UNIVERSIDADE FEDERAL DE SANTA CATARINA - UFSC
CENTRO DE CIÊNCIAS JURÍDICAS - CCJ
DEPARTAMENTO DE DIREITO
CURSO DE GRADUAÇÃO EM DIREITO

Luciano Gevaerd Konescki

SMART CONTRACTS: TECNOLOGIAS DISRUPTIVAS E A REGULAMENTAÇÃO DOS CONTRATOS INTELIGENTES NO DIREITO BRASILEIRO

Florianópolis, SC
2023

LUCIANO GEVAERD KONESCKI

SMART CONTRACTS: TECNOLOGIAS DISRUPTIVAS E A REGULAMENTAÇÃO DOS CONTRATOS INTELIGENTES NO DIREITO BRASILEIRO

Trabalho de Conclusão de Curso de Graduação em Direito do Centro de Ciências Jurídicas, da Universidade Federal de Santa Catarina, como requisito para a obtenção do título de Bacharel em Direito.

Orientadora: Profa. Dra. Melissa Ely Melo
Coorientadora: Profa. Me. Isabela Moreira do Nascimento Domingos

Florianópolis, SC

2023

AGRADECIMENTOS

Antes de mais nada, agradeço imensamente aos meus pais, Luciano e Monique, por serem muito mais do que meus provedores: meus parceiros, incentivadores e professores. Aqueles de quem eu não tenho dúvidas que estarão sempre perto para me apoiar e que permitiram, a partir de todo seu esforço, que eu tivesse a oportunidade de estar neste momento concluindo mais uma etapa da minha vida. Eu sei que vocês sempre colocaram eu e meus irmãos acima de todas as suas outras prioridades, sei o sacrifício que foi essa jornada e espero poder algum dia conseguir retribuir tudo isso.

Não menos importante é a parceira que escolhi ter ao meu lado. Obrigado, Iana, por todos os momentos vividos e experiências compartilhadas, por todos os ensinamentos, por toda a atenção e compreensão que eu nem mereço. Por ser a grande incentivadora que é e nunca ter desistido de mim, por mais difícil que eu seja. Por ser a pessoa mais incrível, disciplinada e determinada que eu já conheci e por me inspirar a ser melhor todos os dias. Sem você eu não teria nem começado este curso, muito menos terminado.

Aos meus amados avós, pelo infinito carinho, ensinamentos e todo o suporte que me deram e ainda dão. Meus pais são as pessoas que são graças a vocês e eu sou apenas um reflexo disso.

Aos meus irmãos, Victor e Clara, por serem também meus melhores amigos, pelas risadas e todos os momentos que vivemos juntos e que deixaram mais leve essa caminhada.

Ao meu irmão do coração, David, que sempre esteve ao meu lado desde os tempos de colégio, até dividiu comigo a sala de cursinho quando tomamos a difícil decisão de mudar de curso. Você é também uma inspiração para mim e seu sucesso é nada menos do que merecido.

A todos os meus amigos, pelos momentos de descontração, pelas horas de discussão, pela companhia e parceria de sempre. Pain e amigos do Colégio Militar, Chat CM, Resenha Azurra, Alyrio, amigos da universidade, amigos do futebol, todos foram muito importantes nessa minha jornada e ajudaram a moldar quem eu sou hoje.

À minha orientadora, Profa. Dra. Melissa Ely Melo, pela oportunidade, todo o suporte e contribuição na elaboração deste trabalho. Igualmente agradeço à minha coorientadora Profa. Me. Isabela Moreira do Nascimento Domingos, por toda a ajuda e atenção dada, principalmente nessas últimas semanas.

Por fim, agradeço a todos que contribuíram de alguma forma para a minha formação e crescimento como indivíduo e culminaram na construção deste trabalho.

RESUMO

Este trabalho investiga o impacto das tecnologias disruptivas, com enfoque na regulamentação dos *Smart Contracts* no Brasil. Os *Smart Contracts*, contratos autoexecutáveis programados em plataformas *blockchain*, são acordos digitais que se executam e se cumprem de maneira automática e autônoma ao atingir condições pré-estabelecidas. O objetivo desta pesquisa é analisar a adequação da atual estrutura regulatória brasileira frente a esta nova tecnologia, com o propósito de identificar possíveis lacunas legislativas e propor diretrizes para um ambiente regulatório mais harmonioso e favorável ao uso seguro e eficiente dos *Smart Contracts*. Esta análise é realizada a partir de uma metodologia qualitativa, que combina a revisão de literatura e análise comparativa da regulamentação em diferentes jurisdições, inclusive no direito estrangeiro. Os resultados esperados incluem o entendimento do atual cenário legal, os desafios e as oportunidades que os *Smart Contracts* apresentam, bem como sugestões para um caminho regulatório coerente e adaptativo no Brasil. A contribuição principal deste trabalho reside na compreensão da interseção entre tecnologia disruptiva e direito, provendo uma base sólida para discussões futuras em torno do tema.

Palavras-chave: Smart Contracts. Blockchain. Criptomoedas. Regulação.

ABSTRACT

This study investigates the impact of disruptive technologies, with a focus on the regulation of Smart Contracts in Brazil. Smart Contracts, self-executing contracts programmed on blockchain platforms, are digital agreements that automatically and autonomously execute and fulfill themselves upon meeting pre-established conditions. The objective of this research is to analyze the adequacy of the current Brazilian regulatory structure in the face of this new technology, with the aim of identifying possible legislative gaps and proposing guidelines for a more harmonious and favorable regulatory environment for the safe and efficient use of Smart Contracts. This analysis is carried out using a qualitative methodology, which combines literature review and comparative analysis of regulation in different jurisdictions, including foreign law. The expected results include understanding the current legal scenario, the challenges and opportunities that Smart Contracts present, as well as suggestions for a coherent and adaptive regulatory pathway in Brazil. The main contribution of this work lies in understanding the intersection between disruptive technology and law, providing a solid basis for future discussions on the topic.

Keywords: Smart Contracts. Blockchain. Cryptocurrency. Regulation.

LISTA DE FIGURAS

SUMÁRIO

1. INTRODUÇÃO

A tecnologia *blockchain*, popularizada com a criação da criptomoeda *Bitcoin* em 2009, trouxe consigo uma revolução nas transações financeiras, permitindo a criação de moedas digitais e a realização de transferências sem a necessidade de intermediários financeiros. A partir dessa tecnologia, foi possível desenvolver os *smart contracts* (contratos inteligentes), que são contratos digitais que se executam automaticamente com base em uma série de condições previamente estabelecidas.

Eles têm sido vistos como uma grande inovação no campo dos negócios e do direito, já que permitem a execução automática de acordos sem a necessidade de um intermediário. Isso pode levar a uma maior eficiência e segurança nas transações, além de reduzir os custos envolvidos em processos de contratação e litígios.

A partir desses avanços tecnológicos, vários setores da economia começaram a explorar as possibilidades oferecidas pelos *smart contracts*. Desde serviços financeiros até imobiliárias e indústrias de entretenimento, empresas em todo o mundo estão investindo em pesquisas e desenvolvimento de aplicações práticas para essa tecnologia.

O funcionamento dos contratos inteligentes é baseado em algoritmos e em condições pré-programadas, que são executadas automaticamente quando as condições são atendidas. Eles são armazenados em uma *blockchain*, o que garante transparência e segurança, já que todas as partes têm acesso a uma cópia do contrato e as informações nele contidas não podem ser modificadas.

A importância dos *smart contracts* é crescente, uma vez que eles possibilitam a criação de uma nova gama de aplicações descentralizadas e serviços financeiros, que antes não eram possíveis devido à falta de confiança nas transações. Além disso, sua utilização também pode ajudar a reduzir fraudes e conflitos, já que todas as transações são registradas e verificáveis.

Contudo, apesar de seu potencial de transformação, ainda há muitas questões a serem resolvidas em relação à sua regulamentação no direito brasileiro. É importante entender como as normas jurídicas se aplicam às novas tecnologias, de forma a garantir sua segurança e sua eficácia.

Nesse sentido, a pesquisa em relação à regulamentação dos *smart contracts* no direito brasileiro se mostra de grande relevância, especialmente para os profissionais do direito, desenvolvedores de tecnologia e empreendedores que buscam inovar por meio da *blockchain*.

Dessa forma, a questão central que orienta este estudo é: "Existe a necessidade de uma regulamentação específica no Brasil para lidar com os desafios que envolvem as tecnologias disruptivas, em particular, os *smart contracts*?".

A hipótese apresentada é que a regulação dos contratos inteligentes é importante para preencher as lacunas existentes na lei nacional em relação a esses contratos e tecnologias disruptivas relacionadas, de forma a garantir maior segurança e eficiência nas relações contratuais e estimular o desenvolvimento dessa e outras inovações tecnológicas.

O principal objetivo desta pesquisa é analisar a adequação da atual estrutura regulatória brasileira frente aos contratos inteligentes. O trabalho busca identificar possíveis lacunas legislativas e propor diretrizes para um ambiente regulatório mais harmonioso e favorável ao uso seguro e eficiente dos *Smart Contracts*.

A análise é realizada através de uma metodologia qualitativa, que combina revisão de literatura e análise comparativa da regulamentação em diferentes jurisdições, inclusive no direito estrangeiro.

Os objetivos específicos deste trabalho incluem: apontar as principais tecnologias disruptivas envolvidas na *Blockchain* e descrever a criação e os impactos desta, bem como os desafios envolvidos; registrar o surgimento dos contratos inteligentes, investigando suas principais aplicações e desafios; e identificar o cenário da regulamentação dos *Smart Contracts* no Brasil, considerando a aplicação do arcabouço legal vigente e a necessidade de um marco regulatório específico, além de buscar informações do direito estrangeiro para elaborar uma base comparativa e analisar as tendências globais a respeito do tema para verificar se a hipótese apresentada é pertinente.

Diante da crescente adoção das tecnologias disruptivas baseadas em *blockchain*, torna-se fundamental que o direito brasileiro esteja preparado para lidar com os desafios e oportunidades trazidos por essa nova realidade. A pesquisa a ser realizada neste trabalho visa contribuir para o debate e para o avanço nesse tema tão relevante e atual.

2. TECNOLOGIAS DISRUPTIVAS

As tecnologias disruptivas têm sido agentes transformadores fundamentais em diversas esferas da sociedade contemporânea. Elas redefinem a maneira como operamos, desde a interação pessoal até os processos comerciais e governamentais, rompendo com os sistemas estabelecidos e introduzindo novos modelos de negócio e de interação. Caracterizam-se por inovações que deslocam tecnologias existentes, alterando produtos, serviços, ou até mesmo indústrias inteiras.

A cada nova onda de inovação tecnológica, emergem incontáveis possibilidades que podem transformar aspectos fundamentais da vida cotidiana. Uma dessas tecnologias disruptivas é a *Blockchain*, originalmente concebida como uma plataforma para a criptomoeda *Bitcoin*, mas cujo potencial de aplicação transcende o mundo das moedas digitais.

Neste capítulo inicial, serão detalhadas as principais tecnologias disruptivas envolvidas no funcionamento da plataforma *Blockchain*, traçando um panorama sobre o seu surgimento, impacto e desafios.

2.1 *Blockchain* e tecnologias relacionadas

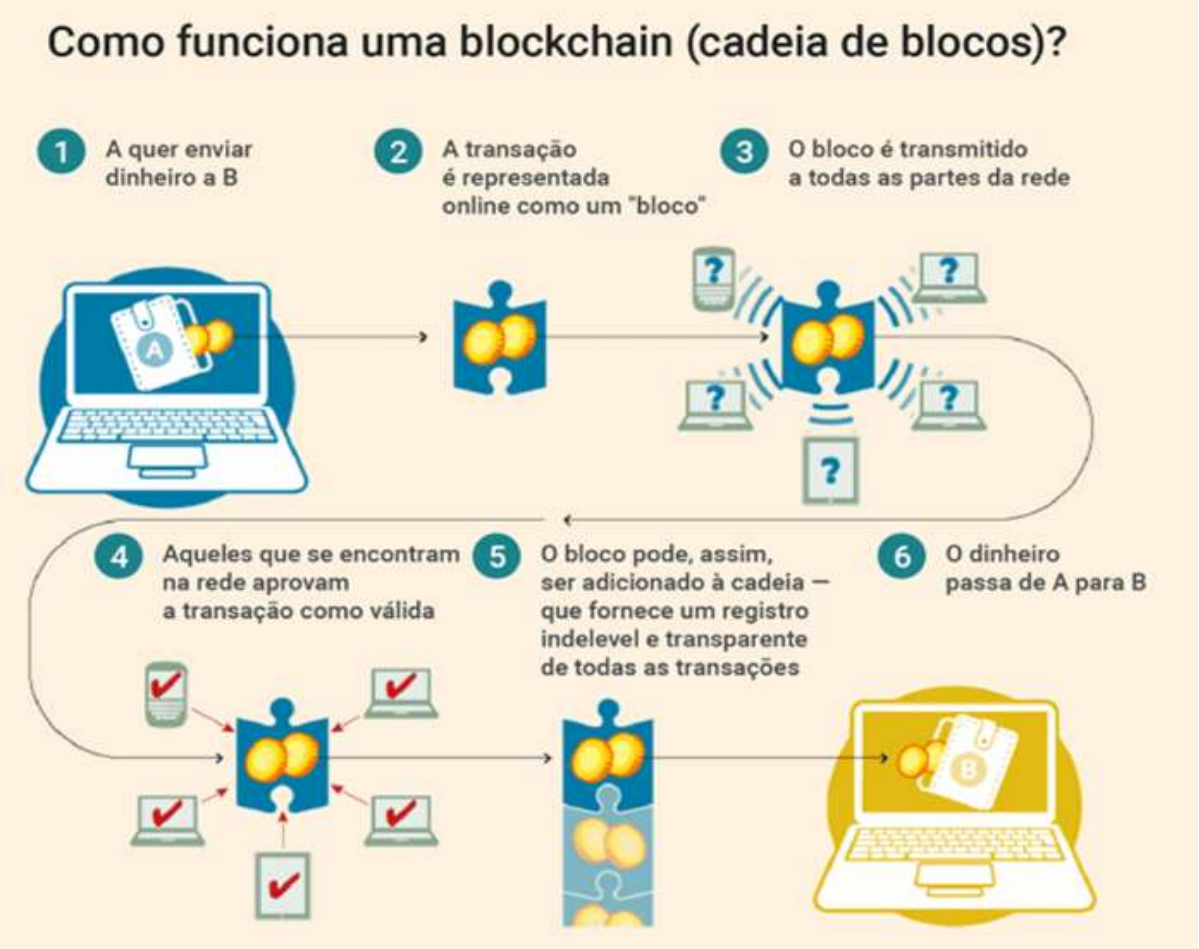
Blockchain, expressão em inglês que significa “corrente de blocos” ou “cadeia de blocos”, é o termo utilizado para designar uma tecnologia de livro-razão compartilhado, cujo objetivo principal é facilitar o registro de transações e de controle de ativos em uma rede de negócios. Ela usa de uma forma de criptografia sofisticada para registrar dados e seu funcionamento baseia-se em armazenar essas transações em uma lista de blocos, em que cada nova transação adiciona um novo bloco ao livro-razão.

Segundo Swan (2015, tradução nossa), *blockchain* é uma "base de dados descentralizada, distribuída e pública, onde as transações são registradas em blocos criptograficamente seguros e interligados por *hashes*, formando uma cadeia de blocos (*blockchain*)".

Para Tapscott e Tapscott (2016), *blockchain* é uma "plataforma confiável e descentralizada que permite a transferência de valor e a realização de transações seguras sem a necessidade de intermediários" (tradução nossa).

A tecnologia da *blockchain* foi introduzida por Stornetta e Haber em 1991, com o objetivo de criar um sistema de registro de documentos digital que fosse resistente à adulteração (SWAN, 2015). Desde então, ela tem evoluído e encontrado aplicações em diversas áreas, incluindo finanças, logística, saúde, entre outras.

FIGURA 1 - Funcionamento da *Blockchain*.



Fonte: IHODL, 2017.

Como a *Blockchain* envolve uma gama de tecnologias complexas e conceitos pouco usuais ao mundo jurídico, estes serão apresentados a seguir.

2.1.1 *Peer-to-Peer*

Peer-to-Peer (P2P) é uma tecnologia de rede de computadores em que os usuários atuam como clientes e servidores, diferentemente das redes tradicionais em que um servidor disponibiliza os serviços a todos os usuários de forma centralizada (KAMIENSKI *et al.*, 2005). Em tradução para o português, significa ponto a ponto, ou seja, cada participante da rede representa um ponto, que funciona como um servidor e auxilia o sistema a permanecer funcionando.

Em uma rede P2P, não há necessidade de uma organização central, visto que os usuários atuam como “nós” que permanecem conectados entre si. Isso permite que haja maior segurança contra perda de dados e garante uma maior disponibilidade do sistema. Em uma rede tradicional centralizada, a queda do servidor prejudica o funcionamento de toda a operação, enquanto no modelo P2P, caso um dos nós deixe de funcionar, os restantes manterão a rede operando (KAMIENSKI *et al.*, 2005).

Outra vantagem importante da tecnologia P2P é a escalabilidade, o que resolve problemas que envolvem a capacidade de rede e de processamento de um servidor central, pois todos os usuários contribuem para a formação da rede sem necessidade de um investimento adicional em *hardwares* de alto desempenho (KAMIENSKI *et al.*, 2005).

Apesar de garantir maior segurança contra perda de dados, o mesmo não pode ser dito quanto à idoneidade das transações em redes P2P, o que acarreta em um problema de confiança e a possibilidade de ocorrência de golpes.

A *blockchain*, sendo uma rede descentralizada, utiliza a tecnologia P2P e solucionou essa limitação que envolve confiança das transações com o protocolo *Proof-of-Work* (prova de trabalho).

2.1.2 *Proof-of-Work* (PoW)

O *Proof-of-Work*, ou prova de trabalho, é um mecanismo de consenso descentralizado que utiliza de poder computacional para verificar as transações ocorridas na *blockchain.* É responsável por inserir os novos blocos na *blockchain* a

partir de uma competição que envolve a resolução de cálculos matemáticos complexos e também por solucionar o problema de “gasto duplo”, um dos grandes desafios relacionados ao funcionamento das criptomoedas (BECKER *et al*, 2012).

A prova de trabalho é a resolução vencedora desses cálculos, realizada por computadores com alto poder de processamento de dados em um processo conhecido como *mining* ou mineração, que será melhor detalhado a seguir.

Os responsáveis pela mineração são chamados de “mineradores” e devem seguir um conjunto de regras durante o processo. Atingindo os objetivos, uma recompensa é ganha - no caso da mineração de *Bitcoin*, uma fração da criptomoeda é recebida como prêmio.

A prova de trabalho impede que os usuários repliquem as moedas indevidamente ou as gastem mais do que uma vez (gasto duplo), considerando a facilidade de copiar arquivos e dados em um computador. Como não há uma entidade central que controle quantas *Bitcoins* cada indivíduo possui, como um banco responsável, já que trata-se de um sistema descentralizado, o *Proof-of-Work* cumpre essa função (NAKAMOTO, 2008).

Entre as principais desvantagens do *Proof-of-Work* está o gasto de energia alto, a centralização da mineração nos chamados *“pools”,* que controlam a maior parte do poder computacional da rede e a possibilidade dos “ataques de 51%” ou “ataque de maioria”, em que um usuário ou grupo adquire domínio de uma *blockchain* ao ter mais do que a metade do poder de computação dela e passar a poder realizar modificações em suas transações.

2.1.3 *Proof-of-Stake* (PoS)

O *Proof-of-Stake* (PoS) é um protocolo de consenso utilizado em *blockchains* que difere do *Proof-of-Work* (PoW) por não depender da resolução de problemas matemáticos complexos para validação das transações. Enquanto o PoW usa a energia computacional para resolver problemas complexos e criar novos blocos na cadeia, o *proof-of-stake* depende da posse de criptomoedas como forma de garantia de validação das transações, utilizando um algoritmo que seleciona aleatoriamente um validador para validar as transações e criar um novo bloco.

O protocolo *proof-of-stake* tem como base a seleção aleatória de um validador para criar um novo bloco na *blockchain*. Os validadores são escolhidos com base na quantidade de criptomoedas que possuem como garantia, sendo que quanto maior a quantidade, maior a probabilidade de serem selecionados. Os validadores também são incentivados a seguir as regras e garantir a integridade da cadeia por meio de recompensas em criptomoedas.

King e Nadal (2012) destacam que o protocolo *proof-of-stake* apresenta vantagens em relação ao *proof-of-work*, como o menor consumo de energia e a redução da centralização da validação em grandes mineradoras. Além disso, afirmam que o *proof-of-stake* permite uma maior escalabilidade da *blockchain*, pois o processo de validação é menos complexo e pode ser executado em dispositivos com menor capacidade computacional.

Um dos principais benefícios da PoS em relação à PoW é a redução do consumo de energia elétrica para validar as transações e criar novos blocos. Isso ocorre porque a PoS não requer o uso de hardware especializado (como no caso das mineradoras de Bitcoin), o que torna o processo de validação de transações muito menos intensivo em recursos. Outro benefício é a maior segurança que a PoS proporciona, uma vez que para um ator malicioso comprometer a rede, seria necessário ter mais de 50% das moedas em circulação, o que se torna mais difícil à medida que a rede cresce.

De acordo com Antonopoulos (2018), o protocolo *proof-of-stake* foi introduzido pela primeira vez pelo *PeerCoin* (ou PPCoin) em 2012. Nesse protocolo, os validadores são escolhidos com base na quantidade de criptomoedas que possuem e mantêm bloqueadas em uma carteira. Quanto mais criptomoedas possuem, maior a probabilidade de serem escolhidos como validadores.

O PPCoin também usa um algoritmo de ajuste de dificuldade que varia de acordo com a quantidade de criptomoedas que estão sendo usadas para validar as transações. Conforme descrito no paper "*PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake*" (KING, NADAL, 2012), o algoritmo de ajuste de dificuldade incentiva a manutenção das criptomoedas na carteira para aumentar a probabilidade de ser escolhido como validador, o que ajuda a manter a segurança da rede.

Apesar dos benefícios da PoS, o protocolo ainda enfrenta alguns desafios, como o problema do "nada em jogo" (*nothing-at-stake*) e o problema do "ataque de

longo alcance" (*long-range attack*). O problema do "nada em jogo" refere-se à possibilidade de validadores tentarem validar blocos em várias cadeias simultaneamente, uma vez que não há custo associado a essa atividade, ao contrário do que ocorre na PoW. Já o problema do "ataque de longo alcance" ocorre quando um ator malicioso tenta reescrever uma parte significativa do histórico da *blockchain*, o que se torna mais fácil na PoS, pois o ator malicioso pode acumular uma grande quantidade de moedas e, portanto, poder de voto na rede (LI *et al*, 2017).

Dessa forma, a seleção aleatória de validadores pode levar à centralização da validação em um pequeno grupo de usuários com grandes quantidades de criptomoedas. Apesar de uma alternativa interessante ao PoW, o *proof-of-stake* ainda é uma tecnologia em desenvolvimento e precisa ser aprimorado para garantir a segurança e a integridade da *blockchain*.

Além da já citada PPCoin, o PoS é aplicado em várias *blockchains*, como a *Ethereum*, a *Cardano* e a *Cosmos*. Na *Ethereum*, o PoS tem como objetivo aumentar a escalabilidade da rede e reduzir os custos de validação de transações. Na *Cardano*, o PoS é utilizado desde o lançamento da rede, com o objetivo de torná-la mais segura e escalável. Na *Cosmos*, o PoS é utilizado para validar transações e criar novos blocos na rede.

2.1.4 *Hash*

Um elemento central na ciência da computação e, em particular, na segurança da informação, é a função *hash*. Segundo Stinson e Paterson (2018), essa função é uma operação fundamental na criptografia, transformando dados de entrada, ou "mensagem", em um valor fixo de saída, ou "*hash*". A operação de transformação é conhecida como "*hashing*".

Criada na década de 1950, a função *hash* foi inicialmente aplicada na aceleração da busca de dados em estruturas computacionais (ZOBEL, MOFFAT, 1998). No entanto, com o passar do tempo, e especialmente na era digital, essa função encontrou aplicações em uma variedade de áreas, incluindo a criptografia.

A partir da perspectiva da criptografia, o objetivo de uma função *hash* é garantir a integridade dos dados. Isso significa que, mesmo uma pequena alteração

nos dados de entrada, deve resultar em uma mudança significativa no valor *hash* resultante, tornando quase impossível reconstruir os dados originais a partir do *hash* (MERKLE, 1980).

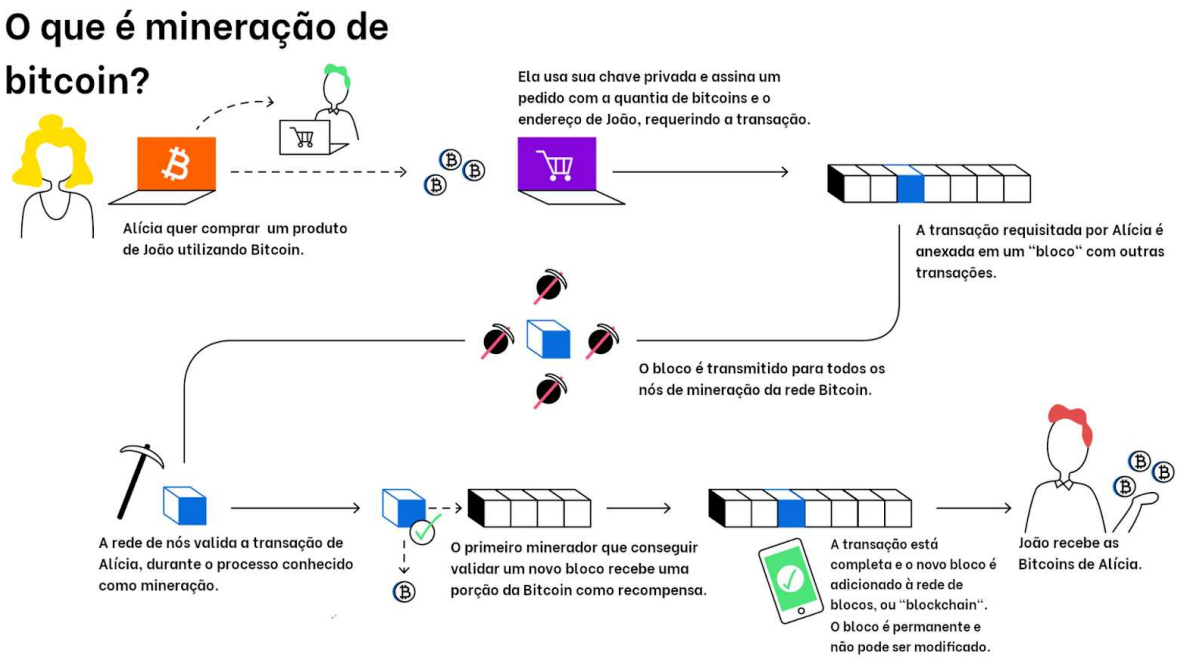
Esse recurso torna a função *hash* um componente essencial na tecnologia *blockchain*. O *blockchain*, uma estrutura de dados descentralizada e à prova de violação, confia em *hashes* para garantir a integridade dos blocos de dados que contém (NAKAMOTO, 2008). Cada bloco na *blockchain* contém um *hash*, que é calculado a partir dos dados do bloco anterior, criando assim uma ligação contínua e imutável entre os blocos.

Por exemplo, no contexto da *Bitcoin*, a primeira criptomoeda baseada em *blockchain*, a função *hash* é usada para validar as transações e evitar a duplicação de gastos, conforme descrito por Nakamoto (2008). Além disso, ela é utilizada no processo de mineração de *Bitcoin*, onde os mineradores competem para resolver um quebra-cabeça criptográfico baseado em *hash*, com o objetivo de adicionar um novo bloco à cadeia (BACK, 2002).

2.1.5 Mineração de Criptomoeda

Um aspecto crucial do sistema *Bitcoin* é a mineração. Este processo envolve nós na rede (chamados de mineradores) resolvendo problemas criptográficos complexos para adicionar um novo bloco à cadeia e validá-lo. Como recompensa por este trabalho, o minerador que adiciona o bloco recebe uma certa quantidade da criptomoeda. Este processo não só ajuda a adicionar transações ao *blockchain*, mas também serve para introduzir novas *Bitcoins* no sistema (NARAYANAN et al., 2016).

Figura 2 - O que é mineração de *bitcoin*?



.Fonte: Jornalismo UFV

A complexidade desses problemas matemáticos é ajustada automaticamente pela rede para garantir que uma nova transação seja adicionada ao *blockchain* aproximadamente a cada dez minutos (no caso da *Bitcoin*). Este ajuste de dificuldade, juntamente com o número limitado de criptomoedas que podem ser mineradas, ajuda a regular o fornecimento de novas unidades da criptomoeda e a manter a segurança e integridade da rede (NARAYANAN *et al*., 2016).

Os mineradores competem entre si para resolver o problema matemático e validar a próxima transação. O primeiro a conseguir resolver o problema anuncia sua solução para toda a rede, que então verifica a solução e, se correta, a transação é adicionada ao *blockchain*. Esta competição ajuda a garantir a aleatoriedade na seleção de qual transação é validada a seguir, o que contribui para a segurança da rede (NARAYANAN *et al*., 2016).

No entanto, a mineração de criptomoedas é um processo que consome muita energia, uma vez que exige um poder de computação significativo, o que levantou preocupações sobre o impacto ambiental causado pela atividade. Além disso, como a mineração requer um investimento significativo em *hardware* de computação

especializado, ela se tornou menos acessível para o usuário médio ao longo do tempo (NARAYANAN *et al*., 2016).

Para realizar a mineração de uma criptomoeda como a *Bitcoin*, os mineradores precisam de um computador com uma placa de vídeo poderosa, um *software* de mineração, uma carteira digital para armazenar suas criptomoedas e uma conexão com a internet. Eles também precisam se juntar a um *pool* de mineração, um grupo de "*miners"* que combinam seu poder de computação para aumentar suas chances de validar transações e receber recompensas (NARAYANAN *et al*., 2016).

2.2 Desafios enfrentados pela tecnologia *Blockchain*

O universo das criptomoedas, com suas nuances e peculiaridades, tem apresentado desafios significativos à segurança de informações. A tecnologia *blockchain*, que suporta a maioria dessas moedas digitais, não é imune a esses desafios. Uma dessas ameaças conhecidas é o ataque de 51%, que, embora raro, tem o potencial de comprometer significativamente a segurança e a integridade da rede *blockchain* (NAKAMOTO, 2008).

Além disso, outro problema conhecido gerado pela tecnologia é o gasto de energia e o possível impacto ambiental causado, principalmente pelo processo de mineração.

2.2.1 Gasto de Energia

Como já citado, muitas redes *blockchain* notáveis, como a *Bitcoin*, utilizam um mecanismo de consenso chamado Prova de Trabalho (*Proof-of-Work* ou PoW). Este método envolve a realização de um trabalho computacional difícil de resolver, mas fácil de verificar, cujo propósito é evitar ataques maliciosos ao sistema. No entanto, o PoW é intensivo em termos energéticos, uma vez que exige uma quantidade substancial de energia elétrica para realizar essas operações computacionais complexas (STOLL; KLAAßEN; GALLERSDÖRFER, 2019).

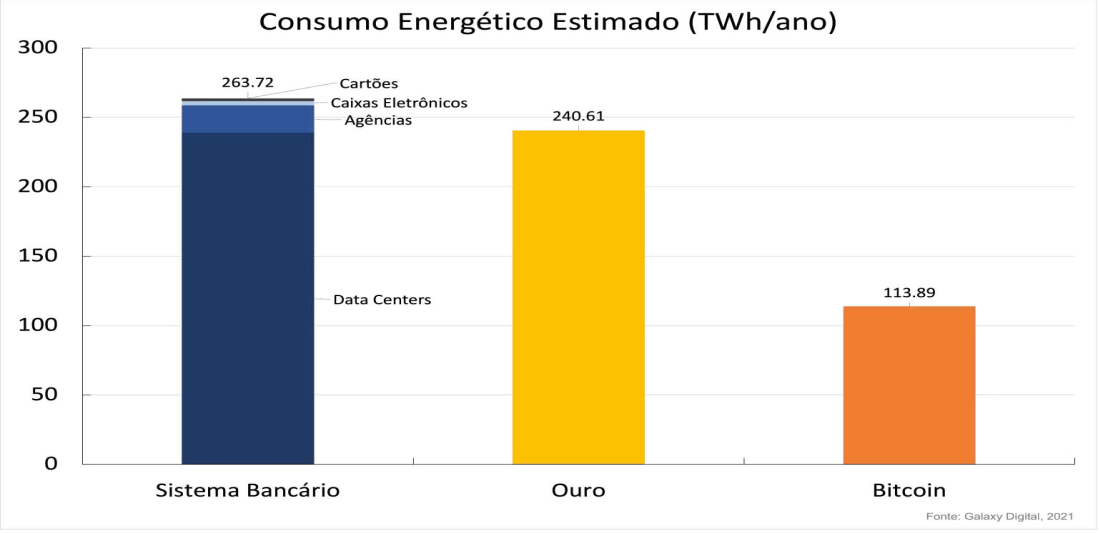
Essa intensa utilização de energia vem levantando sérias preocupações ambientais. Há argumentos de que a sustentabilidade a longo prazo das operações

blockchain baseadas em PoW pode ser questionável devido ao elevado consumo de energia, com estudos projetando que a utilização de *Bitcoin* sozinha pode produzir emissões de dióxido de carbono suficientes para elevar a temperatura média global em 2ºC nas próximas três décadas (MORA *et al*., 2018).

Uma pesquisa conduzida por acadêmicos da Universidade de Münster, na Alemanha, comparou a utilização de um protocolo de PoW processando todas as transações financeiras do mundo em relação a um hipotético sistema centralizado de pagamento por cartão e concluiu que a emissão de CO^2 mundial aumentaria em 2,1%, o que representa aproximadamente o gás carbônico emitido por todas as companhias de tráfego aéreo anualmente (BECKER *et al*, 2012).

Por outro lado, há estudos que defendem que a rede *Bitcoin* gasta consideravelmente menos energia do que o sistema financeiro e bancário clássico. Além de uma transação de *Bitcoin* ser pelo menos duzentas vezes mais rápida que uma transação eletrônica padrão, acredita-se que a rede da criptomoeda opera ainda longe da sua eficiência máxima, podendo elevar ainda quatro vezes seu volume de transações sem aumentar seu consumo de energia (KHAZZAKA, 2022). Outros levantamentos, como o da Galaxy Digital, apontam que a rede *Bitcoin* consome menos que o sistema bancário e a mineração de ouro, como ilustra a figura a seguir:

Figura 3 - Consumo Energético da *Bitcoin* x Sistema Bancário e Mineração de Ouro



Fonte: Galaxy Digital

De qualquer modo, apesar da divergência existente sobre a questão do gasto energético, estão sendo estudadas alternativas mais eficientes para garantir a sustentabilidade a longo prazo da tecnologia *blockchain*. Algumas plataformas estão considerando a transição ou já migraram para o protocolo *Proof-of-Stake*, que é menos intensivo em energia, apesar de apresentar seus próprios desafios.

2.2.2 Centralização e o “Ataque de 51%”

O conceito de ataque de 51% foi inicialmente apresentado por Satoshi Nakamoto, o criador pseudônimo do *Bitcoin*, no *white paper* da criptomoeda em 2008. No entanto, conforme mencionado por Eyal e Sirer (2018), este ataque não se limita apenas ao *Bitcoin*, mas se estende a todos os sistemas que utilizam a tecnologia *blockchain* com base no protocolo *Proof-of-Work* (PoW), devido ao problema da centralização.

Em um ataque de 51%, um único minerador ou pool de mineração acumula mais de 50% do poder de *hash* total da rede. Isso dá ao ator maligno a capacidade de controlar as transações dentro da *blockchain*, permitindo a ele gastar duas vezes a mesma moeda digital e impedir que outras transações sejam confirmadas (KARAME, ANDROULAKI, CAPKUN, 2012).

Muitos argumentam que o potencial de um ataque de 51% é contrabalançado pelo alto custo de sua execução. A teoria da "jogada egoísta" (*Selfish-Mine Strategy*), conforme proposta por Eyal e Sirer (2018), sugere que um ator racional provavelmente não executaria um ataque de 51% devido ao prejuízo potencial que isso poderia causar ao valor da criptomoeda que ele mesmo detém.

No entanto, um relatório recente de Bonneau *et al*. (2015) demonstra que, na prática, um ataque de 51% pode ser muito mais barato de executar do que o previsto. Isto é particularmente verdadeiro para criptomoedas alternativas com menor poder de *hash* na rede, o que leva à conclusão preocupante de que muitas *blockchains* podem ser mais vulneráveis a um ataque de 51% do que se pensava anteriormente.

A discussão contínua sobre os riscos e a viabilidade de um ataque de 51% reflete a necessidade de melhorias de segurança dentro do ecossistema *blockchain*.

A implementação de protocolos alternativos de consenso, como o *Proof-of-Stake (PoS)*, pode oferecer uma defesa mais robusta contra um ataque de 51%, embora esses protocolos também tenham suas próprias vulnerabilidades.

Matzutt *et al*. (2018) destacam que o controle sobre a maioria dos recursos de mineração não apenas abre a porta para o duplo gasto, mas também permite ao invasor censurar transações, ignorando blocos propostos por outros nós e validando apenas os próprios. Embora tal cenário ainda seja teórico, sua possibilidade poderia ter um impacto devastador na confiança no sistema *blockchain*.

A mitigação do ataque de 51% tem sido um tópico quente de pesquisa. Como mencionado por Bentov *et al*. (2014), uma abordagem possível é mudar para um sistema PoS, em que a criação de blocos não é mais dependente da quantidade de poder de *hash*, mas da quantidade de criptomoedas que um nó possui. No entanto, Kiayias, Russell, David e Oliynykov (2017) argumentam que isso traz seus próprios desafios, como o chamado problema "Nada em jogo" (*Nothing-at-stake*).

Outra abordagem, de acordo com Rosenfeld (2014), seria a introdução de um sistema de mineração cooperativa, no qual vários mineradores unem seus recursos para aumentar suas chances de criar um bloco, mas sem permitir que um único minerador tenha controle majoritário. Embora essa abordagem possa parecer promissora, ela ainda está sujeita à manipulação e exige confiança entre os participantes.

Finalmente, vale ressaltar que o ataque de 51% representa uma ameaça real, mas também fornece um impulso para o contínuo desenvolvimento e refinamento da tecnologia *blockchain*. Através do estudo contínuo das vulnerabilidades da rede e da exploração de possíveis soluções, o futuro do *blockchain* pode tornar-se ainda mais seguro e robusto (TAPSCOTT, TAPSCOTT, 2016).

De forma mais recente, pesquisadores começaram a explorar a possibilidade de combinar vários protocolos de consenso, na esperança de que tal abordagem possa fornecer uma defesa mais robusta contra os ataques de 51%. No entanto, esses estudos ainda estão em estágio inicial e é necessário que sejam desenvolvidas mais pesquisas sobre o tema antes que qualquer conclusão possa ser feita.

2.3 O Surgimento da *Blockchain e a* criação da *Bitcoin*

A *Blockchain* ganhou mais relevância a partir da criação do criptoativo *Bitcoin*, uma moeda digital desenvolvida por Satoshi Nakamoto (pseudônimo de uma pessoa ou grupo que permanece anônimo). Nakamoto (2008) verifica a necessidade de um sistema de pagamento eletrônico baseado em mecanismos de criptografia que possam garantir a segurança da transação sem a utilização de um terceiro e que sejam impossíveis de reverter, de modo a proteger as partes envolvidas.

O grande desafio do modelo proposto da moeda digital era assegurar a possibilidade de verificação de que o ativo não foi comercializado duas ou mais vezes pelo dono original sem que houvesse a necessidade de uma autoridade central que verificasse transações duplicadas, já que a ideia da *Bitcoin* é ser descentralizada, não requerendo intermediários e não estando sob controle ou fiscalização de um Estado.

Esse problema, conhecido como “gasto duplo”, ocorre quando um usuário consegue utilizar um ativo digital mais de uma vez, graças a uma falha de registro. Para solucioná-lo, a *Bitcoin* conta com um registro do histórico das transações que é compartilhado publicamente e distribuído a todos os usuários de forma instantânea, utilizando a tecnologia *peer-to-peer* (ponto a ponto), um tipo de arquitetura em que a conexão é feita diretamente entre os computadores dos usuários, que funcionam como servidores (NAKAMOTO, 2008; ALI, Robleh *et al*, 2014).

A composição de tecnologias que permitiu essa solução é justamente a *Blockchain*. Nakamoto, em sua pesquisa publicada em 2008, faz referência aos conceitos e ideias criados no fim dos anos 1980 e começo dos anos 1990 pelos cientistas americanos W. Scott Stornetta e Stuart Haber, o que inclusive suscitou discussão sobre a possibilidade do primeiro ser a real identidade por trás de Nakamoto, fato que Stornetta negou (BHARATAN, 2020).

Uma das principais contribuições responsáveis pela idealização da *Blockchain* surgiu dos trabalhos de Haber e Stornetta em 1991, quando publicaram um artigo intitulado "*How to Time-Stamp a Digital Document*". Na época, a intenção dos autores era criar um método seguro para garantir a integridade e autenticidade de documentos digitais, evitando a necessidade de confiança em terceiros.

A solução proposta por Haber e Stornetta consistia em uma estrutura de dados que permitiria a criação de um registro imutável, à medida que novas informações eram adicionadas. Essa estrutura é baseada em blocos encadeados, onde cada um contém um *hash* criptográfico do bloco anterior, garantindo assim a integridade da cadeia. Dessa forma, a *blockchain* foi concebida como um livro contábil digital descentralizado e imutável, com a capacidade de armazenar transações e outros tipos de informações de forma segura e transparente (HABER; STORNETTA, 1991).

Os estadunidenses idealizaram, então, o sistema de *time-stamping*, carimbos digitais com o propósito de provar a veracidade de dados de forma que não pudessem ser adulterados com mudança de data. Dessa forma, eles conseguiam ordenar os arquivos gravados de forma segura, representando uma solução para a ordem e gerenciamento de documentos digitais, de modo que não pudessem ser modificados ou manipulados (HABER; STORNETTA, 1991).

A partir disso, eles criaram a primeira *blockchain,* chamada *Surety,* em que um programa que desenvolveram, nomeado de "*AbsoluteProof*" usava criptografia e a tecnologia de *time-stamping* para marcar documentos digitais e gerar um selo, que era enviado ao servidor da *Surety*. O programa então criaria um *hash* (uma função matemática que converte qualquer arquivo em um código alfanumérico, servindo como uma "impressão digital" do documento) para todos os selos adicionados à sua base de dados semanalmente e que passaria a ser publicado em pequenos anúncios no jornal *New York Times,* o que tornaria impossível para qualquer pessoa modificar os valores, já que eles eram divulgados em um periódico de alta circulação (CZULEGER, 2018).

A *Surety* surgiu em 1995 e teve como objetivo fornecer um método seguro para armazenar e compartilhar dados de forma descentralizada. A ideia central era criar uma estrutura descentralizada e inviolável, com um sistema de verificação de dados que permitiria que documentos e informações importantes fossem armazenados em uma rede segura e imutável (HABER; STORNETTA, 1995).

Ela foi projetada para evitar o problema do "*double-spending*" ou "gasto duplo", que se refere à possibilidade de gastar uma mesma unidade de moeda digital mais de uma vez. Esse problema foi resolvido através de um sistema de registro distribuído que tornava impossível modificar transações já registradas.

O trabalho pioneiro de Stornetta e Haber sobre a tecnologia *blockchain* foi a grande inspiração para a criação da *Bitcoin* em 2008 por Satoshi Nakamoto. Ela é uma criptomoeda descentralizada que utiliza a tecnologia *blockchain* para criar um sistema de registro distribuído seguro, onde as transações são armazenadas de forma imutável e transparente (NAKAMOTO, 2008). Nakamoto acreditava que um sistema descentralizado de transação de dinheiro permitiria maior liberdade e controle sobre as próprias finanças, além de maior privacidade e segurança.

Sendo o funcionamento da *Bitcoin* baseado nessa combinação de criptografia e a tecnologia *blockchain*, cada transação de criptomoeda é registrada em um bloco, e cada bloco é conectado ao bloco anterior para formar uma cadeia, daí o termo "*blockchain*". Essa cadeia é armazenada e mantida por um número de nós na rede *Bitcoin*, cada um mantendo uma cópia completa da *blockchain*. Isso cria um sistema altamente resistente a adulterações, pois qualquer alteração em um bloco exigiria que todos os blocos subsequentes na cadeia fossem alterados, o que seria quase impossível devido à quantidade de poder computacional necessário (NARAYANAN *et al*., 2016).

Os usuários de *Bitcoin* mantêm suas moedas em carteiras digitais, que podem ser armazenadas localmente em um computador ou smartphone, ou mantidas online. As transações são realizadas criando-se uma mensagem que especifica o remetente, o destinatário e a quantidade a ser transferida, que então é assinada digitalmente usando a chave privada do remetente (NARAYANAN *et al*., 2016). Esta transação é então transmitida para a rede *Bitcoin*, onde é verificada por nós na rede e, em seguida, adicionada a um bloco.

A *Bitcoin* foi a primeira aplicação bem-sucedida da tecnologia *blockchain*, tornando-se um marco importante na história das criptomoedas e da tecnologia em questão. A partir daí, diversas outras criptomoedas surgiram e utilizam a *blockchain* como base para seu funcionamento.

Nos primeiros anos de existência, a *Bitcoin* era utilizada principalmente por um nicho de entusiastas da tecnologia e ativistas políticos. Em 2011, outras criptomoedas surgiram, como o *Litecoin* e o *Namecoin*, seguindo o modelo do *Bitcoin* com algumas variações (SWAN, 2015).

O avanço das criptomoedas e da tecnologia *blockchain* começou a chamar a atenção do mercado financeiro e dos governos em meados de 2013, quando a

cotação da *Bitcoin* atingiu um valor de cerca de US$ 1.000,00 (SWAN, 2015). Isso levou a uma onda de especulação em torno das criptomoedas, com a *Bitcoin* chegando ao pico de valor de US$ 68.000,00 em 2021. Atualmente, em junho de 2023, está cotada em US$ 26.652,30, conforme pode ser visto no gráfico a seguir.

Figura 4 - Gráfico da cotação da Bitcoin (2014-2023).

Fonte: CoinMarketCap

O sucesso da *Bitcoin* pode ser atribuído a vários fatores. A sua natureza descentralizada oferece liberdade de restrições e controle governamental. Além disso, como as transações são anônimas (as identidades reais dos usuários não são publicamente reveladas, apenas os seus endereços públicos do criptoativo), há um alto nível de privacidade em comparação com os sistemas financeiros tradicionais (TAPSCOTT; TAPSCOTT, 2016). Finalmente, a segurança robusta fornecida pelo *blockchain*, juntamente com a natureza deflacionária da *Bitcoin* (o número total dessa criptomoeda que pode existir é limitado a 21 milhões), aumentou o seu apelo como uma forma de reserva de valor, semelhante ao ouro.

Enquanto a *Bitcoin* permaneceu como a criptomoeda mais popular e amplamente adotada, a *blockchain* começou a ser reconhecida como uma solução viável para problemas em uma variedade de setores além das finanças. A imutabilidade e a transparência da tecnologia *blockchain* são atrativas para setores como a saúde, onde pode ser usada para proteger dados sensíveis e rastrear o histórico de atendimento ao paciente (KUO *et al*., 2017), bem como no controle e transparência das contas públicas (GONÇALVES; DOMINGOS, 2021).

Na área de logística, a tecnologia promete resolver problemas de rastreabilidade e confiança, permitindo um rastreamento seguro e transparente de produtos ao longo da cadeia de suprimentos (RADMANESH; HAJI; VALILAI, 2023). Na esfera política, a tecnologia *blockchain* também tem sido proposta como uma solução para questões de segurança e transparência na votação eletrônica (ALVI *et al*., 2022).

Apesar da contínua popularidade da *Bitcoin*, o *Ethereum*, lançado em 2015, demonstrou outra faceta do potencial da tecnologia *blockchain* para além das criptomoedas ao introduzir contratos inteligentes, programas de computador autônomos que executam automaticamente as condições de um contrato quando determinadas condições são atendidas (BUTERIN, 2014).

A evolução do *Bitcoin* ao longo do tempo teve um impacto significativo na tecnologia *blockchain*. O seu sucesso não apenas validou a tecnologia, mas também estimulou o seu desenvolvimento e aplicação em uma variedade de outros contextos. Com o surgimento de contratos inteligentes e a crescente adoção da *blockchain* em vários setores, a tecnologia demonstrou o potencial de ser muito mais do que apenas uma plataforma para criptomoedas.

3. SMART CONTRACTS

Como consequência direta das inovações trazidas pela tecnologia *Blockchain*, surgem os *Smart Contracts*, contratos inteligentes que buscam revolucionar a maneira como estabelecemos e cumprimos acordos. Esses contratos são códigos de computador armazenados dentro de uma *Blockchain* que, quando acionados, são capazes de verificar e executar automaticamente os termos de um contrato, reduzindo a necessidade de intermediários e proporcionando maior rapidez e segurança nas transações.

Os *Smart Contracts* representam uma potencial mudança paradigmática na forma como realizamos transações de negócios, desde contratos imobiliários até acordos comerciais internacionais. Essa nova tecnologia traz consigo promessas de maior eficiência e transparência, mas também levanta uma série de questões complexas e desafios que precisam ser abordados para garantir a sua aplicação segura e eficaz.

Este capítulo apresentará os *Smart Contracts*, abordando o contexto de sua criação, seus principais impactos e aplicações, bem como os desafios enfrentados na aplicação e execução destes contratos inteligentes. Dessa forma, pretende-se oferecer uma compreensão mais aprofundada dessas ferramentas revolucionárias, estabelecendo um alicerce sólido para as discussões subsequentes sobre sua regulamentação e implicações jurídicas.

3.1 Surgimento dos Contratos Inteligentes

Apesar de não ser um conceito criado a partir das *Blockchains,* os *Smart Contracts*, ou contratos inteligentes, ganharam muita relevância com o advento da tecnologia de corrente de blocos e das criptomoedas.

Graças aos seus diversos benefícios, como uma grande economia de custos à Indústria de serviços financeiros, a simplificação de contratos complexos e a redução de custo de transações, há cada vez mais interesse em pesquisa por instituições financeiras e acadêmicas, que buscam cada vez mais formalizar e simplificar a implementação dos *smart contracts* em diversas áreas, tornando-a cada vez mais simples e prática (BASHIR, 2018).

Segundo Bashir (2018), não há consenso quanto a uma definição padrão do que são *Smart Contracts*. Ele conceitua a tecnologia como “um programa de computador seguro e imparável que representa um acordo que é automaticamente executável” (p. 373, tradução nossa).

Nick Szabo, jurista e criptógrafo americano de ascendência húngara, criador do conceito original de contrato inteligente e do *“Bit gold”* (precursor da *Bitcoin* que nunca chegou a ser implementado de fato), teorizou os contratos inteligentes como um protocolo de transação computadorizada que executa os termos de um contrato e cujos objetivos gerais são satisfazer condições contratuais comuns (como termos de pagamento, ônus, confidencialidade e obrigações, entre outras), minimizar exceções maliciosas e acidentais e também reduzir a necessidade de um intermediário. Também visa a redução de perdas por fraude e redução de custos (SZABO, 1997).

Szabo introduziu o conceito de *smart contracts* em 1994. Ele vislumbrou a possibilidade de criar contratos autoexecutáveis e autorreforçáveis, que dispensassem intermediários e garantissem a execução das cláusulas acordadas por meio de códigos de computador (SZABO, 1997). A ideia foi inspirada pela evolução dos sistemas de comércio eletrônico, que estavam se tornando cada vez mais populares no início dos anos 90.

Szabo percebeu que a execução das cláusulas contratuais poderia ser melhorada com a digitalização e a descentralização, eliminando a necessidade de intervenção humana e, consequentemente, reduzindo os custos e o tempo de resolução dos conflitos contratuais (SZABO, 1997).

A visão de Szabo incluía a utilização de regras lógicas e protocolos matemáticos para verificar o cumprimento das condições estabelecidas em um contrato e garantir a execução das cláusulas acordadas. Essas regras e protocolos seriam implementados por meio de um código de computador, criando um "contrato inteligente" (SZABO, 1996).

3.1.1 Conceito de *smart contracts*

Smart contracts são programas de computador que executam automaticamente os termos de um contrato quando as condições estabelecidas são

cumpridas (ANTONOPOULOS; WOOD, 2018). Eles são projetados para serem transparentes, imutáveis e seguros, garantindo que as partes envolvidas possam confiar na execução do contrato sem a necessidade de intermediários.

Szabo (1996) definia contratos inteligentes como um conjunto de promessas, especificadas em forma digital, que incluem protocolos nos quais as partes cumprem essas promessas. Desde então, o termo evoluiu com o advento das criptomoedas e *blockchain*.

Buterin (2014) enfatiza que os contratos inteligentes agora se referem a programas de computador que operam em um *blockchain* e são capazes de executar automaticamente as condições de um contrato quando certas condições predefinidas são atendidas.

Os contratos inteligentes desempenham um papel crucial no ambiente de *blockchain*, uma vez que são responsáveis por controlar e transferir o estado dos ativos digitais entre os participantes de uma rede (MOUGAYAR, 2016). A natureza descentralizada, transparente e imutável da *blockchain* ajuda a garantir a segurança e a confiabilidade desses contratos.

Essencialmente, os contratos inteligentes permitem a codificação de regras e condições de contrato de uma maneira que só permita a execução de transações quando todas as condições forem cumpridas, promovendo, assim, a confiança, a transparência e a eficiência nas transações digitais (TAPSCOTT; TAPSCOTT, 2016).

3.1.2 Criação da plataforma *Ethereum* e sua evolução

A popularização dos *smart contracts* ocorreu com a criação da plataforma *Ethereum*, desenvolvida por Vitalik Buterin em 2015. Ela é uma rede *blockchain* descentralizada que permite o desenvolvimento e a execução de *smart contracts* e aplicações descentralizadas (*dApps*) usando a criptomoeda *Ethe*r como forma de pagamento (WOOD, 2014).

A *Ethereum* trouxe várias inovações em relação à *blockchain* do *Bitcoin*, como a capacidade de criar e executar contratos inteligentes e a introdução de uma linguagem de programação *Turing* completa chamada *Solidity*. Isso permitiu que os desenvolvedores criassem *smart contracts* mais complexos e personalizados,

expandindo o escopo de aplicação dessa tecnologia (ANTONOPOULOS; WOOD, 2018).

Desde sua criação, a *Ethereum* tem sido a plataforma de escolha para o desenvolvimento de contratos inteligentes e *dApps*. Ela tem evoluído constantemente, com atualizações e melhorias em seu protocolo, a fim de aumentar a escalabilidade, segurança e eficiência da rede. Além disso, várias outras plataformas de *blockchain*, como Cardano, Tezos e NEO, surgiram com o objetivo de oferecer soluções alternativas e complementares aos *smart contracts* e *dApps*, ampliando o ecossistema de contratos inteligentes (ZHENG *et al*., 2020).

3.1.3 Relação entre *Ethereum* e *smart contracts*

A plataforma *Ethereum* desempenhou um papel crucial na disseminação e adoção dos contratos inteligentes. Ao oferecer uma infraestrutura descentralizada e ferramentas de desenvolvimento amigáveis, a *Ethereum* permitiu que desenvolvedores, empresas e indivíduos explorassem o potencial dos *smart contracts* em uma ampla gama de setores e aplicações (ZHENG *et al*., 2020).

Eles têm sido aplicados em diversos setores, como finanças, logística, propriedade intelectual, governança e até mesmo em jogos online. Um exemplo concreto é a aplicação dos *smart contracts* na rastreabilidade da cadeia de suprimentos agrícola e alimentar na China, que utiliza tecnologia RFID e *blockchain* para garantir a autenticidade e a qualidade dos produtos (TIAN, 2016). O advento dos *tokens* ERC-20 *(Ethereum Request for Comments,* ou Solicitação de Comentários da *Ethereum*) e dos projetos de financiamento descentralizado (DeFi) demonstram como a Ethereum e os contratos inteligentes podem ser utilizados para criar novos modelos de negócio e soluções inovadoras para problemas complexos (ZHENG et al., 2020).

3.2 Aplicações e exemplos concretos de *smart contracts*

A utilização de *smart contracts* em finanças e criptomoedas representa uma verdadeira revolução no modo como as transações financeiras são realizadas. A

adoção dessa tecnologia resulta em operações mais transparentes, seguras e eficientes, além de eliminar a necessidade de intermediários.

Em relação às criptomoedas, a plataforma *Ethereum* tem sido pioneira na implementação de *smart contracts*. Com sua linguagem de programação chamada *Solidity*, *Ethereum* permite a criação de aplicações descentralizadas (*dApps*) e contratos inteligentes que podem ser executados automaticamente quando certas condições são atendidas (BUTERIN, 2014). Um exemplo disso é a criação de *tokens ERC-20 (Ethereum Request for Comments,* ou Solicitação de Comentários da *Ethereum*), que são essencialmente *smart contracts* que implementam um conjunto padrão de regras dentro do ecossistema *Ethereum*. Esses *tokens* são frequentemente usados em *Initial Coin Offerings* (ICOs), ou Ofertas Iniciais de Moeda, onde um novo projeto de criptomoeda vende uma parte de seus *tokens* para investidores iniciais.

Outra aplicação relevante dos smart contracts no domínio das criptomoedas é a DeFi (*Decentralized Finance ou* Finanças Descentralizadas). A DeFi utiliza *smart contracts* para criar protocolos financeiros transparentes e abertos que funcionam sem intermediários. Dentro desse ecossistema, encontram-se os protocolos de empréstimo e tomada de empréstimos, trocas descentralizadas (DEXs), *stablecoins*, entre outros (SCHÄR, 2021). Por exemplo, plataformas como Compound e Aave permitem aos usuários emprestar ou tomar empréstimos de criptomoedas com taxas determinadas por algoritmos (SHEVCHENKO, 2020).

As moedas estáveis (*stablecoins*), são criptomoedas projetadas para ter um valor estável em relação a uma moeda fiduciária ou a outros ativos, como commodities. Os *smart contracts* desempenham um papel fundamental na criação e manutenção de moedas estáveis. Um exemplo é a *stablecoin* DAI, criada pela plataforma *MakerDAO*. O DAI é lastreado pelo *Ether (ETH*), a criptomoeda nativa da plataforma *Ethereum*, e seu valor é mantido estável por meio de *smart contracts* que ajustam automaticamente a oferta e a demanda (SCHÄR, 2021). Também existem *stablecoins* lastreadas em moedas oficiais, como o dólar, é o caso da *USDT* e *USDC* (SCHÄR, 2021).

Os *smart contracts* possibilitam a criação de plataformas de empréstimo descentralizadas, nas quais os usuários podem conceder e receber empréstimos diretamente entre si, sem a necessidade de intermediários financeiros tradicionais,

como bancos e instituições financeiras. A plataforma Aave é um exemplo de uma solução de empréstimo baseada em contratos inteligentes, que permite aos usuários obter empréstimos e ganhar juros sobre seus depósitos em criptomoedas (SCHÄR, 2021).

Os contratos inteligentes também podem ser usados para criar mercados de negociação descentralizados, conhecidos como *exchanges* descentralizadas (DEXs). Essas *exchanges* permitem a negociação de criptomoedas e outros ativos digitais diretamente entre os usuários, sem a necessidade de um intermediário centralizado. Um exemplo popular de DEX baseada em contratos inteligentes é a *Uniswap*, que utiliza um modelo de liquidez automatizada para facilitar a negociação de *tokens ERC-20* na plataforma *Ethereum* (SCHÄR, 2021)

No setor financeiro tradicional, os *smart contracts* têm o potencial de transformar a maneira como as transações são realizadas. As aplicações incluem pagamentos, seguros, empréstimos e até mesmo o cumprimento de obrigações contratuais complexas. Por exemplo, os contratos inteligentes podem ser usados para automatizar pagamentos de juros de títulos ou dividendos de ações, eliminando a necessidade de processamento manual e reduzindo o risco de erro humano (MILEV, 2018).

Saindo do setor de finanças e transações, ainda há diversas aplicações em que os *smart contracts* podem ser utilizados, desde governança e votação, propriedade intelectual e direitos autorais, logística, mercado imobiliário, seguros e até em jogos online e colecionáveis digitais.

Eles podem ser aplicados no setor de seguros para automatizar o processo de reivindicação e pagamento de indenizações. Um exemplo é a plataforma *Etherisc*, que oferece seguros descentralizados para voos, onde os pagamentos são acionados automaticamente em caso de atrasos ou cancelamentos, sem a necessidade de intervenção humana (LICORISH, 2022).

Também podem ser utilizados para implementar sistemas de votação transparentes e seguros. Um exemplo é a plataforma Aragon, que permite a criação de organizações descentralizadas autônomas (DAOs), onde os membros podem votar em propostas e tomar decisões coletivamente. Além disso, há a *DVTChain*, uma proposta de mecanismo baseado em *blockchain* que visa garantir a segurança de sistemas de votação digitais (ALVI *et al*., 2022).

Em relação à gestão de cadeias de suprimentos, os contratos inteligentes têm o potencial de melhorar a rastreabilidade dos produtos e aumentar a eficiência operacional. Um exemplo mencionado anteriormente é a aplicação na rastreabilidade da cadeia de suprimentos agrícola e alimentar na China (TIAN, 2016).

Um *smart contract* pode ser configurado para registrar automaticamente cada passo do caminho de um produto, desde sua origem até o consumidor final. Por exemplo, quando um item é produzido, o contrato inteligente pode ser ativado para registrar esse evento na *blockchain*. Quando o item é então transferido para um distribuidor, um novo *smart contract* pode ser executado para registrar essa transação. Assim, é criada uma trilha de auditoria imutável e transparente que pode ser verificada por todas as partes envolvidas.

Além de melhorar a rastreabilidade, os *smart contracts* também podem aumentar a eficiência das cadeias de suprimentos. Eles podem ser programados para executar automaticamente pagamentos ou iniciar processos quando certas condições são atendidas, eliminando a necessidade de processos manuais que podem ser demorados e propensos a erros. Por exemplo, um contrato inteligente pode ser configurado para liberar o pagamento a um fornecedor assim que um produto chega ao seu destino e a entrega é confirmada na *blockchain* (RADMANESH; HAJI, VALILAI, 2023).

No entanto, é importante ressaltar que, apesar das vantagens mencionadas, a adoção de *smart contracts* enfrenta desafios regulatórios significativos, principalmente na harmonização entre a velocidade da inovação tecnológica e a adequação da regulamentação. Além disso, questões de segurança e privacidade também devem ser abordadas para garantir a confiança dos usuários e a integridade das transações.

3.3 Desafios enfrentados pela tecnologia dos contratos inteligentes

Os *smart contracts* prometem uma transformação revolucionária em várias indústrias, mas sua implementação efetiva está intrinsecamente ligada à superação de uma série de desafios técnicos, operacionais e regulatórios.

Um dos principais desafios para seu desenvolvimento e implementação reside nas questões técnicas e de segurança. Em um ambiente *blockchain*, onde a imutabilidade é uma das características principais, a precisão e a segurança do código do contrato se tornam cruciais e a presença de erros ou vulnerabilidades nesse código pode ter consequências significativas.

De acordo com Szabo (1997), a eficácia de um *smart contract* é tão robusta quanto o código em que é baseado. Nesse sentido, qualquer erro de codificação pode ter consequências de longo alcance, pois, uma vez que o contrato é implementado na *blockchain*, não pode ser facilmente modificado ou corrigido.

Um exemplo histórico desse problema é o incidente com a *Decentralized Autonomous Organization* (DAO), ou Organização Autônoma Descentralizada, em 2016. A DAO foi uma organização baseada na rede *Ethereum* que tinha o objetivo de fornecer um novo modelo de organização descentralizada e era controlado por *smart contracts*. No entanto, devido a uma falha no código do contrato, um invasor foi capaz de drenar milhões de dólares em *Ether* (criptomoeda) da organização, ressaltando as vulnerabilidades de segurança possíveis na implementação de contratos inteligentes (MORRIS, 2023).

Além disso, a segurança da própria plataforma *blockchain* é fundamental para a execução confiável dos *smart contracts*. Ataques à rede, como o ataque de 51%, onde uma entidade ganha controle da maioria dos recursos de mineração, podem comprometer a integridade da *blockchain* e, por extensão, dos contratos inteligentes nela hospedados.

Portanto, embora os *smart contracts* ofereçam potencial para automatizar e garantir a execução de acordos, a superação dos problemas técnicos e de segurança é um passo crucial para a sua adoção mais ampla.

A interoperabilidade entre diferentes plataformas *blockchain*, capacidade dos sistemas se comunicarem e trabalharem efetivamente juntos, é outro desafio significativo. Com várias plataformas oferecendo suporte para contratos inteligentes, cada uma com sua própria linguagem de programação e conjunto de recursos, a comunicação eficaz entre contratos em diferentes *blockchains* pode ser um obstáculo, conforme destacado por Mougayar (2016).

Cada plataforma *blockchain*, seja *Ethereum*, *Bitcoin* ou outras, tem sua própria linguagem de codificação e protocolos. Isso significa que os *smart contracts*

escritos para uma plataforma específica não podem ser diretamente transplantados para outra. Esta falta de padronização pode ser um obstáculo para a adoção em massa de contratos inteligentes, pois reduz a flexibilidade e a escalabilidade potencial do seu uso em diferentes plataformas (HELAL; ALSOUD; ALSHAREEF, 2022).

Ainda mais desafiador é permitir que *smart contracts* em diferentes *blockchains* interajam uns com os outros. Embora haja esforços para construir pontes e protocolos de interoperabilidade entre diferentes plataformas, essa ainda é uma área de pesquisa ativa e um problema técnico complexo a ser resolvido (HELAL; ALSOUD; ALSHAREEF, 2022).

Além disso, a interoperabilidade não é apenas um desafio técnico, mas também um organizacional. Diferentes *blockchains* podem ser administradas por diferentes organizações ou comunidades, cada uma com sua própria governança e política. Portanto, para alcançar a interoperabilidade completa, também é necessário encontrar um terreno comum a nível organizacional e político (HELAL; ALSOUD; ALSHAREEF, 2022).

A superação desse desafio é crucial para o futuro dos *smart contracts*, já que a interoperabilidade melhoraria a sua utilidade e eficiência, permitindo que contratos inteligentes comuniquem-se e interajam entre diferentes plataformas *blockchain* (HELAL; ALSOUD; ALSHAREEF, 2022).

No cenário legal e regulatório, a natureza global e descentralizada da *blockchain* e dos *smart contracts* pode criar obstáculos para a aplicação de leis e regulamentos existentes. Por exemplo, determinar a jurisdição aplicável pode ser desafiador quando as partes envolvidas em um *smart contract* estão localizadas em diferentes países. Em uma *blockchain* pública e descentralizada, é difícil determinar onde ocorrem as transações e, portanto, qual jurisdição ou conjunto de regras se aplicam (TAPSCOTT; TAPSCOTT, 2016).

Ademais, a natureza autônoma dos contratos inteligentes também levanta questões sobre responsabilidade e resolução de disputas. No caso de algo dar errado, pode ser difícil determinar quem é responsável. Por exemplo, se um *smart contract* não executar conforme o esperado devido a um erro de codificação, a responsabilidade seria do desenvolvedor que escreveu o código, da plataforma que executa o código, ou das partes que entraram no contrato?

A resolução de disputas é outra área problemática. Tradicionalmente, contratos são interpretados e disputas são resolvidas por juízes em um tribunal. No entanto, contratos inteligentes, como códigos de computador, não são facilmente interpretáveis por humanos sem conhecimento técnico. Além disso, dada a natureza imutável e autônoma dos *smart contracts*, pode ser difícil corrigir ou reverter uma transação uma vez que seja executada (TAPSCOTT; TAPSCOTT, 2016).

A ambiguidade regulatória também pode desacelerar a adoção de *smart contracts*. A ausência de diretrizes claras ou a presença de regulamentos contraditórios em diferentes jurisdições pode desencorajar empresas e indivíduos de adotarem a tecnologia por medo de futuras implicações legais.

Apesar desses desafios, a integração bem-sucedida do direito e da regulamentação com a tecnologia *blockchain* e *smart contracts* é crucial para a adoção em massa e a realização do potencial transformador dessas tecnologias.

Sendo assim, o último desafio, mas não menos importante, reside na adoção dessas tecnologias. A adoção em massa de qualquer tecnologia nova e disruptiva enfrenta uma série de desafios, e com os *smart contracts* não é diferente. Um desses desafios é a falta de conhecimento e compreensão da tecnologia *blockchain* e dos contratos inteligentes por parte do público em geral, das empresas e até mesmo de legisladores e reguladores (MOUGAYAR, 2016).

Embora essas tecnologias tenham o potencial de transformar várias indústrias, a complexidade envolvida pode ser um obstáculo significativo para a sua adoção. Para muitas pessoas, os conceitos de *blockchain* e contratos inteligentes são abstratos e difíceis de entender. A falta de conhecimento e compreensão dessas tecnologias pode gerar desconfiança e relutância em adotá-las.

Além disso, a implementação de *smart contracts* exige um conhecimento técnico especializado na programação de contratos e na operação de plataformas *blockchain*. Atualmente, há uma escassez de profissionais com o conhecimento e as habilidades necessárias para desenvolver e implementar *smart contracts* eficazes.

Também há resistência à mudança por parte de empresas e instituições estabelecidas. Muitas indústrias têm sistemas e processos já definidos que funcionam com base em contratos tradicionais. A transição para *smart contracts* pode exigir mudanças significativas nessas estruturas e processos existentes, o que pode gerar resistência.

Ainda assim, o potencial transformador dos *smart contracts* é indiscutível. À medida que a tecnologia amadurece e os desafios são superados, é provável que vejamos uma adoção cada vez mais difundida de contratos inteligentes em diversos setores.

4. REGULAMENTAÇÃO DOS *SMART CONTRACTS*

Embora o potencial disruptivo e inovador dos *smart contracts* seja indiscutível, a necessidade de um quadro regulatório que rege sua aplicação não pode ser ignorada. A falta de uma estrutura legal clara para contratos inteligentes pode criar um ambiente de incerteza e risco legal, o que pode limitar sua adoção e uso em larga escala.

A necessidade de regulamentação surge em grande parte devido à natureza autônoma dos *smart contracts*. Este nível de automação pode levar a complicações legais, especialmente em situações onde o resultado do contrato não foi o esperado ou desejado por uma ou ambas as partes (SKLAROFF, 2017). A capacidade de operar além das fronteiras nacionais também traz a necessidade de uma abordagem harmonizada à regulamentação para evitar conflitos de leis e garantir a certeza jurídica (WRIGHT; DE FILIPPI, 2018).

Além disso, é importante notar que nem todos os países sentem a necessidade de criar um novo marco regulatório para lidar com os contratos inteligentes. Por exemplo, no Reino Unido, a *Law Commission* concluiu que a atual legislação comercial e de contratos é suficientemente robusta para enfrentar os desafios apresentados pelos *smart contracts*. Eles argumentam que os princípios legais fundamentais que regem os contratos tradicionais também são aplicáveis a eles (UK LAW COMMISSION, 2021).

De todo modo, a questão da regulamentação dos *smart contracts* continua a ser uma área de discussão em alta em muitos países e que cresce a cada dia no Brasil. Neste capítulo será discutido como o tema tem sido visto no país, quais os projetos de lei em discussão e se a legislação brasileira atual contempla as principais questões envolvendo os contratos inteligentes, além de trazer as abordagens em diferentes jurisdições ao redor do mundo e quais as tendências globais na regulamentação dos *Smart Contracts.*

4.1. Regulamentação dos *Smart Contracts* no Brasil

No Brasil, a regulamentação dos *smart contracts* ainda está em fase embrionária, e até o momento, não há uma legislação específica que trate

especificamente do tema. No entanto, algumas iniciativas já foram apresentadas no Congresso Nacional, destacando-se o Projeto de Lei nº 2303/2015, que deu origem à Lei nº 14.478/2022, e o PL nº 954/2022, além de outros projetos de lei que visam regulamentar as moedas virtuais e os contratos inteligentes.

4.1.1 Projeto de Lei nº 2303/2015 e Lei n. 14.478/2022

O Projeto de Lei nº 2303/2015, de autoria do Deputado Federal Aureo Ribeiro, visava regulamentar as moedas virtuais e os contratos inteligentes no Brasil (CÂMARA DOS DEPUTADOS, 2015). O projeto de lei propunha a criação de um arcabouço regulatório específico para as criptomoedas e os *smart contracts*, estabelecendo diretrizes para a atuação das empresas que oferecem serviços relacionados a essas tecnologias.

O PL 2303/2015 sugeria, entre outras medidas, a criação de uma autoridade reguladora para o setor de moedas virtuais e contratos inteligentes e a obrigação das empresas de realizar o registro de suas operações no país. Além disso, o projeto de lei previa a implementação de mecanismos de controle e fiscalização por parte do Banco Central, da Comissão de Valores Mobiliários (CVM) e do Conselho de Controle de Atividades Financeiras (COAF).

O PL em questão deu origem à Lei 14.478/22, que institui a regulamentação das criptomoedas no Brasil, e foi aprovada no dia 21 de dezembro de 2022. Ela estabelece diretrizes a serem observadas na prestação de serviços de ativos virtuais e na regulamentação desses prestadores de serviços. Também altera o Código Penal e inclui o crime de fraude utilizando ativos virtuais, valores mobiliários e ativos financeiros (BRASIL, 2022).

O objetivo desse marco legal é regular o mercado de criptoativos no país. Define-se ativo virtual como qualquer "representação digital de valor que pode ser negociada ou transferida eletronicamente e utilizada para realização de pagamentos ou com propósito de investimento" (BRASIL, 2022).

A lei prevê diretrizes para a prestação de serviços virtuais, levando em consideração a livre iniciativa e livre concorrência, boas práticas de governança, transparência nas operações, segurança da informação e proteção de dados pessoais, proteção e defesa dos consumidores e usuários e a prevenção à lavagem

de dinheiro e ao financiamento ao terrorismo. A expectativa é que o órgão regulador seja o Banco Central do Brasil (LEAL, 2023).

Prestadoras de serviços de ativos virtuais são definidas como entidades jurídicas que realizam, em nome de terceiros, pelo menos um dos serviços de ativos virtuais listados na lei. A lei também introduz um novo tipo de fraude na prestação de serviços virtuais, valores mobiliários ou ativos financeiros no Código Penal, punível com prisão de quatro a oito anos e multa (BRASIL, 2022).

Este marco regulatório chega em um momento crucial, pois estabelece regras quanto às responsabilidades das agências prestadoras de serviços virtuais e do futuro órgão regulador. Ele tem o potencial de aumentar a confiança dos investidores ao fornecer mais segurança e transparência e prevenir atividades ilegais (LEAL, 2023).

No entanto, ainda que seja um avanço, a lei aprovada não menciona explicitamente os *smart contracts* e foca apenas na regulação das criptomoedas, sem abranger também os *tokens* não fungíveis (NFTs) e *tokens* de segurança.

4.1.2 Projeto de Lei nº 954/2022

A mais recente proposta legislativa que trata da regulamentação dos contratos inteligentes no Brasil é o Projeto de Lei nº 954/2022. Idealizado pelo Deputado Federal Luizão Goulart (Solidariedade-PR), o projeto sugere alterações no Código Civil para permitir o uso de tecnologias na validação e autenticação de contratos atípicos, aqueles que não possuem forma geral prevista em lei (CÂMARA DOS DEPUTADOS, 2022).

Na prática, a proposta legislativa busca autorizar o uso de contratos autoexecutáveis ou *smart contracts*, em casos específicos. Esses contratos inteligentes utilizam tecnologias como *blockchain* e criptografia para validação e autenticação das informações, dispensando intermediários, como os cartórios.

O autor do projeto de lei acredita que, por trazer comandos de forma automática, sem precisar envolver terceiros, esse tipo de contrato vem animando empresas e setores da economia em razão da redução de custos e da burocracia (CÂMARA DOS DEPUTADOS, 2022).

A tramitação do PL será analisada, em caráter conclusivo, pela Comissão de Constituição e Justiça e de Cidadania.

4.1.3 Outros projetos de lei e considerações

Além dos PL 2303/2015 e PL 954/2022, outros projetos de lei também tratam da regulamentação das moedas virtuais e dos contratos inteligentes, como o PL nº 3825/2019, que visa criar um ambiente regulatório favorável ao desenvolvimento e à adoção dessas tecnologias no Brasil (SENADO FEDERAL, 2019). O projeto, de autoria do Senador Flávio Arns, propõe a criação de um marco legal específico para a utilização de *blockchain*, contratos inteligentes e criptomoedas, com o objetivo de estimular a inovação e o empreendedorismo no setor.

Tais projetos de lei ainda estão em tramitação no Congresso Nacional e, caso sejam aprovados, poderão trazer maior segurança jurídica e previsibilidade para a utilização de contratos inteligentes no Brasil. Contudo, é importante ressaltar que a regulamentação de tecnologias emergentes é um processo complexo e dinâmico, que demanda discussões aprofundadas e a participação de diferentes atores, como legisladores, reguladores, academia, setor privado e sociedade civil.

Diante do cenário atual, é fundamental que os debates em torno da regulamentação dos *smart contracts* no Brasil continuem, levando em consideração os desafios e oportunidades que essa tecnologia oferece. A aprovação de uma legislação específica poderá contribuir para o desenvolvimento do setor, além de garantir segurança jurídica e proteção aos direitos dos usuários e partes envolvidas.

Além das iniciativas legislativas mencionadas, destaca-se a importância da colaboração entre os diferentes atores envolvidos na discussão sobre a regulamentação dos *smart contracts*. Esse processo pode envolver a realização de consultas públicas, audiências e debates, que permitam a construção de um arcabouço regulatório eficiente e adequado à realidade brasileira.

A evolução da regulamentação dos contratos inteligentes no Brasil depende não apenas da aprovação de leis específicas, mas também da capacidade do sistema jurídico de acompanhar as mudanças tecnológicas e adaptar-se às novas realidades. Nesse sentido, é determinante que os profissionais do direito, assim

como os demais atores envolvidos, busquem atualizar-se constantemente sobre as inovações tecnológicas e seus impactos no campo jurídico.

Com isso em tela, a ausência de legislação específica sobre *smart contracts* no Brasil representa um desafio para a consolidação dessa tecnologia no país. No entanto, os projetos de lei em tramitação no Congresso Nacional e as discussões em torno do tema indicam que avanços estão sendo realizados nesse sentido. A construção de um marco regulatório adequado e eficiente é importante para garantir segurança jurídica e proteção aos direitos dos usuários e partes envolvidas nos contratos inteligentes.

Contudo, apesar dos benefícios potenciais, existem algumas críticas e preocupações em relação aos *smart contracts*. Por exemplo, eles não substituirão os parâmetros regulares do direito contratual, mas se aplicam a circunstâncias restritas e específicas (NOBREGA; CAVALCANTI, 2020). Além disso, a criação de contratos inteligentes em um ambiente volátil ou com um alto nível de incerteza pode ser muito cara.

Apesar desses desafios, acredita-se que a *blockchain* e os *smart contracts* podem provocar uma grande disrupção na teoria da informação e na abordagem de contratos incompletos, melhorando a contratualidade e a distribuição de informações.

4.1.4 Aplicação do Código Civil e do CDC aos *smart contracts*

Embora o Brasil ainda não possua legislação específica para os *smart contracts*, é possível aplicar normas já existentes no Código Civil (CC) e no Código de Defesa do Consumidor (CDC) a esses contratos. A interpretação e a aplicação dessas normas aos *smart contracts* podem fornecer um arcabouço jurídico provisório para tratar questões relativas à validade, eficácia e responsabilidade civil decorrentes desses contratos.

O Código Civil brasileiro estabelece os princípios e regras gerais que regem os contratos, como a liberdade de contratar, a autonomia da vontade, a boa-fé e a obrigatoriedade do cumprimento das obrigações (BRASIL, 2002). Tais princípios podem ser aplicados aos *smart contracts*, uma vez que esses contratos também são

baseados na manifestação da vontade das partes e visam a estabelecer direitos e obrigações entre elas.

No que diz respeito à validade dos *smart contracts*, o Código Civil estabelece que um contrato é válido quando preenche os requisitos de agente capaz, objeto lícito e determinado ou determinável e forma prescrita ou não defesa em lei (BRASIL, 2002, art. 104). Assim, desde que esses requisitos sejam atendidos, os contratos inteligentes podem ser considerados válidos no Brasil.

O Código de Defesa do Consumidor (CDC) também pode ser aplicado aos *smart contracts*, especialmente quando a relação jurídica estabelecida envolve um consumidor e um fornecedor de produtos ou serviços (BRASIL, 1990). Nesse contexto, os contratos inteligentes que envolvam relações de consumo estão sujeitos às normas protetivas estabelecidas pelo CDC, como a obrigação de informação, a proteção contra cláusulas abusivas e a responsabilidade civil do fornecedor.

A aplicação do CDC aos contratos inteligentes pode garantir maior proteção aos consumidores que utilizam essa tecnologia, uma vez que as normas protetivas do código visam equilibrar a relação entre clientes e fornecedores e assegurar o respeito aos direitos dos consumidores.

4.1.5 Desafios na aplicação das normas existentes

Apesar da aplicação do Código Civil e do CDC aos *smart contracts* ser possível, existem desafios relacionados à interpretação e adaptação dessas normas às particularidades dessa tecnologia. Os contratos inteligentes são baseados em código computacional e são executados de forma automática e autônoma, o que pode gerar dificuldades na análise de questões como a manifestação da vontade das partes, a interpretação das cláusulas contratuais e a responsabilização em casos de falhas ou vícios na execução do contrato.

Além disso, os *smart contracts* operam em um ambiente descentralizado e global, o que pode gerar conflitos de jurisdição e dificuldades na aplicação das normas nacionais. Nesse sentido, é fundamental que os profissionais do direito e os legisladores busquem compreender as especificidades dos contratos inteligentes e desenvolvam soluções jurídicas adequadas para lidar com esses desafios.

4.1.6 Necessidade de legislação específica

A aplicação do Código Civil e do CDC aos contratos inteligentes, embora possa fornecer um arcabouço jurídico provisório, não é suficiente para abordar todos os aspectos específicos dessa tecnologia. A criação de uma legislação específica para os *smart contracts* no Brasil poderia trazer maior segurança jurídica, previsibilidade e eficácia para esses contratos, além de contribuir para o desenvolvimento do setor e a consolidação dessa tecnologia no país.

Uma legislação específica poderia abordar questões como a definição e classificação dos *smart contracts*, a identificação das partes e a atribuição de responsabilidades, a solução de conflitos de jurisdição e a aplicação de normas de proteção ao consumidor, entre outros aspectos. Além disso, a elaboração de uma legislação específica poderia incentivar o diálogo entre os diferentes atores envolvidos, como legisladores, reguladores, academia, setor privado e sociedade civil, favorecendo a construção de um arcabouço jurídico eficiente e adequado à realidade brasileira.

Sendo assim, a aplicação do Código Civil e do CDC aos *smart contracts* representa uma solução provisória para a ausência de legislação específica no Brasil. Contudo, a criação de um marco regulatório específico para os contratos inteligentes é fundamental para garantir segurança jurídica e proteção aos direitos dos usuários e partes envolvidas, além de estimular o desenvolvimento e a adoção dessa tecnologia no país.

4.1.7 *Smart contracts* como contratos eletrônicos e a Lei do Marco Civil da Internet

A Lei do Marco Civil da Internet (Lei nº 12.965/2014) estabelece os princípios, garantias, direitos e deveres para o uso da internet no Brasil (BRASIL, 2014). Embora não trate especificamente dos *smart contracts*, essa lei pode ser aplicada a eles, uma vez que são contratos eletrônicos que funcionam com base em código computacional e são executados em redes de computadores, como a internet.

Os *smart contracts* podem ser enquadrados como contratos eletrônicos, já que são acordos criados e executados por meio de sistemas eletrônicos, como a *blockchain*. Essa tecnologia permite que as partes envolvidas celebrem contratos sem a necessidade de interação física ou presença de intermediários, reduzindo custos e aumentando a eficiência das transações.

De acordo com a Lei do Marco Civil da Internet, os contratos eletrônicos gozam da mesma validade e eficácia dos contratos celebrados por escrito, desde que atendam aos requisitos legais e sejam capazes de assegurar a integridade e a autenticidade das informações trocadas (BRASIL, 2014, art. 10, §1º). Assim, os *smart contracts* podem ser considerados válidos e eficazes no Brasil, desde que preencham os requisitos previstos na legislação.

A Lei nº 12.965/2014 também estabelece normas para a proteção dos dados pessoais dos usuários e a privacidade na internet (BRASIL, 2014). Essas normas podem ser aplicadas aos *smart contracts*, especialmente no que diz respeito à coleta, armazenamento, tratamento e compartilhamento de informações pessoais dos usuários envolvidos nesses contratos.

É importante destacar que, além da Lei do Marco Civil da Internet, a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) também é aplicável aos *smart contracts* e estabelece princípios, direitos e deveres relacionados ao tratamento de dados pessoais no Brasil (BRASIL, 2018). Portanto, os contratos inteligentes devem estar em conformidade com as normas previstas nessas leis, a fim de garantir a proteção dos dados pessoais e a privacidade dos usuários.

Um artigo publicado na Revista Eletrônica do Ministério Público do Estado do Piauí relacionou a Lei Geral de Proteção de Dados Pessoais (LGPD) com os *Smart Contracts* e concluiu que “a proteção jurídica introduzida pela LGPD, no que se refere ao direito do titular quanto à exclusão de seus dados é ineficiente nesses novos contratos tecnológicos” (ALVES; CAVALCANTE; BENTO, 2021). Isso traz à tona um dos desafios que envolve a segurança de dados e a implementação dos contratos inteligentes.

A aplicação da Lei do Marco Civil da Internet aos *smart contracts* também pode trazer alguns desafios, principalmente devido às características descentralizadas e globais dessa tecnologia. Por exemplo, pode ser difícil determinar a jurisdição aplicável e as autoridades competentes para fiscalizar e

regular os contratos inteligentes, bem como garantir a proteção dos direitos dos usuários.

Além disso, eles podem apresentar questões técnicas e jurídicas complexas, que exigem conhecimento específico e atualizado por parte dos profissionais do direito e dos reguladores. Esses desafios reforçam a necessidade de criação de uma legislação específica no Brasil, capaz de abordar as particularidades dessa tecnologia e fornecer um arcabouço jurídico adequado e eficiente.

Embora a Lei nº 12.965/2014 possa ser aplicada aos *smart contracts* como contratos eletrônicos, é importante considerar a necessidade de adaptação e atualização dessa legislação para abordar os desafios específicos apresentados por essa tecnologia. O desenvolvimento de normas e diretrizes específicas para os contratos inteligentes poderia complementar as disposições existentes no Marco Civil da Internet e proporcionar maior segurança jurídica e previsibilidade para as partes envolvidas.

Nesse sentido, é fundamental que legisladores, reguladores, profissionais do direito e demais atores envolvidos na discussão sobre a regulamentação dos *smart contracts* no Brasil busquem compreender as especificidades dessa tecnologia e trabalhem juntos para desenvolver soluções jurídicas adequadas e eficientes.

O enquadramento dos *smart contracts* como contratos eletrônicos segundo a Lei do Marco Civil da Internet representa mais uma solução provisória para a ausência de legislação específica no Brasil. Contudo, a criação de um marco regulatório específico é fundamental para garantir segurança jurídica e proteção aos direitos dos usuários e partes envolvidas, além de estimular o desenvolvimento e a adoção dessa tecnologia no país.

4.1.8 Adaptação do sistema jurídico aos *smart contracts*

A crescente adoção de contratos inteligentes e outras tecnologias disruptivas no âmbito jurídico exige uma adaptação do sistema jurídico brasileiro. Profissionais do direito, legisladores, reguladores e demais atores envolvidos na discussão sobre a regulamentação dos *smart contracts* no Brasil devem trabalhar juntos para enfrentar os desafios apresentados por essa tecnologia e garantir a eficiência e a segurança das relações contratuais.

A compreensão das particularidades dos *smart contracts* e das tecnologias subjacentes, como a *blockchain*, é fundamental para os profissionais do direito que atuam nessa área. Advogados, juízes, promotores e outros profissionais do direito precisam adquirir conhecimentos técnicos e jurídicos atualizados para lidar com questões relacionadas aos contratos inteligentes.

Universidades, escolas de direito e outras instituições de ensino devem incluir em seus currículos disciplinas relacionadas à tecnologia e ao direito digital, a fim de formar profissionais capacitados para atuar nesse campo. Além disso, cursos de atualização e treinamentos específicos sobre *smart contracts* e outras tecnologias emergentes devem ser oferecidos aos profissionais já atuantes no mercado.

Como mencionado anteriormente, a criação de um marco regulatório específico para os *smart contracts* é fundamental para garantir segurança jurídica e proteção aos direitos dos usuários e partes envolvidas. Legisladores e reguladores devem trabalhar em conjunto para desenvolver leis e normas que abordem as especificidades dos contratos inteligentes e outras tecnologias disruptivas.

Esse processo deve envolver um diálogo aberto e colaborativo entre os diferentes atores, como legisladores, reguladores, academia, setor privado e sociedade civil, a fim de garantir a construção de um arcabouço jurídico eficiente e adequado à realidade brasileira.

Considerando que a natureza descentralizada e global dos *smart contracts* pode gerar conflitos de jurisdição e dificuldades na aplicação das normas nacionais, também é importante desenvolver mecanismos de solução de conflitos específicos para lidar com disputas envolvendo contratos inteligentes.

A mediação e a arbitragem podem ser alternativas eficientes e flexíveis para solucionar conflitos relacionados a esse tipo de tecnologia, especialmente quando envolvem partes de diferentes jurisdições. Além disso, a criação de tribunais especializados em tecnologia e direito digital pode contribuir para a rápida resolução de disputas e garantir a aplicação de normas específicas aos *smart contracts*.

O desenvolvimento de pesquisas e inovações relacionadas aos *smart contracts* e outras tecnologias disruptivas é fundamental para garantir a evolução do sistema jurídico brasileiro. Universidades, institutos de pesquisa e entidades governamentais devem incentivar a realização de estudos e projetos que busquem

compreender as implicações jurídicas e tecnológicas dos contratos inteligentes e propor soluções adequadas aos desafios apresentados por essa tecnologia.

O fomento à pesquisa e inovação pode incluir a criação de programas de financiamento, parcerias público-privadas e incentivos fiscais para projetos relacionados aos *smart contracts* e ao direito digital. Além disso, é importante promover a cooperação internacional e o intercâmbio de conhecimentos entre pesquisadores, profissionais e instituições de diferentes países, a fim de garantir a construção de um arcabouço jurídico global e harmonizado para os contratos inteligentes.

Ademais, a adaptação do sistema jurídico aos *smart contracts* também passa pelo envolvimento e conscientização da sociedade em relação a essa tecnologia e suas implicações legais. Campanhas de informação e esclarecimento sobre contratos inteligentes, seus benefícios e riscos, bem como seus aspectos jurídicos, podem contribuir para a formação de uma opinião pública informada e para a construção de um ambiente regulatório favorável à adoção e desenvolvimento dessa tecnologia.

Em suma, a adaptação do sistema jurídico brasileiro aos contratos inteligentes envolve uma série de iniciativas que abrangem a formação e capacitação dos profissionais do direito, a atualização da legislação, o desenvolvimento de mecanismos de solução de conflitos, o fomento à pesquisa e inovação e a conscientização e engajamento da sociedade. Essas ações são fundamentais para garantir a eficiência e segurança das relações contratuais e estimular o desenvolvimento e a adoção dos *smart contracts* no Brasil.

4.2 Regulamentação e validade dos *smart contracts* no Direito Estrangeiro

Embora alguns países, como o Reino Unido, possam considerar que suas leis atuais são suficientes para lidar com os desafios dos *smart contracts*, muitos outros estão ativamente explorando a necessidade de regulações específicas. Essas novas regulamentações seriam capazes de enfrentar os desafios inerentes à tecnologia *blockchain* e sua aplicação em contratos inteligentes, permitindo, ao mesmo tempo, o melhor aproveitamento de suas vantagens.

Vários países já realizaram movimentos significativos em direção à regulamentação dos *smart contracts*, incluindo os Estados Unidos, Japão e Singapura, além do bloco econômico da União Europeia. A análise das características distintivas dessas abordagens e suas implicações para o futuro dos contratos inteligentes no cenário jurídico global são de suma importância para entender como o Brasil pode se posicionar sobre o tema.

4.2.1 Estados Unidos da América

Nos Estados Unidos, a regulamentação e a validade dos *smart contracts* são abordadas em diferentes níveis, tanto federal quanto estadual. A seguir, são apresentados alguns aspectos relevantes da regulamentação dos contratos inteligentes no país.

No âmbito federal, a validade dos *smart contracts* pode ser respaldada pelo *Electronic Signatures in Global and National Commerce Act (E-Sign Act*), promulgada em 2000. O *E-Sign Act* estabelece que um contrato ou assinatura eletrônica não pode ser considerado inválido apenas por ser eletrônico (15 U.S.C. § 7001). Dessa forma, os *smart contracts*, como contratos eletrônicos, podem ser considerados válidos e eficazes nos Estados Unidos, desde que preencham os requisitos legais e sejam capazes de assegurar a integridade e a autenticidade das informações trocadas.

A nível estadual, a maioria dos estados norte-americanos adotou a *Uniform Electronic Transactions Act (UETA)*, que estabelece a validade e a eficácia dos contratos eletrônicos e das assinaturas eletrônicas (*UNIFORM LAW COMMISSION*, 1999). A UETA é compatível com a *E-Sign Act* e fornece um arcabouço jurídico uniforme para a celebração de contratos eletrônicos, incluindo os *smart contracts*.

Além da UETA, alguns estados promulgaram leis específicas relacionadas aos contratos inteligentes e à tecnologia *blockchain*. Por exemplo, o estado do Arizona aprovou uma lei em 2017 que reconhece a validade dos *smart contracts* e estabelece que eles têm a mesma força legal que outros contratos eletrônicos (*ARIZONA REVISED STATUTES*, § 44-7061).

Algumas agências federais dos Estados Unidos, como a *Commodity Futures Trading Commission* (CFTC) e a *Securities and Exchange Commission* (SEC),

também desempenham um papel importante na regulamentação dos *smart contracts*, especialmente quando estão relacionados a ativos digitais, como criptomoedas e *tokens*.

A CFTC, por exemplo, já emitiu orientações sobre a aplicação das leis de commodities aos contratos inteligentes (CFTC, 2018). A SEC, por sua vez, tem analisado casos em que eles são usados para emitir e gerenciar *tokens* que podem ser considerados valores mobiliários, sujeitos à regulamentação da agência.

De modo geral, a regulamentação dos *smart contracts* nos Estados Unidos ainda enfrenta desafios, como a falta de uma abordagem unificada e harmonizada em todo o país. A diversidade de leis estaduais e a atuação de diferentes agências federais podem gerar incertezas e obstáculos para a adoção e desenvolvimento dos contratos inteligentes.

Além disso, assim como no Brasil, os profissionais do direito nos EUA precisam adquirir conhecimentos técnicos e jurídicos atualizados para lidar com questões relacionadas aos *smart contracts*. Universidades, escolas de direito e outras instituições de ensino devem incluir em seus currículos disciplinas relacionadas à tecnologia e ao direito digital, a fim de formar profissionais capacitados para atuar nesse campo.

Também é importante que legisladores, reguladores e demais atores envolvidos na discussão sobre o tema busquem compreender as especificidades dessa tecnologia e trabalhem juntos para desenvolver soluções jurídicas adequadas e eficientes.

Em suma, a regulamentação e a validade dos *smart contracts* nos Estados Unidos são abordadas em diferentes níveis, tanto federal quanto estadual, e envolvem a atuação de várias agências reguladoras. A adoção de uma abordagem unificada e harmonizada para a regulamentação dos contratos inteligentes, bem como a capacitação dos profissionais do direito, são aspectos fundamentais para enfrentar os desafios apresentados por essa tecnologia e garantir a eficiência e a segurança das relações contratuais.

4.2.2 Europa

A regulamentação dos contratos inteligentes na União Europeia (UE) é abordada por meio de diretrizes e regulamentações que buscam harmonizar a legislação dos Estados-membros e criar um ambiente propício para a adoção e desenvolvimento dessa tecnologia.

A Diretiva 1999/93/CE estabeleceu um arcabouço jurídico comum para as assinaturas eletrônicas na UE (PARLAMENTO EUROPEU E CONSELHO DA UNIÃO EUROPEIA, 1999). Embora a diretiva não se refira especificamente aos *smart contracts*, ela é relevante para a validade dos contratos eletrônicos, incluindo aqueles baseados em *smart contracts*. A diretiva foi posteriormente substituída pelo Regulamento (UE) Nº 910/2014 (eIDAS).

O Regulamento (UE) Nº 910/2014, conhecido como eIDAS, estabelece regras para a identificação eletrônica e os serviços de confiança para transações eletrônicas na UE (PARLAMENTO EUROPEU E CONSELHO DA UNIÃO EUROPEIA, 2014). O eIDAS é diretamente aplicável em todos os Estados-membros da UE e prevê a validade legal das assinaturas eletrônicas, selos eletrônicos, horários eletrônicos e outros serviços relacionados. Embora o eIDAS não mencione especificamente os *smart contracts*, ele fornece um arcabouço jurídico que pode ser aplicado a eles, garantindo a validade e a eficácia dos contratos eletrônicos.

A UE também emitiu diretrizes e regulamentações relacionadas a criptomoedas e *tokens*, que podem ser relevantes para a regulamentação de *smart contracts* envolvendo esses ativos digitais. A Diretiva (UE) 2018/843, conhecida como a Quinta Diretiva Anti-Lavagem de Dinheiro (5AMLD), estende as regras de combate à lavagem de dinheiro e financiamento do terrorismo a provedores de serviços de câmbio de criptomoedas e carteiras digitais (PARLAMENTO EUROPEU & CONSELHO DA UNIÃO EUROPEIA, 2018). Além disso, a UE está trabalhando no desenvolvimento de um regime regulatório abrangente para os mercados de criptoativos, conhecido como "MiCA" (Markets in Crypto-assets Regulation).

Na França, a Lei PACTE de 2019 (*Plan d'Action pour la Croissance et la Transformation des Entreprises*) trouxe uma série de inovações no âmbito dos ativos digitais. Incluiu a definição legal de *smart contracts* e estabeleceu um marco

regulatório para *tokens* e ofertas iniciais de moedas (ICOs). Esta abordagem proativa destaca a intenção do governo francês de incentivar a inovação, proporcionando ao mesmo tempo um ambiente regulatório seguro para a operação de contratos inteligentes e outros ativos digitais (NAVACELLE; ZORRILLA; LAPIERRE, 2021).

No Reino Unido, em que pese não fazer mais parte da União Europeia, a Comissão de Direito (*Law Comission*), após uma extensa consulta, concluiu que o atual quadro jurídico é suficiente para lidar com a maioria dos problemas legais que podem surgir com o uso de *smart contracts*. A Comissão afirmou que os princípios legais existentes que governam a formação de contratos, a interpretação de termos contratuais e a resolução de disputas são aplicáveis aos contratos inteligentes. No entanto, eles também reconheceram que algumas áreas, como a identidade e capacidade das partes em um *smart contract*, podem necessitar de maior clareza legal e que uma das maiores problemáticas é definir a jurisdição em uma disputa envolvendo contratos inteligentes, além da dificuldade de identificar onde eles foram formados (LAW COMMISSION, 2021).

De forma geral, a regulamentação dos *smart contracts* na Europa enfrenta desafios semelhantes aos encontrados em outras jurisdições, como a necessidade de adaptação das leis existentes e a formação de profissionais do direito com conhecimento técnico e jurídico adequado. Além disso, a União Europeia precisa garantir a harmonização das regras entre os Estados-membros para criar um ambiente regulatório unificado e coerente para os contratos inteligentes e a tecnologia *blockchain*.

Outro desafio é garantir a proteção dos direitos dos consumidores em transações envolvendo *smart contracts*. A legislação da UE, como a Diretiva 2011/83/UE relativa aos direitos dos consumidores, estabelece normas para garantir que os consumidores sejam informados e protegidos em suas relações contratuais (PARLAMENTO EUROPEU E CONSELHO DA UNIÃO EUROPEIA, 2011). É crucial que essas normas também sejam aplicadas aos contratos inteligentes, garantindo transparência e justiça nas transações eletrônicas.

Além disso, a UE deve considerar a possibilidade de desenvolver uma regulamentação específica para os *smart contracts* e a tecnologia *blockchain*, abordando questões como responsabilidade, resolução de disputas e

interoperabilidade. Esforços nesse sentido já estão em andamento, como o projeto do *European Blockchain Services Infrastructure (EBSI)*, uma iniciativa da Comissão Europeia para desenvolver uma infraestrutura de serviços de *blockchain* segura e confiável para a UE.

Dessa forma, a regulamentação dos contratos inteligentes na União Europeia é atualmente abordada por meio de diretrizes e regulamentações relacionadas a assinaturas eletrônicas, serviços de confiança e criptoativos. Os desafios enfrentados incluem a harmonização das regras entre os Estados-membros, a adaptação das leis existentes e a formação de profissionais do direito com conhecimento técnico e jurídico adequado. A UE também deve garantir a proteção dos direitos dos consumidores em transações envolvendo *smart contracts* e considerar o desenvolvimento de uma regulamentação específica para essa tecnologia.

A UE também pode se inspirar nas abordagens regulatórias de outras jurisdições, como os Estados Unidos e países asiáticos, para desenvolver um arcabouço jurídico eficaz e adaptado às especificidades dos contratos inteligentes e da tecnologia *blockchain*. A cooperação internacional e o diálogo entre os legisladores, reguladores e partes interessadas são fundamentais para garantir a convergência e a harmonização das regras em nível global.

Em última análise, a evolução da regulamentação dos *smart contracts* na União Europeia dependerá da capacidade dos legisladores e reguladores de compreender as implicações e os desafios desta tecnologia emergente e de adaptar a legislação existente de acordo. Ao mesmo tempo, é essencial promover a inovação e o desenvolvimento tecnológico, garantindo que a UE se mantenha na vanguarda das tecnologias de *blockchain* e contratos inteligentes.

Com o avanço das tecnologias de *blockchain* e *smart contracts*, é provável que a UE e os Estados-membros continuem a enfrentar desafios e a adaptar suas regulamentações para garantir um ambiente regulatório eficiente e propício para a inovação e o crescimento econômico. O sucesso desses esforços dependerá da capacidade das autoridades e partes interessadas de trabalhar juntas e desenvolver soluções jurídicas adequadas e eficientes para enfrentar os desafios apresentados por essa tecnologia disruptiva.

4.2.3 Ásia

A Ásia é uma região diversificada, com diferentes abordagens para a regulamentação de *smart contracts* e tecnologia *blockchain*. A seguir, será apresentada uma análise das regulamentações em alguns dos principais países asiáticos.

Na China, adotou-se uma postura cautelosa em relação às tecnologias envolvendo *smart contracts*. Embora o governo chinês tenha reconhecido o potencial da *blockchain*, ele também impôs restrições significativas à sua implementação, especialmente no que diz respeito às criptomoedas.

Em 2017, a China proibiu as Ofertas Iniciais de Moedas (ICOs) e fechou as *exchanges* de criptomoedas (ZHAO, 2017). No entanto, o governo também lançou iniciativas para incentivar o desenvolvimento da tecnologia *blockchain*, como a criação do *Blockchain Service Network* (BSN) e a introdução de um plano nacional para o desenvolvimento dessa tecnologia até 2025 (KHARPAL, 2022).

A regulamentação dos contratos inteligentes na China tem evoluído consideravelmente nos últimos anos. A JD.com, uma das maiores varejistas do país, tem liderado o esforço para elaborar regras sobre como os *smart contracts* podem ser utilizados para automatizar o desembolso de fundos quando um contrato é concluído, bem como serem admitidos em tribunal como prova notarizada (DECRYPT.CO, 2020). Essa iniciativa tem contribuído para a proliferação da tecnologia *blockchain* no país.

O mercado de *smart contracts* na China tem experimentado um crescimento acelerado, impulsionado pela Covid-19 e pela incapacidade das partes se reunirem pessoalmente para negociar termos e fechar negócios. Uma reportagem de Maio da Evergrande Research Institute, o braço de pesquisa de mercado do gigante do desenvolvimento imobiliário Evergrande Group, sugere que os contratos inteligentes são potencialmente a aplicação mais revolucionária da *blockchain* (DECRYPT.CO, 2020).

No Japão, foi adotada uma abordagem mais favorável à tecnologia *blockchain* e aos *smart contracts*. Em 2016, o governo japonês aprovou a Lei de Serviços de Pagamento, que reconhece as criptomoedas como método de pagamento legal e

estabelece um arcabouço regulatório para as *exchanges* de criptomoedas (KOBAYASHI, 2019).

Embora o Japão não tenha uma legislação específica para contratos inteligentes, a Lei de Serviços de Pagamento e outras leis relacionadas, como o Código Civil e o Código Comercial, podem ser aplicadas a esses contratos. Além disso, o governo japonês lançou iniciativas para promover o desenvolvimento da tecnologia *blockchain*, como a *Japan Blockchain Association* (JBA) e o *Japan Virtual Currency Exchange Association* (JVCEA).

Singapura, um dos principais centros financeiros da Ásia, tem sido proativa na adoção e regulamentação da tecnologia *blockchain* e *smart contracts*. A Autoridade Monetária de Singapura (MAS) emitiu diretrizes para a regulamentação de tokens e ICOs e estabeleceu um arcabouço regulatório para provedores de serviços de pagamento que lidam com criptomoedas (SINGAPURA, 2019).

Embora Singapura não possua legislação específica para contratos inteligentes, o país tem um ambiente jurídico favorável para contratos eletrônicos, incluindo *smart contracts*, com base na Lei de Transações Eletrônicas (ETA) (SINGAPURA, 2010). Além disso, Singapura lançou iniciativas para promover a adoção da tecnologia *blockchain*, como a colaboração entre a MAS e a Associação de Bancos de Singapura (ABS) para desenvolver um projeto de pagamentos interbancários baseado em *blockchain* (MAS, 2017).

Em um âmbito geral, a regulamentação dos *smart contracts* na Ásia enfrenta desafios semelhantes aos encontrados em outras regiões, como a necessidade de adaptar leis existentes, proteger os direitos dos consumidores e garantir a segurança e a privacidade das transações. Além disso, a diversidade de abordagens regulatórias na Ásia pode levar a uma fragmentação do mercado e dificultar a cooperação entre os países, visto que a regulamentação dos contratos inteligentes no continente asiático acaba refletindo as diferentes abordagens e prioridades dos governos locais.

No entanto, a Ásia também oferece oportunidades significativas para o desenvolvimento e a adoção de contratos inteligentes e tecnologia *blockchain*. Países como a China, o Japão e Singapura já estão investindo em pesquisa e desenvolvimento nessa área, e há um grande interesse por parte de empresas e investidores na implementação dessas tecnologias. Inclusive Singapura e Japão

assinaram um acordo de cooperação em matéria de inovação de serviços financeiros (MOHANTY, SHIRAKAWA, 2017).

Para aproveitar essas oportunidades e enfrentar os desafios associados, os países asiáticos devem buscar harmonizar suas regulamentações e desenvolver uma abordagem colaborativa para a governança da tecnologia *blockchain* e *smart contracts*. A criação de fóruns regionais, acordos internacionais e parcerias público-privadas pode ser fundamental para promover a inovação e o crescimento econômico nesta área, ao mesmo tempo em que se garante um ambiente regulatório eficiente e propício.

4.3 Tendências globais na regulamentação dos *smart contracts*

Em todo o mundo, a regulamentação dos *smart contracts* ainda está em um estágio embrionário. No entanto, existem tendências emergentes que ajudam a moldar o desenvolvimento e a adoção dessa tecnologia em diferentes jurisdições.

Um número crescente de países está se esforçando para reconhecer a validade jurídica dos contratos inteligentes em suas respectivas legislações. Alguns países, como os Estados Unidos, já têm leis específicas que reconhecem os *smart contracts* como contratos juridicamente vinculativos. Outros países estão explorando a aplicação de leis existentes, como o Código Civil, o Código Comercial e a legislação de contratos eletrônicos, para abordar a validade e aplicabilidade dos *smart contracts*.

Dada a estreita relação entre *smart contracts* e criptomoedas, muitos países estão se concentrando na regulamentação de criptomoedas e *tokens* digitais, o que afeta indiretamente a adoção e a implementação de contratos inteligentes. Alguns países, como o Japão e Singapura, têm legislação específica que trata das criptomoedas e fornece um arcabouço regulatório para o uso de tokens digitais em *smart contracts*. Essa tendência também reflete o esforço dos governos para abordar questões como a lavagem de dinheiro, financiamento do terrorismo e proteção dos investidores.

Governos de todo o mundo estão cada vez mais envolvidos no desenvolvimento e na promoção da tecnologia *blockchain* e *smart contracts*, por meio de iniciativas públicas e parcerias público-privadas. Essas iniciativas incluem a

criação de zonas experimentais e *sandbox* regulatórios, o financiamento de projetos de pesquisa e desenvolvimento e a colaboração com o setor privado para desenvolver infraestruturas e padrões comuns.

Essa natureza global e descentralizada da tecnologia *blockchain* e dos contratos inteligentes levanta a questão da necessidade de harmonização e cooperação internacional na regulamentação dessas tecnologias. Países estão cada vez mais buscando coordenar seus esforços regulatórios e trabalhar juntos para desenvolver abordagens comuns para questões como a validade dos *smart contracts*, a proteção dos consumidores e a segurança das transações. Essa tendência é evidente em fóruns internacionais como a União Europeia, onde os países-membros estão trabalhando juntos para desenvolver uma abordagem harmonizada para a regulamentação dos contratos inteligentes e da tecnologia *blockchain*.

Os *smart contracts* apresentam desafios únicos para o sistema jurídico, como a questão da responsabilidade em caso de falhas no contrato ou a aplicação de princípios contratuais tradicionais, como a boa-fé e a justiça. Para enfrentar esses desafios, os sistemas jurídicos em todo o mundo estão buscando adaptar-se à crescente adoção e implementação dos contratos inteligentes. Isso pode incluir a revisão de leis e regulamentações existentes, a criação de novas normas específicas para *smart contracts* e o desenvolvimento de jurisprudência que aborde questões relacionadas a essa tecnologia.

Como os *smart contracts* e a tecnologia *blockchain* são relativamente novos, a educação e a conscientização são fundamentais para garantir que as partes interessadas, incluindo legisladores, reguladores, profissionais do direito e consumidores, compreendam os princípios básicos e os benefícios dessa tecnologia. Através de programas educacionais, workshops e seminários, governos e organizações internacionais estão trabalhando para aumentar o conhecimento e a compreensão dos contratos inteligentes e de sua regulamentação.

Por fim, a privacidade e a segurança dos dados são preocupações fundamentais na implementação de *smart contracts* e tecnologia *blockchain*. Os países estão buscando abordar essas questões por meio de leis e regulamentações específicas relacionadas à proteção de dados, como o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia (UNIÃO EUROPEIA, 2016), e por

meio de diretrizes e melhores práticas para garantir a segurança das transações e a privacidade dos usuários.

De modo geral, as tendências globais na regulamentação dos contratos inteligentes refletem um esforço conjunto para reconhecer a validade jurídica dessa tecnologia, adaptar o sistema jurídico aos desafios apresentados pelos *smart contracts*, proteger os interesses dos consumidores e investidores, e garantir a privacidade e a segurança das transações. À medida que a adoção e a implementação de *smart contract*s continuam a crescer, é provável que a regulamentação nessa área continue a evoluir e se adaptar às necessidades e desafios emergentes.

5. CONCLUSÃO

Este trabalho se propôs a investigar o impacto das tecnologias disruptivas, focando na regulamentação dos *Smart Contracts* no Brasil. Em meio à rápida evolução das tecnologias disruptivas, especialmente da *blockchain* e dos contratos inteligentes, torna-se evidente que o Direito deve acompanhar tais progressos para assegurar segurança jurídica e eficiência nas relações contratuais.

Quanto aos objetivos específicos, foi possível destacar as principais tecnologias disruptivas envolvidas na *Blockchain*, descrever seu surgimento e impactos, além de analisar os desafios enfrentados pela tecnologia *Blockchain* e a relevância da evolução da *Bitcoin* em seu desenvolvimento.

O estudo também abarcou o surgimento dos contratos inteligentes, expondo sua criação a partir da tecnologia *blockchain Ethereum*. A partir do levantamento das principais aplicações dos *Smart Contracts*, foi possível verificar a sua capacidade disruptiva e importância nos mais diversos segmentos, desde finanças, saúde, logística e tantos outros.

Por fim, identificou-se o cenário da regulamentação dos *Smart Contracts* no Brasil, abordando os projetos de lei que visam à regulação, como se dá a aplicação da legislação vigente e os principais desafios envolvidos. A análise do Direito Estrangeiro demonstrou que o tema é atual e discutido em todo o planeta, com a maioria dos países buscando acompanhar a evolução das tecnologias e discutindo seu sistema legal para adequar-se e abarcar todas as possibilidades que abrangem a utilização dos contratos inteligentes.

A hipótese inicial de que a regulamentação dos *Smart Contracts* é importante para preencher as lacunas existentes na lei nacional se mostrou consistente. A análise conduzida evidencia que, apesar da legislação atual brasileira possuir mecanismos para lidar com os desafios e especificidades trazidas pelos contratos inteligentes e tecnologias disruptivas correlatas, há espaços que poderiam se beneficiar de um marco regulatório específico para os contratos inteligentes.

Portanto, com base nos resultados obtidos na pesquisa, é possível concluir que o estudo contínuo e a atualização da legislação brasileira são importantes para uma melhor adequação à realidade dos *Smart Contracts*. Isso não somente pode

ajudar a garantir maior segurança e eficiência nas relações contratuais, mas também estimular o desenvolvimento dessa e de outras tecnologias.

Este trabalho contribuiu para o entendimento do atual cenário legal, dos desafios e das oportunidades que os *Smart Contracts* apresentam, sugerindo caminhos para um ambiente regulatório coerente e adaptativo no Brasil. Dada a constante evolução da matéria, é imprescindível um acompanhamento e atualização contínuos das discussões acerca da regulamentação dos contratos inteligentes, considerando também a evolução das legislações estrangeiras. A principal contribuição deste trabalho reside em fornecer uma base sólida para futuras discussões acerca do tema, favorecendo o debate e a construção de um ambiente regulatório mais seguro e confiável.

REFERÊNCIAS

ALI, Robleh *et al*. *Innovations in payment technologies and the emergence of digital currencies. Quarterly Bulletin, Bank of England*, Londres, 2014. Disponível em: <https://econpapers.repec.org/article/boeqbullt/0147.htm>. Acesso em 03/11/2022.

ALVES, Denilson D. M.; CAVALCANTE, Albert V. F.; BENTO, Cléa M. C. A relação da Lei Geral de Proteção de Dados e Smart Contracts gerados por blockchain nas empresa. Revista EletrÔnica do Ministério Público do Estado do Piauí, 2021. Disponível em: <https://www.mppi.mp.br/internet/wp-content/uploads/2022/06/A-relac%CC%A7a%CC%83o-da-Lei-Geral-de-Protec%CC%A7a%CC%83o-de-Dados-e-Smarts-Contracts-gerados-por-blockchain-nas-empresas.pdf>. Acesso em: jun. 2023.

ALVI, Syada Tasmia *et al*. *DVTChain: A blockchain-based decentralized mechanism to ensure the security of digital voting system*. Journal of King Saud University - Computer and Information Sciences, v. 34, n. 9, p. 6855-6871, 2022. ISSN 1319-1578. Disponível em: <https://doi.org/10.1016/j.jksuci.2022.06.014.> Acesso em: mai. 2023.

ANTONOPOULOS, Andreas. *Mastering Bitcoin*. O'Reilly Media, 2018.

ANTONOPOULOS, Andreas M.; WOOD, Gavin. *Mastering Ethereum: Building Smart Contracts and dApps*. 1. ed. Sebastopol, CA: O'Reilly Media, 2018.

ARIZONA. Arizona Revised Statutes, § 44-7061. Smart contracts; blockchain technology. 2017. Disponível em: <https://www.azleg.gov/ars/44/07061.htm>. Acesso em: abr. 2023.

BACK, Adam. *Hashcash - a denial of service counter-measure*. 2002. Disponível em: <http://www.hashcash.org/hashcash.pdf> Acesso em nov. 2022.

BASHIR, Imran. *Mastering Blockchain: Distributed Ledger Technology, Decentralization, and Smart Contracts Explained*. 2ª ed. Packt Publishing, 2018.

BECKER, Jörg *et al*. *Can We Afford Integrity by Proof-of-Work? Scenarios Inspired by the Bitcoin Currency. Department of Information Systems*. Universidade de Münster, Alemanha. 2012. Disponível em: <https://www.researchgate.net/publication/242345869_Can_We_Afford_Integrity_by_Proof-of-Work_Scenarios_Inspired_by_the_Bitcoin_Currency>. Acesso em fev. 2023.

BENTOV, Iddo; LEE, Charles; MIZRAHI, Alex; ROSENFELD, Meni. *Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake*. ACM SIGMETRICS Performance Evaluation Review, 2014. Disponível em: <https://eprint.iacr.org/2014/452.pdf>. Acesso em dez. 2022.

BHARATHAN, Vipin. *Blockchain Was Born 20 Years Before Bitcoin. Forbe*s, 2020. Disponível em:

<https://www.forbes.com/sites/vipinbharathan/2020/06/01/the-blockchain-was-born-20-years-before-bitcoin/?sh=32b5efdf5d71>. Acesso em nov. 2022.

BONNEAU, Joseph *et al*. *Research Perspectives on Bitcoin and Second-Generation Cryptocurrencies*. 2015. Disponível em: <https://jbonneau.com/doc/BMCNKF15-IEEESP-bitcoin.pdf> Acesso em nov. 2022.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L8078.htm> Acesso em: dez 2022.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm> Acesso em: dez. 2022.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2014/Lei/L12965.htm> Acesso em dez. 2022.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm> Acesso em dez. 2022.

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. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/L14478.htm>. Acesso em mai. 2023.

BUTERIN, Vitalik. *A Next-Generation Smart Contract and Decentralized Application Platform*. Ethereum White Paper. 2014. Disponível em: <https://ethereum.org/en/whitepaper/>. Acesso em mar. 2023.

CÂMARA DOS DEPUTADOS. Projeto de Lei 954, de 2022. Disponível em: <https://www.camara.leg.br/propostas-legislativas/2320041>. Acesso em: mar. 2023.

CÂMARA DOS DEPUTADOS. Projeto de Lei nº 2303, de 2015. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2166221> Acesso em dez. 2022.

CHRISTIDIS, Kostantinos; DEVETSIKIOTIS, Michael. *Blockchains and Smart Contracts for the Internet of Things*. IEEE Access, v. 4, p. 2292-2303, 2016. Disponível em: <https://ieeexplore.ieee.org/document/7467408>. Acesso em 26 mar. 2023.

COMISSÃO EUROPEIA. *European Blockchain Services Infrastructure (EBSI)*. Disponível em: <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI> Acesso em mar. 2023.

COMMODITY FUTURES TRADING COMMISSION (CFTC). *CFTC releases primer on smart contracts*. 2018. Disponível em: <https://www.cftc.gov/PressRoom/PressReleases/7839-18>. Acesso em: abr. 2023.

CZULEGER, Eric. *Finding the Oldest Blockchain in the New York Times Classifieds*, 2018. Disponível em:<https://crypto.news/finding-the-oldest-blockchain-in-the-new-york-times-classifieds/>. Acesso em 03/11/2022.

DE VRIES, Alex. *Bitcoin's growing energy problem.* Joule 2. 2018. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2542435118301776>. Acesso em fev. 2023.

DECRYPT.CO*. JD.com lays out vision for smart contract laws in China*. Decrypt, 6 ago. 2020. Disponível em: <https://decrypt.co/37780/jd-com-lays-out-vision-for-smart-contract-laws-in-china>. Acesso em mai. 2023.

ESTADOS UNIDOS. *Electronic Signatures in Global and National Commerce Act*. 15 U.S.C. § 7001. 2000. Disponível em: <https://www.law.cornell.edu/uscode/text/15/7001>. Acesso em: abr. 2023.

EYAL, Ittay; SIRER, Emin G. *Majority Is Not Enough: Bitcoin Mining Is Vulnerable*. Department of Computer Science, Cornell University, 2013. Disponível em: <https://arxiv.org/pdf/1311.0243.pdf>. Acesso em dez. 2022.

FERNÁNDEZ-CARAMÉS, T. M.; FRAGA-LAMAS, P. A review on the use of blockchain for the internet of things. *IEEE Access*, v. 7, p. 32979-33001, 2018. Disponível em: <https://ieeexplore.ieee.org/document/8370027.>. Acesso em mar. 2023.

FUNDO MONETÁRIO INTERNACIONAL. *The rise of digital money.* 2019. Disponível em: <https://www.imf.org/en/Publications/fintech-notes/Issues/2019/07/12/The-Rise-of-Digital-Money-47097>. Acesso em mar. 2023.

GONÇALVES, Rubén Miranda; DOMINGOS, Isabela Moreira. Gobernanza Blockchain: tecnología disruptiva para el control de la corrupción en la salud pública. Revista Jurídica Unicuritiba, vol 4, n. 66, p. 31-49. Curitiba, 2021. Disponível em: <https://revista.unicuritiba.edu.br/index.php/RevJur/article/view/5065>. Acesso em jun. 2023.

HABER, Stuart; STORNETTA, W. Scott. *How to time-stamp a digital document. Journal of Cryptology*. 1991. Disponível em <https://link.springer.com/article/10.1007/BF00196791>. Acesso em 31/10/2022.

HABER, Stuart; STORNETTA, W. Scott. *Secure names for bit-strings.* 1995. Disponível em: <https://nakamotoinstitute.org/static/docs/secure-names-bit-strings.pdf>. Acesso em fev. 2023.

HELAL, Maha; ALSOUD, Anas Ratib; ALSHAREEF, Hazzaa. *Cross-Chain interoperability - validating smart contracts to interoperate over diverse blockchain networks using interoperable blockchain framework design*. 2022. Disponível em: <https://www.researchsquare.com/article/rs-2217138/v1>. Acesso em mai. 2023.

KAMIENSKI, Carlos *et al*. Colaboração na Internet e a Tecnologia Peer-to-Peer. In: *XXV Congresso da Sociedade Brasileira de Computaçã*o, 25, 2005. São Leopoldo, Rio Grande do Sul. Disponível em: <https://www.researchgate.net/publication/255653983_Colaboracao_na_Internet_e_a_Tecnologia_Peer-to-Peer>.. Acesso em nov. 2022.

KARAME, Ghassan O.; ANDROULAKI, Elli; CAPKUN, Srdjan. *Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin*. IACR Cryptology ePrint Archive, 2012. Disponível em <https://eprint.iacr.org/2012/248.pdf>. Acesso em dez. 2022.

KHARPAL, Arjun. *China has been quietly building a blockchain platform. Here's what we know*. CNBC, 2022. Disponível em: <https://www.cnbc.com/2022/05/16/china-blockchain-explainer-what-is-bsn-.html>. Acesso em mai. 2023

KHAZAKKA, Michel. *Bitcoin: Cryptopayments Energy Efficiency*. 2022. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4125499>. Acesso em mai. 2023.

KIAYIAS, Aggelos; RUSSELL, Alexander; DAVID, Bernardo; OLIYNYKOV, Roman. *Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol*. In: Annual International Cryptology Conference, 2017. Disponível em: <https://eprint.iacr.org/2016/889.pdf>. Acesso em nov. 2022.

KING, Sunny; NADAL, Scott. *PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake*. 2012. Disponível em: <https://peercoin.net/assets/paper/peercoin-paper.pdf.> Acesso em: jan. 2023.

KOBAYASHI, Eduardo Mesquita. Regulação de criptoativos no Japão - Marco Regulatório, jurisprudência e doutrina. *Revsita de Direito Público da Economia*. NUPEDE, 2019. Disponível em: <https://www.researchgate.net/publication/338779262_Regulacao_de_criptoativos_no_Japao_-_Marco_regulatorio_jurisprudencia_e_doutrina_Cryptoassets_Regulation_in_Japan_-_Legal_framework_case_law_and_theory>. Acesso em mai. 2023.

LAW COMMISSION. *Smart legal contracts - Advice to Government*. 2021. Disponível em: <https://www.lawcom.gov.uk/document/smart-contracts-2/>. Acesso em jun. 2023.

LEAL, Martha. A Lei 14.478/2022, marco regulatório das criptomoedas. Conjur, 2023. Disponível em: <https://www.conjur.com.br/2023-jan-07/martha-leal-lei-1447822-marco-regulatorio-criptomoedas>. Acesso em jun. 2023.

LI, Wenting; ANDREINA, Sebastien; BOHLI, Jens-Matthias; KARAME, Ghassan. *Securing Proof-of-Stake Blockchain Protocols*. 2017. Disponível em: <https://www.researchgate.net/publication/319647471_Securing_Proof-of-Stake_Blockchain_Protocols>. Acesso em fev. 2023

LICORISH, Elizabeth. Etherisc's FlightDelay Transforms Flight Insurance With Chainlink Oracles. Chainlinktoday, 2022. Disponível em: <https://chainlinktoday.com/etheriscs-flightdelay-transforms-flight-insurance-with-chainlink-oracles/>. Acesso em jun. 2023.

MATZUTT, Roman *et al*. *A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin*. In: *Proceedings of the 22nd International Conference on Financial Cryptography and Data Security*, 2018. Disponível em: <https://www.comsys.rwth-aachen.de/fileadmin/papers/2018/2018_matzutt_bitcoin-contents_preproceedings-version.pdf>. Acesso em dez. 2022.

MERKLE, Ralph. *Protocols for public key cryptosystems*. *In 1980 IEEE Symposium on Security and Privacy*. IEEE, 1980. Disponível em: <http://diyhpl.us/~bryan/papers2/bitcoin/Protocols%20for%20public-key%20cryptosystems.pdf>. Acesso em nov. 2022.

MILEV, Angel. *Dividend Tokens*, Explained. CoinTelegraph, 2018. Disponível em: <https://cointelegraph.com/explained/dividend-tokens-explained>. Acesso em jun. 2023.

MOHANTY, Sopnendu; SHIRAKAWA, Shunsuke. *Exchange of Letters on Co-Operation framework between the Financial Services Agency of Japan and the Monetary Authority of Singapore*, 2017. Disponível em: <https://www.fsa.go.jp/en/news/2017/20170313-1/01.pdf>. Acesso em mai. 2023.

MONETARY AUTHORITY OF SINGAPORE (MAS) *Project Ubin: SGD on Distributed Ledger*, 2017. Disponível em: <https://www.mas.gov.sg/-/media/MAS/ProjectUbin/Project-Ubin--SGD-on-Distributed-Ledger.pdf>. Acesso em mai. 2023.

MORA, Camilo *et al*. *Bitcoin emissions alone could push global warming above 2°C.* Nature Clim Change 8, 2018. Disponível em: <https://doi.org/10.1038/s41558-018-0321-8>. Acesso em jun. 2023.

MORRIS, David Z. *CoinDesk Turns 10: 2016 - How The DAO Hack Changed Ethereum and Crypto*. CoinDesk, 2023. Disponível em: <https://www.coindesk.com/consensus-magazine/2023/05/09/coindesk-turns-10-how-the-dao-hack-changed-ethereum-and-crypto/>. Acesso em jun. 2023.

MOUGAYAR, William. *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*. Wiley, 2016.

NAKAMOTO, Satoshi. *Bitcoin: a peer-to-peer electronic cash system. Working Paper*, 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em out. 2022.

NARAYANAN, Arvind *et al*. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press, Estados Unidos da América, 2016. Disponível em: <https://www.lopp.net/pdf/princeton_bitcoin_book.pdf>. Acesso em: mai. 2023.

NAVACELLE, Stéphane de; ZORRILLA, Julie; LAPIERRE, Thomas. *A French law perspective on blockchain technology*, 2021. Disponível em: <https://www.ibanet.org/french-law-blockchain>. Acesso em jun. 2023.

NOBREGA, Marcos R.; CAVALCANTI, Mariana O. de Melo. Smart contracts ou “contratos inteligentes”: o direito na era da blockchain. Revista Científica Disruptiva, [S. l.], v. 2, n. 1, p. 91-118, 2020. Disponível em: <http://revista.cers.com.br/ojs/index.php/revista/article/view/75.> Acesso em: jun. 2023.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). *Blockchain Technology and Competition Policy*. 2018. Disponível em: <https://www.oecd.org/competition/blockchain-and-competition-policy.htm>. Acesso em mar. 2023.

PARLAMENTO EUROPEU. *Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law? European Parliamentary Research Service,* 2019*.* Disponível em: <https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/IPOL_STU(2020)641530_EN.pdf>. Acesso em mar. 2023.

PARLAMENTO EUROPEU E CONSELHO DA UNIÃO EUROPEIA. *Diretiva 1999/93/CE do Parlamento Europeu e do Conselho, de 13 de dezembro de 1999, relativa a um quadro comunitário para as assinaturas eletrônicas.* Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31999L0093>. Acesso em mar. 2023.

PARLAMENTO EUROPEU E CONSELHO DA UNIÃO EUROPEIA. *Regulamento (UE) nº 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, relativo à identificação eletrónica e aos serviços de confiança para transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE*. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32014R0910>. Acesso em mar. 2023.

PARLAMENTO EUROPEU E CONSELHO DA UNIÃO EUROPEIA. *Diretiva (UE) 2018/843 do Parlamento Europeu e do Conselho, de 30 de maio de 2018, que altera a Diretiva (UE) 2015/849 relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo.* Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32018L0843> Acesso em mar. 2023.

PARLAMENTO EUROPEU E CONSELHO DA UNIÃO EUROPEIA. *Diretiva 2011/83/UE do Parlamento Europeu e do Conselho, de 25 de outubro de 2011, relativa aos direitos dos consumidores*. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32011L0083>. Acesso em mar. 2023.

RADMANESH, Seyyed-Alireza; HAJI, Alireza; VALILAI, Omid Fatahi. *Blockchain-Based Architecture for a Sustainable Supply Chain in Cloud Architecture*. Sustainability, v. 15, n. 11, 9072, 2023. Disponível em: <https://doi.org/10.3390/su15119072>. Acesso em: mai. 2023.

ROSENFELD, Meni. *Analysis of Bitcoin Pooled Mining Reward Systems*. 2011. Disponível em: <https://arxiv.org/abs/1112.4980>. Acesso em nov. 2022.

SCHÄR, F. Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets. Review of Financial Economics, v. 105, n. 2, p. 53-71, 2021. Disponível em: <https://research.stlouisfed.org/publications/review/2021/02/05/decentralized-finance-on-blockchain-and-smart-contract-based-financial-markets.>. Acesso em mar. 2023.

SENADO FEDERAL. Projeto de Lei nº 3825, de 2019. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=7973487&ts=1564782337171&disposition=inline>. Acesso em mar. 2023.

SHEVCHENKO, Andrey. Protocolo Aave ultrapassa Maker e Compound e toma liderança entre DeFi. CoinTelegraph, 2020. Disponível em: <https://br.cointelegraph.com/news/the-aave-protocol-beats-maker-and-compound-to-become-1-in-defi-rankings>. Acesso em jun. 2023.

SINGAPURA. *Electronic Transactions Act*, 2010. Disponível em: <https://sso.agc.gov.sg/Act/ETA2010> Acesso em mai. 2023.

SINGAPURA. *Payment Services Act*, 2019. *Monetary Authority of Singapore* (MAS). Disponível em: <https://sso.agc.gov.sg/Acts-Supp/2-2019/Published/20190220?DocDate=20190220>. Acesso em mai. 2023.

STINSON, Douglas. R.; PATERSON, Maura B. *Cryptography: theory and practice*. CRC press, 2018. Disponível em: <https://www.ic.unicamp.br/~rdahab/cursos/mo421-mc889/Welcome_files/Stinson-Pa

terson_CryptographyTheoryAndPractice-CRC%20Press%20%282019%29.pdf>. Acesso em nov. 2022.

STOLL, Christian, KLAAßEN, Lena; GALLERSDÖRFER, Ulrich. *The Carbon Footprint of Bitcoin*. Joule, v. 3, Issue 7, 2019, p. 1647-1661. Disponível em: <https://doi.org/10.1016/j.joule.2019.05.012.> Acesso em jun. 2023.

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

SZABO, Nick. *Formalizing and Securing Relationships on Public Networks*. 1997. Disponível em: <https://nakamotoinstitute.org/formalizing-securing-relationships/>. Acesso em nov. 2022.

SZABO, Nick. *Smart Contracts: Building Blocks for Digital Markets.* 1996. Disponível em: <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html.> Acesso em: jan. 2023.

SZABO, Nick. *Smart contracts: building blocks for digital markets*. Extropy, 16, 18-21. 1996. Disponível em: <https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html> Acesso em jan. 2023.

SZABO, Nick. *The Idea of Smart Contracts*. 1997. Disponível em: <https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html>. Acesso em mai. 2023.

TAPSCOTT, Don; TAPSCOTT, Alex. *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. New York: Portfolio, 2016.

TIAN, F. An Agri-food Supply Chain Traceability System for China Based on RFID & Blockchain Technology. In: *2016 13th International Conference on Service Systems and Service Management (ICSSSM). IEEE, 2016*. p. 1-6. Disponível em: <https://ieeexplore.ieee.org/document/7538424>. Acesso em abr. 2023.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:02016R0679-20160504.>. Acesso em mai. 2023.

UNIFORM LAW COMMISSION. *Uniform Electronic Transactions Act.* 1999. Disponível em: <https://higherlogicdownload.s3-external-1.amazonaws.com/UNIFORMLAWS/21c36

6b3-b11c-d774-f34d-7901ab76e9a5_file.pdf?AWSAccessKeyId=AKIAVRDO7IEREB57R7MT&Expires=1685673627&Signature=pXrSNtCtwIEh67fp3AsRyb7cuHE%3D> Acesso em: abr. 2023.

UNITED NATIONS COMMISSION ON INTERNATIONAL TRADE LAW (UNCITRAL). *Model Law on Electronic Transferable Records*. 2017. Disponível em: <https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/mletr_ebook_e.pdf>. Acesso em mar. 2023.

WOOD, Gavin. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Project Yellow Paper*, 2014. Disponível em: <https://ethereum.github.io/yellowpaper/paper.pdf>. Acesso em: 20 abr. 2023.

WORLD BANK. *Distributed ledger technology and blockchain*. 2020. Disponível em: <https://www.worldbank.org/en/topic/financialsector/brief/blockchain-dlt>. Acesso em mar. 2023.

ZHAO, Wolfie. *China's ICO Ban: A Full Translation of Regulator Remarks*. Coindesk, 2017. Disponível em: <https://www.coindesk.com/chinas-ico-ban-full-translation-regulator-remarks> Acesso em mai. 2023.

ZHENG, Zibin *et al*. *An overview on smart contracts: Challenges, advances and platforms*. Future Generation Computer Systems, v. 110, p. 475-491, 2020. Disponível em: <https://www.sciencedirect.com/science/article/abs/pii/S0167739X19316280> Acesso em abr. 2023.

ZOBEL, Justin; MOFFAT, Alistair. I*nverted files for text search engines*. ACM computing surveys (CSUR), 2006. Disponível em: <https://www.inf.ed.ac.uk/teaching/courses/ad/lectures16/ZobelMoffat.pdf>. Acesso em dez. 2022.

ZOHAR, Aviv; SOMPOLINSKY, Yonatan. Secure high-rate transaction processing in Bitcoin. In: *International Conference on Financial Cryptography and Data Security. Springer*, 2015. p. 507-527. Disponível em: <https://link.springer.com/chapter/10.1007/978-3-662-47854-7_32>. Acesso em: 26 mar. 2023.