não sejam obscurecidos pelo progresso da computação quântica.

Ao analisarmos o futuro, é relevante não apenas continuar, mas também expandir nossas pesquisas. Devemos explorar a robustez da criptografia quântica, compreender as implicações da computação quântica em estruturas como a blockchain e, além disso, investigar as potenciais vulnerabilidades dos contratos inteligentes, considerando novos métodos de proteção.

A atenção dedicada ao potencial da computação quântica e da tecnologia *blockchain* está crescendo a cada dia. No Brasil, já podemos observar iniciativas como o Programa e-Cidadania e propostas de novas leis, como o projeto de lei 1979/2022 e o 1458/2022. Essas ações demonstram um forte interesse em desenvolver regulamentações para essas tecnologias emergentes.

Nos Estados Unidos, leis como o *National Quantum Initiative Act of 2018* (S. 3143) e o *Quantum Computing Cybersecurity Preparedness Act of 2022* (H.R. 7535) foram aprovadas, despertando a curiosidade e incentivando estudos no campo da computação quântica, além de ressaltar a importância de proteger essas tecnologias.

A implementação dessas medidas legislativas reforça a necessidade de adotar uma abordagem preventiva e informada para garantir que inovações como a computação quântica e a tecnologia blockchain sejam utilizadas de maneira segura, eficiente e em conformidade com as diretrizes legais e regulatórias. É importante ressaltar que esse aumento do conhecimento não marca o fim de nossa jornada, mas sim o início de uma trajetória em que devemos nos aprofundar no universo dessas

tecnologias.

## 6 CONCLUSÃO

A tecnologia *Blockchain* tem o potencial de trazer inovações ao campo do Direito em diversas relações e situações. Ao longo deste artigo, foi demonstrado o impacto dessa tecnologia no âmbito jurídico, analisando suas vantagens e destacando a necessidade de explorar ainda mais suas aplicações e uso, especialmente diante dos desafios dos *smart contracts* na era da computação quântica, outro ponto foi a análise sobre a segurança do *blockchain* também foi realizada.

Pode-se afirmar que a *Blockchain* surge como uma tecnologia disruptiva, tornando desnecessária a presença de intermediários centrais para a concretização de operações. Com isso, os riscos associados à dependência de intermediários ou à sua ausência são suprimidos por esse sistema descentralizado, confiável e transparente, que vem ganhando destaque no mundo, como também no Brasil, no ordenamento jurídico.

A expansão da *Blockchain* é inevitável, uma vez que avançamos para um futuro cada vez mais interligado com a tecnologia. Ela funciona como um grande livro-razão globalizado, intrínseco ao desenvolvimento de novas relações, garantindo sua segurança e transparência, permitindo assim que o Direito possa ser operacionalizado de forma concisa nas relações digitais.

Por meio do estudo pode-se verificar que a viabilidade jurídica da celebração de *smart contracts* no ordenamento jurídico brasileiro, destacando sua natureza bilateral e a relação direta com o desenvolvimento da *blockchain*.

Os riscos e benefícios na adoção desse instrumento contratual também foram abordados, contribuindo para a compreensão do tema. Diante de tudo isso, é possível concluir que os *smart contracts* representam uma evolução na automatização das promessas contratuais, com potencial para alterar, em curto prazo, a forma como as relações contratuais ocorrem no ordenamento jurídico, trazendo novos parâmetros no direito.



## REFERÊNCIAS

ABIJAUDÊ, Jauberth Weyll; GREVE, Fabíola; SOBREIRA, Péricles de Lima. Blockchain e Contratos Inteligentes para Aplicações em IoT, Uma Abordagem Prática. In: ANDRADE, Aline M. S.; WAZLAWICK, Raul S. (Org.). 40ª Jornada de Atualização em Informática (JAI 2021). Porto Alegre: Sociedade Brasileira de Computação, 2021. p. 1-12. Disponível em: <https://doi.org/10.5753/sbc.6757.3.4>. Acesso em 14 de jan. de 2024.

ALCHIERI, Eduardo Adilio Pelinson; TOMELIN, Luiz Renato; BESSANI, Alysson Neves; FRAGA, Joni da Silva. Aspectos Práticos sobre o Consenso Bizantino entre Participantes Desconhecidos. In: Workshop de testes e tolerância a falhas (WTF), 12, 2011, Campo Grande/MS. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2011. p. 63-76. ISSN 2595-2684. Disponível em: <https://doi.org/10.5753/wtf.2011.23090>. Acesso em 13 de jan. de 2024.

ALECRIM, Jaqueline de Souza Cardoso. Análise crítica da sistemática de compras governamentais pela perspectiva de novas tecnologias de contratos inteligentes. Programa de Pós-Graduação Stricto Sensu em Gestão do Conhecimento e da Tecnologia da Informação. Brasília, 2019. Disponível em: <http://bdtd.ucb.br:8443/jspui/handle/tede/2655>. Acesso em 13 de jan. de 2024.

ANDRIGHI, F. N. Blockchain e o Poder Judiciário: uma análise sob a perspectiva da segurança jurídica. Revista de Direito, Estado e Telecomunicações, v. 12, n. 1, p. 609-624, 2018.

BASHIR, I. Mastering Blockchain: Distributed ledgers, decentralization and smart contracts explained. Packt Publishing, 2017.

BLOG TD SYNnex. 7 Principais mitos sobre Blockchain. Disponível em: <https://blog-pt.lac.tdsynnex.com/7-principais-mitos-sobre-blockchain>. Acesso em: 14 de jan. de 2024.

BOECHAT, G. Contratações abertas: uma análise da Nova Lei de Licitações e Contratos Administrativos (nº 13.133/2021) à luz dos princípios de Governo Aberto. Revista da CGU. [S.l.]. v. 14, n. 25. p. 64-79. Disponível em: DOI: 10.36428/revistadacgu.v14i25.493. Acesso em 13 de janeiro de 2024.

BRASIL. Tribunal de Contas da União. TCU realiza estudo inovador sobre a tecnologia Blockchain e elabora guia para orientar os gestores. 2020. Disponível em: <https://portal.tcu.gov.br/imprensa/noticias/tcu-realiza-estudo-inovador-sobre-a-tecnologia-blockchain-e-elabora-guia-para-orientar-os-gestores.htm>. Acesso em 13 de jan. de 2024.

BURATTO, R. Blockchain e o Poder Judiciário: uma análise sob a perspectiva da segurança jurídica. Revista de Direito, Estado e Telecomunicações, v. 12, n. 1, p. 643-658, 2022.

CAVALCANTI, Mariana Oliveira de Melo; NÓBREGA, Marcos. Smart contracts ou “contratos inteligentes”: o direito na era da blockchain. In: Revista Científica Disruptiva. Volume II, Número 1, 2020, p. 98.

CHICARINO, Vanessa R. L.; JESUS, Emanuel F., ALBUQUERQUE, Célio V. N., ROCHA, Antônio A. de A. Uso de blockchain para privacidade e segurança em internet das coisas. In: NUNES, Raul C., CANEDO, Edna D., SOUSA JÚNIOR, Rafael T. de. (Org.). XII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais - SBSeg 2017. Porto Alegre: Sociedade Brasileira de Computação, 2017. Disponível em: <https://sol.sbc.org.br/livros/index.php/sbc/catalog/view/84/370/634-1>. Acesso em 13 de jan. de 2024.



COELHO, Fábio Ulhoa. Curso de Direito Civil: Contratos, volume 3. São Paulo: Editora Revista dos Tribunais, 2016.

DINIZ, Maria Helena. Compêndio de Introdução à Ciência do Direito. 23. ed. São Paulo: SaraivaJus, 2014, p. 31.

ESTADOS UNIDOS. National Quantum Initiative Act of 2018. S. 3143. Disponível em: <https://www.congress.gov/bill/115th-congress/senate-bill/3143>. Acesso em: 18 out. 2023.

ESTADOS UNIDOS. Quantum Computing Cybersecurity Preparedness Act of 2022. H.R. 7535. Disponível em: <https://www.congress.gov/bill/117th-congress/house-bill/7535>. Acesso em: 18 out. 2023.

FACHINI, Tiago . Smart contracts: o que é, como funciona e aspectos legais. Disponível em: <https://www.projuris.com.br/blog/smart-contract/>. Acesso em 06 de março de 2023.

HIDARY, Jack D. Quantum computing: an applied approach. Second Edition. Cham: Springer, 2021.

Hattar, M. (30 de agosto de 2023). DATA PROTECTION: How Quantum Computing Will Impact Cybersecurity. Disponível em: <https://www.securityweek.com/how-quantum-computing-will-impact-cybersecurity/>. Acesso em 10 de jan. de 2023.

GUSSON, L. A. Smart Contracts: Uma Análise Jurídica. Revista de Direito, Estado e Telecomunicações, v. 12, n. 1, p. 1-20, 2020.

MACÁRIO, L. M. A., Morais, M. M. S. de, Silva, M. A. X. da. (2022). O advento da computação quântica e seus riscos para o paradigma blockchain/smart contracts. In: Pensando as novas tecnologias, organizado por Maria do Carmo Boaventura Motta e Mariana de Almeida Motta Rezende (p. 15-32). Deerfield Beach, Florida: Pembroke Collins.

MACÁRIO, L. M. A., Morais, M. M. S. de, Silva, M. A. X. da. (2022). O advento da computação quântica e seus riscos para o paradigma blockchain/smart contracts. In: Pensando as novas tecnologias, organizado por Maria do Carmo Boaventura Motta e Mariana de Almeida Motta Rezende (p. 15-32). Deerfield Beach, Florida: Pembroke Collins.

MATTIELO, F., SILVA, G.G., AMORIM, R.G., SILVA, W.B., 2012, “Decifrando a Computação Quântica”, Caderno de Física da Universidade Estadual de Feira de Santana (UEFS) 10 (01 e 02) – Bahia.

MELLO, U., “Como a Computação Quântica Promete Revolucionar Nosso Conhecimento”, Disponível em: <http://idgnow.com.br/ti-corporativa/2018/05/06/como-a-computacao-quantica-promete-revolucionar-nosso-conhecimento/>. Acesso em: 15 de jan. de 2024.

MOZELLI, R. (08/12/2023). Cientistas dão primeiro passo rumo a computadores quânticos moleculares. Disponível em: <https://olhardigital.com.br/2023/12/08/pro/cientistas-dao-primeiro-passo-rumo-a-computadores-quanticos-moleculares/>. Acesso em 12 de jan. de 2024.

NAKAMOTO, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Technical report, Bitcoin Org. <https://bitcoin.org/bitcoin.pdf> . Acesso em: 14 de jan. de 2024.

NICOLAU, A.S., 2010, “Computação Quântica e Inteligência de Enxames Aplicados na Identificação de Acidentes de uma Usina Nuclear PWR”, Dissertação de Mestrado em Ciências em Engenharia Nuclear, COPPE, Universidade Federal do Rio de Janeiro (UFRJ) – Rio de Janeiro.



ØLNES, S. et al. Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. *Government Information Quarterly*, v. 34, n. 3, p. 355-364, sep. 2017. Disponível em: <https://doi.org/10.1016/j.giq.2017.09.007>. Acesso em: 14 de jan. de 2024.

PEREIRA, Caio Mário da Silva. *Instituições de direito civil*. Rio de Janeiro: Forense, 2014.

PORTO, A. C. R.; LIMA JÚNIOR, E. F.; SILVA, P. A. Blockchain e a Autenticação de Documentos Eletrônicos: uma análise sob a perspectiva do Direito Notarial e Registral. *Revista de Direito, Estado e Telecomunicações*, v. 12, n. 1, p. 625-642, 2019.

Revista Eletrônica do TRT-PR. Curitiba: TRT-9ª Região, V. 12 n.118 . Mar. 23

SAVELYEV, P. A. & YAVITZ, A. Q.. Analyzing Social Experiments as Implemented: A Reexamination of the Evidence from the Highscope Perry Preschool Program. *Quantitative Economics*, v. 1, n, 1, p. 1-46, 2017.

SOARES, Marcos José. O sistema de justiça na blockchain. Disponível em: 28 <https://www.conjur.com.br/2022-mar-30/porto-soares-justica-blockchain>. Acesso em: 10 de jan. de 2024.

TARTUCE, Flávio. *Manual de Direito Civil*, Vol. Único, 2020. página 540.

USTER, Lucas. *Contratos Inteligentes (smart contracts): possibilidade e desafios no ordenamento jurídico brasileiro*. 1. ed. 2021.