O USO DA TECNOLOGIA *BLOCKCHAIN* EM CONTRATOS DE SEGURO DE DANO NO BRASIL

Isabella de Lima França Sousa[1]

RESUMO

O presente artigo aborda sobre o uso da tecnologia *blockchain* em contratos de seguro de dano, tendo como hipótese principal a indagação acerca da validade do uso da tecnologia *blockchain* em contratos de seguro de dano, ou seja, se ela se coaduna com as normas pátrias vigentes no Brasil. Justifica-se a escolha deste tema em razão da diminuta existência de pesquisas jurídicas nacionais sobre o tema e da importância em se investigar esta tecnologia disruptiva, que pode ajudar a tornar a realização de contratos de seguro de dano mais célere, automatizada e confiável sem, contudo, ignorar as dificuldades jurídicas e técnicas a serem superadas posteriormente. Objetiva-se estudar os potenciais usos desta tecnologia em contratos de seguro de dano no Brasil, identificando vantagens e desvantagens relativas à sua utilização. Além do mais objetiva-se conceituar a tecnologia *blockchain*, seu funcionamento e características; conceituar os contratos inteligentes e suas características; conceituar os contratos de seguro de dano, seus elementos e características. No que concerne à metodologia adota-se o método dedutivo e o método hipotético-dedutivo. Dentre os tipos genéricos de investigação, adota-se a jurídico-exploratória, a jurídico-prospectiva e projetiva. A forma de abordagem é qualitativa. Os procedimentos técnicos adotados são: o bibliográfico e o documental. Quanto aos objetivos projetados, trata-se de pesquisa exploratória, pois o tema abordado ainda é pouco investigado. Conclui-se no sentido de que *blockchains* privadas e híbridas se adequam mais às exigências deste ramo de seguros, bem como, que a tecnologia *blockchain* já está sendo utilizada no Brasil, com validade jurídica, como meio remoto para emissão de apólices, boletos e endossos e, por fim, a SUSEP está fomentando o uso desta tecnologia em contratos de seguro de dano por meio da adoção de *sandbox* regulatória, sem olvidar da proteção dos consumidores, da proteção de dados e da prevenção à lavagem de dinheiro.

Palavras-Chave: *Blockchain*. Contratos inteligentes. Direito Contratual. Contrato de seguro de dano.

[1] Advogada. Pós-graduanda em Direito Processual Civil pela Faculdade Ibmec de São Paulo. Graduada em Direito pela Universidade Federal da Bahia.

1 INTRODUÇÃO

Numa sociedade permeada por riscos, o contrato de seguro de dano responde aos anseios humanos por mais segurança patrimonial, por meio da diluição dos prejuízos entre diversos agentes mutuamente, sendo indutor do desenvolvimento social e mercantil. Contudo, a complexidade dos mecanismos de funcionamento deste contrato o encarece e o torna extremamente burocrático.

Paulatinamente, estão sendo desenvolvidas novas tecnologias, como a *blockchain*, com o escopo de contribuir para a diminuição de custos, aumentar a segurança no compartilhamento de ativos na rede mundial de computadores e facilitar os procedimentos de contratação, execução e registro de contratos. Dessa forma, o presente artigo busca analisar o uso da tecnologia *blockchain* em contratos de seguro de dano no Brasil, visando contribuir para a evolução das discussões sobre a matéria no campo do direito.

Este artigo justifica-se, não só, por conta da diminuta existência de pesquisas jurídicas nacionais sobre o tema, mas também, pela importância de investigar esta nova tecnologia que pode tornar a realização de contratos de seguro de dano mais célere, automatizada e confiável sem, contudo, ignorar as dificuldades jurídicas e técnicas a serem superadas posteriormente.

O objetivo geral do artigo será analisar o uso da tecnologia *blockchain* em contratos de seguro de dano no Brasil, identificando vantagens e desvantagens relativas à sua utilização. Os objetivos específicos são: conceituar a tecnologia, seu funcionamento e características; conceituar os contratos inteligentes e suas características; conceituar os contratos de seguro de dano, seus elementos e características.

O presente artigo visa investigar o problema inerente à validade jurídica da utilização dessa tecnologia em contratos de seguro de dano no Brasil. É importante destacar que não se observa um estudo aprofundado acerca deste fenômeno e, por esta razão, faz-se mister analisar se esta tecnologia se coaduna com os valores e dispositivos consagrados pelo ordenamento jurídico pátrio. Com base neste questionamento, a hipótese a ser verificada é de que o uso da tecnologia *blockchain* em contratos de seguro de dano pode se coadunar com as normas pátrias vigentes.

No que concerne à metodologia, para examinar a validade do uso da tecnologia *blockchain* em contratos de seguro de dano adota-se o método dedutivo, partindo da compreensão do ordenamento jurídico para se chegar à conclusão deste caso específico. Por sua vez, para analisar os possíveis usos da tecnologia *blockchain* em contratos de seguro de dano no Brasil utiliza-se o método hipotético-dedutivo, pois a simples indução ou dedução não são satisfatórias para tal investigação. Dentre os tipos genéricos de investigação, adotou-se a jurídico-exploratória, a jurídico-prospectiva e projetiva.

A forma de abordagem é a qualitativa. Os procedimentos técnicos adotados são, a saber: o bibliográfico e o documental, utilizando-se de livros, artigos científicos, reportagens, trabalhos de conclusão de curso e dissertações, adquiridos através de biblioteca pessoal, bem como, através de bibliotecas públicas e de artigos disponíveis na rede mundial de computadores. Quanto aos objetivos projetados, trata-se de pesquisa exploratória, pois o tema abordado ainda é pouco investigado.

2 A TECNOLOGIA *BLOCKCHAIN*

Atualmente, a realidade é captada por computadores e smartphones convertendo-se num amplo espaço de conexões e informações, numa interligação contínua entre o real e o virtual [2].

[2] MARTINO, Luís Mauro Sá. *Teoria das Mídias Digitais. Linguagens, ambientes e redes.* 2ª Edição. Rio de Janeiro: Vozes, 2015, p.10.

O avanço dos estudos no campo da criptografia possibilitou o surgimento de uma tecnologia com potencial disruptivo, conhecida como *blockchain*, que foi criada em 2008, quando uma pessoa ou organização com o pseudônimo Satoshi Nakamoto publicou um artigo descrevendo esta tecnologia que viabilizaria a *bitcoin*, uma moeda virtual criptografada, a qual não é produzida por governos ou bancos, mas é criada por um processo computacional complexo chamado de "mineração" [3].

A proposta de Nakamoto seria criar uma tecnologia que permitisse a realização de transações de ativos pela internet sem a necessidade de intermediários para estabelecer confiança e a plataforma *blockchain* possibilitou este intento. A *bitcoin* foi a primeira aplicação desta tecnologia, mas ela está ganhando relevância por conta de suas possibilidades além das criptomoedas.

De acordo com William Mougayar [4], esta tecnologia possui três acepções que se complementam: uma jurídica, uma técnica e uma corporativa. Tecnicamente, a *blockchain* é um banco de dados, que armazena um registro distribuído e auditável. Já em sua acepção corporativa, ela permitiria a validação de transações, valores e ativos entre pessoas, sem a necessidade de intermediários. Por fim, juridicamente, ela valida transações substituindo entidades tradicionais de confiança, por isso também é denominado de protocolo de confiança entre pessoas.

Em síntese, *blockchain* é uma espécie de banco de dados distribuído, em que informações atualizadas são trazidas por cada um dos computadores que a ele se encontra conectado e que prioriza a imutabilidade dos registros, criando um protocolo de confiança para transferência de dados, ativos e documentos entre pessoas.

2.1 FUNCIONAMENTO

Quando uma transação é realizada na *blockchain*, ela é datada e armazenada num bloco. Os blocos, consistem em um conjunto de transações que aparecem sob a forma de um código alfanumérico e são interligados em sequência, por isso, esta tecnologia é chamada de *blockchain* ou cadeia de blocos. Na *blockchain* são utilizadas duas chaves, uma pública e outra privada. A transação só é considerada válida quando o indivíduo assina com sua chave privada.

Exemplificando como funciona o mecanismo de "chaves" na *blockchain* da rede *bitcoin*: se Tício quer enviar bitcoins para Mévio, ele copia a chave pública de Mévio, chamada de "endereço *bitcoin*", coloca o valor que ele quer transferir e utiliza sua chave privada para confirmar a autenticidade da transação. A chave pública cifra a transação produzindo um código de modo que apenas Mévio consiga decifrar aquela mensagem utilizando sua chave privada. Por isso, é como se fossem utilizados dois cadeados diferentes, um para cifrar a mensagem e outro diferente para decodificá-la[5].

Para garantir a ordenação e dificultar a adulteração dos dados, cada bloco possui informações de identidade digital do bloco anterior e quando estas duas informações se conectam formam uma impressão digital própria.[6] Esta impressão digital é formada por um

---

[3] LAURENCE, Tiana. *Blockchain para leigos*. 1ª Ed. Rio de Janeiro: Alta Books, 2019, p. XIX.

[4] MOUGAYAR, William. *Blockchain para negócios: promessa, prática e aplicação da nova tecnologia da internet.* Rio de Janeiro: Alta Books, 2017, p. 04.

[5] ULRICH, Fernando. *Bitcoin: a moeda na era digital*. São Paulo: Instituto Ludwig von Mises Brasil, 2014, p.12.

[6] ROCHA, Lucas Salles Moreira; GOMES, Frederico Felix; MAFRA, Tereza Cristina Monteiro. Validade e Eficácia dos "Testamentos Inteligentes" via Tecnologia Blockchain. *Scientia Iuris*, Londrina, v.23, n.1, p.63-80, 2019, p. 66.

hash, isto é, um tipo de cálculo matemático que transforma informações em um código de identificação com letras e números, representando os dados inseridos [7].

Antes do bloco ser adicionado à cadeia, ele fica com o status de pendente e ocorrem alguns processos: os chamados "mineradores" produzem a prova de trabalho, que consiste na utilização de um *software* específico de seus computadores com a finalidade de calcular o *hash* correto para formar a ligação entre os blocos, o qual mantém a unidade da rede e garante que todos os membros possuam cópias idênticas da *blockchain* [8].

Os "mineradores" são usuários que competem entre si e o primeiro a resolver o problema, valida o bloco, além de ser recompensado em moeda digital. A solução é compartilhada com todos os computadores da rede, que realizam a sua verificação e se estiver correta, o bloco é adicionado a cadeia [9]. Se existirem duas cadeias de blocos distintas na rede, com dados conflitantes, é selecionada a maior cadeia, pois ela possui maior poder computacional presente[10].

Se houver um empate na criação de blocos diferentes, mas válidos, a rede grava os dois blocos em partes diferentes e aguarda-se para verificar em qual das duas cadeias serão adicionados novos blocos. A parte que tiver mais blocos gravados é escolhida e compartilhada por toda a rede. Atualmente, segundo Wright e Filippi este processo de validação dos blocos na *blockchain* da *bitcoin*, que é a cadeia de blocos mais extensa na atualidade, demora por volta de dez minutos [11].

2.2 CARACTERÍSTICAS

A tecnologia *blockchain* foi elaborada tendo como suporte quatro atributos principais, quais sejam: "segurança das operações, descentralização de armazenamento/computação, integridade de dados e a imutabilidade de transações"[12].

Para compreender a segurança da *blockchain*, pode-se imaginar que alguns amigos emprestam dinheiro uns para os outros, possuindo uma espécie de banco de dados digital para anotar quanto cada um está devendo e realizar pagamentos. O primeiro problema que poderia ser gerado é que qualquer pessoa poderia se passar por um desses amigos. A *blockchain* resolve este problema por meio da criptografia assimétrica de chave pública e privada. Assim, a cada indivíduo que participa da rede são destinadas duas chaves: uma privada, que deve ser guardada em sigilo, como uma senha e outra pública, distribuída para todos os usuários[13].

---

[7] PRADO, Jean. O que é blockchain? [indo além do bitcoin]. *Tecnoblog*. 2017. Disponível em: https://tecnoblog.net/227293/como-funciona-blockchain-bitcoin. Acesso em: 08 dez. 2020.

[8] ROCHA, Lucas Salles Moreira; GOMES, Frederico Felix; MAFRA, Tereza Cristina Monteiro. *Op. Cit*. P. 67.

[9] *Ibid*. P. 67.

[10] NAKAMOTO, Satoshi. *Bitcoin: A peer-to-peer Electronic Cash System*. 2008. Disponível em: https://Bitcoin.org/Bitcoin.pdf. Acesso em: 09 dez. 2020.

[11] WRIGHT, Aaron; FILIPPI, Primavera de. Decentralized blockchain technology and the rise of lex cryptographia. In: ELSEVIER. SSRN. Rochester, 20 Mar. 2015. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664. Acesso em: 08 dez. 2020.

[12] FORMIGONI FILHO, José Reynaldo; BRAGA, Alexandre Mello; LEAL, Rodrigo Lima Verde. *Tecnologia Blockchain: uma visão geral*. 2017. Disponível em: https://www.cpqd.com.br/wp-content/uploads/2017/03/cpqd-whitepaper-blockchain-impresso.pdf. Acesso em: 10 dez. 2020, p.6-7.

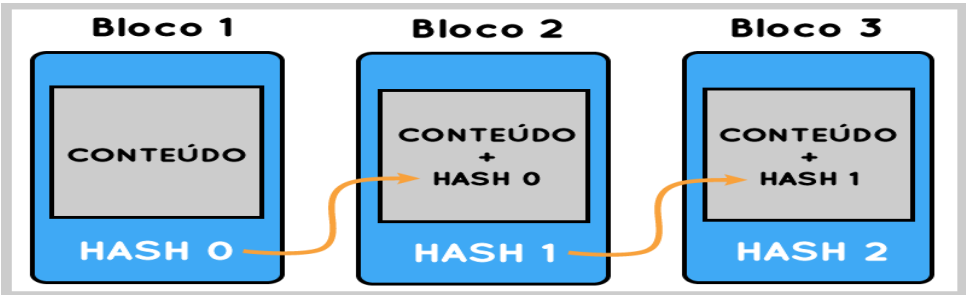
[13] ULRICH, Fernando. *Op. Cit*. p.12.

A chave pública do destinatário é utilizada para codificar determinada mensagem ou documento, a chave privada do remetente é usada para assinar àquela mensagem, a chave privada do destinatário é utilizada para decifrar aquilo que o remetente enviou e a chave pública do remetente, para verificar a validade da assinatura[14]. Para garantir uma troca de mensagens privada e segura entre os usuários, os programadores utilizam uma função matemática para criar uma relação entre as chaves, pois enquanto a chave pública codifica a mensagem, a privada decifra. Para dificultar que outros usuários descubram as chaves privadas, os programadores usam funções matemáticas unidirecionais[15], logo, se alguém possui o número da chave privada é possível descobrir facilmente o da chave pública, mas é extremamente custoso identificar a chave privada com o número da chave pública. Assim, a chave pública pode ser publicada na internet sem comprometer a segurança.

Retornando ao exemplo anterior, outro problema que poderia ocorrer é o do gasto-duplo, em que um desses amigos poderia emprestar ao outro cem reais apenas uma vez, utilizar a chave pública e a privada, formando um código válido, mas de forma fraudulenta copiar várias vezes no banco de dados digital que o outro lhe deve essa quantia. Para evitar que isso aconteça, a mensagem também possui uma identidade digital única associada àquela transação a qual é registrada, carimbada com data e hora e armazenada em um bloco do *blockchain*.

Todos os computadores conectados à rede possuem registros de todas as transações sempre atualizados e verificados. Dessa forma, se o amigo emprestar para o outro cem reais várias vezes, cada um desses empréstimos terá um código próprio. Esse código é chamado de *hash*, uma função matemática que utiliza informações das transações presentes naquele bloco e no bloco precedente, gerando uma espécie de código com letras e caracteres que identifica cada bloco.

Figura 1 – Estrutura básica da cadeia de blocos



Fonte: Artigo sobre Bitcoin do blog dinheironinja[16]

Para um hacker adulterar o sistema não basta alterar apenas uma cópia, devendo alterar mais da metade de toda a rede e antes que seja adicionado um novo bloco na cadeia. O *hash* dificulta eventuais ataques com objetivo de corromper o sistema, pois demandaria que os atacantes detivessem a maior parte do poder computacional de toda rede [17].

---

[14] AMARO, George. *Criptografia simétrica e assimétrica de chaves públicas: vantagens e desvantagens*. Disponível em: publica.fesppr.br/index.php/rnti/issue/download/4/33. Acesso em: 06 dez. 2020, p 06.

[15] Isso é possível graças ao uso de algumas funções matemáticas que possuem propriedadedes irreversíveis. As mais usadas são a fatoração em números primos (IFP-IntegerFactorizationProblem), curvas elípticas (ECDLP-Elliptic Curve Discrete Logarithm Problem) ou logaritmos discretos (DLP - Discrete Logarithm Problem).

[16] BLOG DINHEIRO NINJA. *Sem título*. 2019. 1 gravura. Disponível em: https://www.dinheironinja.com/bitcoin. Acesso em 10 dez. 2020.

[17] ROCHA, Lucas Salles Moreira; GOMES, Frederico Felix; MAFRA, Tereza Cristina Monteiro. *Op. Cit*. P.67.

É tão custoso adulterar a *blockchain*, que por exemplo, todo o poder computacional da Google atualmente representa menos de 1% do poder compartilhado pela maior rede de *blockchain* vigente, que é a do Bitcoin [18]. Além disso, a recompensa desse tipo de ataque também é extremamente limitada, pois o hacker só poderia reverter sua própria transação. Portanto, quando uma informação é escrita dentro da cadeia de blocos torna-se quase impossível removê-la. Essa característica da tecnologia *blockchain* é inovadora, permitindo negociações virtuais de forma permanente e confiável.

A *blockchain* é descentralizada, pois cada computador da rede possui uma cópia de todos os dados, tendo, portanto, igual importância e acesso às informações, prescindindo de órgãos intermediários que aprovem ou determinem a transação. Entretanto, também existem cadeias de blocos centralizadas, por exemplo, as privadas em que uma corporação pode utilizar esta tecnologia para armazenar seus dados dentro do sistema.

Esta tecnologia garante a integridade de dados, pois quando ocorre alguma tentativa de adulteração em algum dos blocos dessa cadeia, o código *hash* é modificado e, por conseguinte, desaparece a correspondência com os demais blocos [19]. Os computadores dos usuários, também chamados tecnicamente de "nós", realizam periodicamente a sincronização entre as informações presentes na *blockchain* por meio da mineração, e o bloco alterado não é validado pela rede. Na ilustração a seguir é possível verificar como uma pequena modificação em uma informação transforma completamente o código *hash*.

Figura 2 - Exemplo de como uma pequena variação em "*Hello, World!*" é capaz de gerar um valor de *hash* completamente diferente

```
"Hello, world!0" => 1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64
"Hello, world!1" => e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8
"Hello, world!2" => ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7
...
"Hello, world!4248" => 6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfdf65cc0b965
"Hello, world!4249" => c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6
"Hello, world!4250" => 0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9
```

Fonte: Lucca Freire, 2018.[20]

As transações na *blockchain* são imutáveis, pois trata-se de um sistema em que o indivíduo pode adicionar novas informações, mas não consegue modificar informações anteriores. Se os sujeitos envolvidos quisessem modificar a transação, deveriam realizar um novo contrato para tal, o que requer a colaboração de todos, porque depende da utilização de suas chaves privadas. Porém, apesar de a transação anterior não ter mais efeito, ela continuará registrada na *blockchain* [21].

---

[18] SMART, Evander. Bitcoin is 100 times More Powerful than Google. *Cryptocoinsnews*. ac. 2015. Disponível em https://www.cryptocoinsnews.com/bitcoin-100-times-powerful-google. Acesso em Salvador, 16 dez. de 2020.

[19] ROCHA, Lucas Salles Moreira; GOMES, Frederico Felix; MAFRA, Tereza Cristina Monteiro. *Op. Cit*. P. 69.

[20] FREIRE, Lucas. Sem título. 2018. 1 gravura. Disponível em: https://medium.com/@luccafreire/os-sete-princípios-do-blockchain-1-integridade-na-rede-dc0e5294d95f. Acesso em 10 dez. 2020.

[21] ABOBOREIRA, Edgar Carmo. *A Imutabilidade Dos Smart Contracts é Um Entrave à Dinâmica Dos Negócios?* 2018. Trabalho de Conclusão de Curso (Graduação em Direito) - Universidade Presbiteriana Mackenzie. São Paulo, 2018, p. 19.

Contudo, esta característica não é absoluta, pois existem possibilidades de modificação, quais sejam: *blockchains* permissionadas podem agregar mecanismos que corrijam erros e que regulem os direitos de acesso, tornando conteúdos invisíveis para terceiros, embora não sejam apagados [22]. Ademais, como já foi mencionado anteriormente, apesar de extremamente custosa e difícil, existe a possibilidade de modificação dos dados por meio de um ataque efetuado por um hacker com mais da metade do poder computacional [23]. Devido a esse baixo risco de adulteração, a *blockchain* adiciona confiança num ambiente de desconfianças e suas características inovadoras estão possibilitando a transformação da rede mundial de computadores, pois está transformando a internet do compartilhamento de informações na internet do compartilhamento de valores [24].

2.3 TIPOS

Existem diversos tipos de *blockchains*: públicos, privados ou híbridos. *Blockchains* públicos, como a *Bitcoin*, são extensas redes disseminadas e abertas a atuação de qualquer um, bem como, tem uma codificação aberta e mantida pela coletividade [25]. Suas vantagens são: a eliminação de intermediários, a descentralização e a transparência.

Por sua vez, uma desvantagem desse tipo de *blockchain* é a lentidão, pois demora mais tempo para toda a rede chegar a um consenso sobre o estado das transações. Outra desvantagem é que o consumo de energia é muito alto, pois conforme estudo realizado por pesquisadores da Universidade de Cambridge, na Inglaterra, o consumo de energia promovido pela *blockchain* da *Bitcoin* é equivalente ao gasto anual de toda Suíça [26].

Existem *Blockchains* privados, como a plataforma Corda[27], em que a participação na rede depende de aprovação e existe um controle sobre quem pode enxergar os dados de uma transação. Esses tipos de *blockchains* são protegidos por pessoa ou grupo de pessoas que têm membros conceituados e informações comerciais confidenciais[28]. Além disso, essas redes são centralizadas, pois abrangem obrigatoriamente uma entidade permissionária, geralmente a organização que a criou. Ela é responsável por estabelecer quem pode ingressar no sistema.

A forma de controle de quem pode participar do sistema é variável: os usuários existentes podem escolher quem serão os futuros; um órgão ou autoridade regulatória pode

---

[22] BACON, Jean; MICHELS, Johan David; MILLARD, Christopher; SINGH, Jatinder. *Blockchain Demystified:* A Technical and Legal Introduction to Distributed and Centralised Ledgers, 25 Rich. J.L. & Tech., no. 1, 2018.

[23] MAGAS, Julia. Imutabilidade na dúvida: precisamos proteger dados de blockchain? *Cointelegraph.* 2018. Disponível em: https://br.cointelegraph.com/news/immutability-in-doubt-do-we-need-to-protect-blockchain-data. Acesso em: 17 dez. 2019.

[24] GNIPPER, Patrícia. Indústrias precisarão repensar seus negócios graças ao blockchain. *Canaltech*. 2018. Disponível em: https://canaltech.com.br/blockchain/industrias-precisarao-repensar-seus-negocios-gracas-ao-blockchain-116656/. Acesso em: 17 dez. 2020.

[25] LAURENCE, Tiana. *Blockchain para leigos*. 1ª Ed. Rio de Janeiro: Alta Books, 2019, p. 08.

[26] BARANIUK, Chris. Bitcoin's energy consumption 'equals that of Switzerland'**.** *BBC News*. 2019. Disponível em: https://www.bbc.com/news/technology-48853230. Acesso em: 20 dez. 2019.

[27] A Corda é uma plataforma blockchain privada criada para que empresas possam gerenciar contratos legalizados e transferir qualquer tipo de valor sem enfrentar qualquer perda de privacidade.

[28] LAURENCE, Tiana. *Op. Cit*. P. 08.

emitir licenças de participação; e um consórcio ou empresa poderia decidir [29]. Usualmente, este ente permissionário também realiza a validação das informações armazenadas na cadeia de blocos, dispensando ou complementando o trabalho dos "mineradores". Dentre as vantagens das *blockchains* privadas em comparação com as públicas, podem-se destacar: maior velocidade, bem como, maior capacidade de suportar e processar um número maior de transações. Já as suas desvantagens são: a centralização e a necessidade de se confiar em quem realiza o processo de verificação.

Blockchains híbridas, como o *Hyperledger*[30], são uma combinação da *blockchain* privada e da pública, não estão abertas a todos para examinar, mas, ainda assim, oferecem recursos como integridade de dados, transparência e segurança. Elas são personalizáveis e os membros têm autoridade para decidir quem pode participar ou quais informações devem ser tornadas públicas [31].

Nas *blockchains* híbridas as informações são validadas num ambiente privado, mas o indivíduo pode verificar o que está sendo feito com a informação e como ela está sendo tratada. Portanto, as *blockchains* híbridas podem ser programadas com as características benéficas das públicas e das privadas, minimizando as suas características desvantajosas.

2.4 CONTRATOS INTELIGENTES

O termo contrato inteligente foi utilizado pela primeira vez pelo jurista e criptógrafo Nick Szabo em seu artigo intitulado "Contratos Inteligentes: Construindo Blocos para Mercados Digitais Livres*"*, que foi publicado em setembro de 1996 [32]. Ele apontou a máquina de venda automática [33] como um exemplo primitivo de contrato inteligente e salientou que eles aprimorariam a efetivação dos quatro objetivos básicos dos contratos, que ele determinou como sendo a observabilidade, a verificabilidade, a privacidade e a obrigatoriedade.

A observabilidade, na visão de Szabo, possibilitaria que as partes observassem a performance de cada uma no contrato ou provassem sua performance, já a verificabilidade permite que terceiros, como um árbitro escolhido pelas partes, investigassem a execução do contrato [34].

Quanto a privacidade, os contratos inteligentes seguem o princípio de que as partes só devem ter o conhecimento e o controle sobre o conteúdo na medida do necessário para a execução desse contrato e de que terceiros, exceto os árbitros e intermediários designados, não

---

[29] GUSSON, Cassio. Quais as diferenças entre blockchain pública e privada? *Criptofacil*. 2018. Disponível em: https://www.criptofacil.com/quais-as-diferencas-entre-blockchain-publica-e-privada. Acesso em: 20 dez. 2020.

[30] A plataforma Hyperledger foi formada por diversas indústrias para criar um livro-razão distribuído de código aberto. Ela incorpora tecnologias, incluindo frameworks, smart contract, interfaces gráficas e amostras de aplicações.

[31]GOMES, Ezequiel. O que é uma blockchain híbrida? *Infochain*. 2019. Disponível em: https://infochain.com.br/o-que-e-uma-blockchain-hibrida. Acesso em: 20 dez. 2020.

[32] SZABO, Nick. *Smart Contracts*: *Building Blocks for Digital Markets*. ac. 1996. Disponível em http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html. Acesso em: 19 dez. 2020, p. 01.

[33] Máquinas de venda automáticas são aquelas que vendem refrigerantes ou lanches de maneira instantânea, depois que o consumidor insere o dinheiro no dispositivo.

[34] *Ibid*. P. 01.

devem ter voz na execução de um contrato [35]. Szabo também vislumbrava que os contratos inteligentes seriam autoexecutáveis. Contudo, na época não havia desenvolvimento tecnológico suficiente para colocá-los em prática. Com o surgimento da tecnologia *blockchain* neste século, os contratos inteligentes se tornaram uma realidade [36].

O *Ethereum* foi a primeira plataforma a possibilitar as aplicações supracitadas, desenvolvendo uma tecnologia *blockchain* capaz de executar qualquer lógica escrita em código de programação, permitindo a definição de regras e consequências para certos eventos, fixando obrigações, benefícios, sanções e procedendo a sua devida execução. Os contratos inteligentes baseados na *blockchain*, "*smart contracts*", são formados através de códigos de criptografia e baseados numa lógica de "se, então". Se o código para o contrato inteligente precisa de uma fonte externa para definir se ele atendeu às condições, ele usará um "oráculo", isto é, uma fonte de alimentação de dados [37].

Os oráculos permitem que o contrato inteligente interaja com dados fora do ambiente *blockchain*. Por exemplo, seria necessário ter um "oráculo" sobre o clima, se o contrato inteligente estivesse executando um contrato de seguro para plantações. Assim, o contrato liberaria imediatamente R$ 3.000,00 (três mil reais) para o segurado se a temperatura caísse abaixo de zero graus Celsius por mais de uma hora [38]. Dessa forma, os contratos inteligentes são personalizáveis e podem se adaptar às diversas espécies contratuais, como contratos de compra e venda, de seguro, de mútuo, de locação, entre outros.

3 CONTRATOS DE SEGURO DE DANO NO BRASIL

O sociólogo alemão Ulrich Beck entende que a modernidade está marcada pela "sociedade de risco", pois os indivíduos vivem num mundo de incertezas em que as inovações tecnológicas e as rápidas respostas sociais geraram um panorama de risco global [39]. Assim, os contratos de seguro ganharam um protagonismo maior, pois eles visam acautelar os segurados dos possíveis prejuízos econômicos decorrentes de certos sinistros que podem ocorrer.

Diante do incremento de situações de risco, este contrato alcançou tamanha relevância que o termo seguro pode abarcar diversos significados, abrangendo os seguros públicos, isto é, aqueles voltados para tutelar os trabalhadores, os seguros privados, que podem ser livremente estipulados entre as partes, bem como, os seguros obrigatórios, por exemplo, o seguro legal obrigatório de automóveis (DPVAT). Contudo, este artigo não visa esgotar a temática, logo seu objetivo é analisar os contratos de seguros de dano livremente pactuados entre as partes.

O art. 757 do Código Civil disciplina o conceito de contrato de seguro, segundo o qual: "Pelo contrato de seguro, o segurador se obriga, mediante o pagamento do prêmio, a garantir interesse legítimo do segurado, relativo à pessoa ou a coisa, contra riscos predeterminados".

Pedro Alvim realiza a distinção entre o contrato de seguro e o de jogo ou aposta, disciplinando que neste o risco é sempre criado artificialmente, logo se o indivíduo não tivesse

---

[35]SZABO, Nick. *Smart Contracts*: *Building Blocks for Digital Markets*. ac. 1996. Disponível em http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html. Acesso em: 19 dez. 2020, p. 01.

[36] CARDOSO, Bruno. *Contratos inteligentes: descubra o que são e como funcionam*. Brasil, 19 dez. 2020. Disponível em: https://brunonc.jusbrasil.com.br/artigos/569694569/contratos-inteligentes-descubra-o-que-sao-e-como-funcionam. Acesso em: 19 dez. 2020, p. 11.

[37] LAURENCE, Tiana. Op. Cit. P. 02.

[38] *Ibid*. P. 02.

[39] BECK, Ulrich. *Sociedade de risco rumo a uma outra modernidade*. São Paulo: Ed. 34, 2010, p.368.

jogado, este risco (de perder o jogo) não seria gerado. Portanto, no jogo, o risco é consequência do próprio contrato. Por sua vez, no contrato de seguro, o risco é a causa do contrato e antecede a sua formação. Assim, o seguro repara o dano e o jogo visa, tão somente, o lucro [40].

Arnaldo Rizzardo define o contrato de seguro como o contrato de garantia contra riscos previstos, discordando do conceito tradicional que o prevê como um contrato em que o segurado transfere o risco para o segurador, pois aquele continua com a possibilidade de sofrer o sinistro e a seguradora apenas irá ressarcir os prejuízos decorrentes do acidente [41].

Quanto ao segurador, segundo o art. 1º do Decreto-Lei nº 2.063 de 1940, as seguradoras privadas só podem ser sociedades anônimas, mútuas e cooperativas, sendo que estas últimas possuem atuação restrita a seguros agrícolas, de acidentes do trabalho e de saúde. Exige-se também que todas sejam previamente autorizadas, segundo prescreve o art. 78 do Decreto-Lei nº 73/1966 [42].

O risco é o acontecimento futuro e incerto previsto no contrato e passível de provocar o dano, causando prejuízo de ordem econômica. Quando o risco acontece, é denominado tecnicamente de sinistro. Segundo Orlando Gomes, o risco é um elemento essencial do contrato de seguro, uma vez que sem ele não existe contrato de seguro [43]. Em regra, todo contrato deve ter objeto lícito.

O art. 762 do CC. considera nulos os contratos de seguro relativos a atos ilícitos dolosos do segurado, do beneficiário ou de representante de um ou de outro, logo suas cláusulas não podem contrariar normas de ordem pública. É importante salientar que não haverá nulidade do contrato por atos culposos. No ramo de seguros, existem ilícitos específicos, previstos nos arts. 778, 781, 782 e 789 do Código Civil, como o seguro por valor maior do que a coisa segurada, ou a pluralidade de seguros sobre o mesmo bem, denominado de seguro cumulativo, com exceção do seguro de vida [44].

A doutrina diverge a respeito do objeto do contrato de seguro, há quem diga que seu objeto seria proteger a coisa, o risco ou um interesse segurável. Segundo Venosa, é melhor concluir que o objeto deste contrato é proteger um interesse segurável, que consiste numa "relação econômica ameaçada ou posta em risco". De fato, pode existir mais de um interesse sobre o mesmo bem, sobre um celular, por exemplo, pode ser contratado um seguro contra deterioração e outro sobre furto ou roubo.

É o interesse segurável legítimo que diferencia o seguro em nome de outrem do jogo ou aposta. O CC. 2002 em seu art. 757 aderiu acertadamente à teoria do interesse legítimo [45]. O contrato de seguro é bilateral, ou seja, revela direitos e deveres recíprocos. Trata-se de um contrato oneroso, pois o segurado remunera o segurador por meio do prêmio e a seguradora tem a obrigação de pagar a indenização prevista em caso de ocorrência do sinistro.

O ramo securitário é regulado por diversas instituições estatais que emitem normas, fiscalizam e autorizam essa atividade. O Sistema Nacional de Seguros Privados é composto do

---

[40] ALVIM, Pedro. *O Contrato de seguro*.1. ed. Rio de Janeiro: Forense, 1983, p. 106-110.
[41] RIZZARDO, Arnaldo. Contratos. 15. ed. Rio de Janeiro: Forense, 2015, p. 977.
[42] Decreto-Lei Nº 73, de 1966. "Art 78. As Sociedades Seguradoras só poderão operar em seguros para os quais tenham a necessária autorização, segundo os planos, tarifas e normas aprovadas pelo CNSP".
[43] GOMES, Orlando. *Contratos*. 26. ed. Rio de Janeiro: Forense, 2009, p. 505.
[44] GONÇALVES, Carlos Roberto. *Direito civil brasileiro: contratos e atos unilaterais*. 11. ed. São Paulo: Saraiva, 2014, p. 352.
[45] VENOSA, Sílvio de Salvo. *Direito Civil: Contratos em espécie*. 13. Ed. São Paulo: Atlas, 2013, p. 403.

Conselho Nacional de Seguros Privados – CNSP, da Superintendência dos Seguros Privados – SUSEP e do Instituto de Resseguros do Brasil – IRB Brasil RE [46].

O CNSP é o órgão de deliberação coletiva que estabelece as diretrizes e normas da política de seguros e resseguros privados, regulando e fiscalizando a orientação básica e o funcionamento dos componentes do sistema. A SUSEP é entidade autárquica que executa a política traçada pelo CNSP. Fiscaliza e autoriza o funcionamento e as operações das Sociedades Seguradoras, das entidades abertas de previdência complementar, das sociedades de capitalização e das corretoras, regulamentando as operações de seguros, prescrevendo as condições da apólice, dos planos de operação e dos valores das tarifas [47].

O Instituto de Resseguros do Brasil é sociedade de economia mista criada pelo Decreto-Lei n. 1.186/39, que regulava o cosseguro e o resseguro, assim como promovia o desenvolvimento das operações de seguro segundo as diretrizes do CNSP até 31/12/2007. Com a promulgação da Lei Complementar nº 126/2007, o mercado foi aberto a competidores estrangeiros e o IRB perdeu o monopólio do mercado de resseguros no Brasil, mas continua atuando como um ressegurador local e a SUSEP passou a exercer a fiscalização e regulação do mercado de resseguros, cosseguros e retrocessões [48].

Segundo Rúben Stiglitz, a intervenção do estado na atividade securitária visa assegurar a higidez econômica da empresa seguradora, que arrecada o capital oriundo dos prêmios pagos pelos segurados, que funcionam como uma "poupança de terceiros", devendo realizar um controle da legitimidade, equidade, legalidade e clareza das cláusulas contratuais[49].

O Código Civil de 2002 optou por dividir os contratos de seguro em duas modalidades principais, quais sejam: o seguro de dano e o seguro de pessoa. Enquanto aquele possui caráter indenizatório, este tem o objetivo de acautelar bens extrapatrimoniais insusceptíveis de valoração, como a vida e a integridade física. No seguro de dano é vedado o sobresseguro [50], ou seja, a contratação de um seguro com valor da cobertura superior ao da coisa no momento do sinistro, além de ser proibido o seguro cumulativo [51], isto é, a contratação de mais de um seguro sobre o mesmo interesse, quando esse fica garantido por valor superior ao que tem, para se evitar o desvirtuamento do contrato de seguro, que visa reembolsar o dano e não enriquecer o segurado [52].

Segundo Paulo Nader, os objetos garantidos no seguro de dano são bens materiais ou qualquer outro interesse susceptível de avaliação econômica, como uma casa, um carro ou uma futura obrigação pecuniária advinda do reconhecimento de responsabilidade civil por parte do segurado [53]. Para Orlando Gomes, os seguros de danos mais corriqueiros são para a cobertura

---

[46] FORTUNA, Eduardo. *Mercado Financeiro: produtos e serviços*. 18. ed. rev. e atual. Rio de Janeiro: Qualymark, 2010, p. 542-543.
[47] *Ibid*. P. 543.
[48] *Ibid*. P. 543.
[49] STIGLITZ, Rubén S. Controle do Estado sobre a Atividade Seguradora. In: FÓRUM DE DIREITO DO SEGURO. 2., 2002, São Paulo. *Anais* [...]. São Paulo: IBDS/EMTS, 2002. p. 44.
[50] Art. 778 do Código Civil de 2002. "Nos contratos de seguro de dano, a garantia prometida não pode ultrapassar o valor do interesse segurado no momento da conclusão do contrato".
[51] Art. 782 do Código Civil de 2002. "O segurado que, na vigência do contrato pretender obter novo seguro sobre o mesmo interesse, e contra o mesmo risco junto a outro segurador, deve previamente comunicar sua intenção por escrito ao primeiro, indicando a soma por que pretende segurar-se, a fim de comprovar a obediência ao disposto no art. 778".
[52] NADER, Paulo. Curso de Direito Civil: contratos. 9. Ed. Rio de Janeiro: Forense, 2018, p.476.
[53] *Ibid*. P.476.

de riscos de fogo e transporte. Entretanto também podem garantir a indenização de quaisquer danos sobrevindos às coisas em razão dos riscos a que são expostas. Até o risco da insolvabilidade dos devedores pode ser transferido a um segurador, mediante seguro de crédito [54].

Segundo prescreve o art. 779 do CC. o seguro de dano deve ter uma cobertura completa do risco assegurado, compreendendo todos os prejuízos resultantes ou consequentes, como sejam os estragos ocasionados para minorar evitar o sinistro, minorar o dano ou salvar a coisa, apenas não podendo ultrapassar o limite da cobertura previsto na apólice ou no bilhete.

Os seguros de responsabilidade civil são aqueles em que o segurado visa obter cobertura em face de eventuais danos que culposamente venha a causar a terceiros. Por imposição do princípio da boa-fé, o §1º do art.787 do CC. determina que "tão logo saiba o segurado das consequências de ato seu, susceptível de lhe acarretar a responsabilidade incluída na garantia, comunicará o fato ao segurador". O prazo desta comunicação geralmente está disposto no contrato e se o segurado demorar para realizar esta comunicação à seguradora, arcará com os danos que forem consequências da mora[55].

O ramo de seguros possui uma estrutura de funcionamento que envolve segurados, sociedades seguradoras, corretores de seguro, resseguradoras e a Superintendência de Seguros Privados (SUSEP). O corretor é a pessoa física ou jurídica habilitada e registrada na SUSEP para intermediar e promover a comercialização de contratos de seguro. Cada plano comercializado pelas seguradoras deve ser submetido a análise e arquivamento pela SUSEP.

4. O USO DA TECNOLOGIA *BLOCKCHAIN* EM CONTRATOS DE SEGURO DE DANO

Diversas empresas já estão aplicando a tecnologia *blockchain* ao setor de seguro de dano. A Seguros SURA, grupo de seguros da América Latina, adotou esta tecnologia para gravação e envio de apólices, endossos e boletos na forma de um contrato inteligente. O grupo utiliza a *blockchain* desde 2017 e salientou que esta tecnologia reduziu 20% na inadimplência em todas as suas linhas de produtos, além de reduzir 32% dos gastos com a reemissão de documentos de cobrança, apólices, boletos e endosso [56]. Para dar validade jurídica à utilização da tecnologia *blockchain* por seguradoras brasileiras, a empresa *Direct.One* desenvolveu um sistema baseado tanto na Medida Provisória Nº 2.200-2, de 24 de agosto de 2001, que instituiu a Infraestrutura de Chaves Públicas Brasileira ou ICP-Brasil, bem como, na Resolução CNSP 294, difundida pela SUSEP, que prescreve regras para a venda de seguros por Meios Remotos.

Esta plataforma utilizou três itens probatórios para gerar consenso nos documentos emitidos pela empresa: assinatura digital com chave pública e privada ICP-Brasil; Carimbo do Tempo com data e hora fornecida pelo Observatório Nacional; e o registro de dados não sigilosos dos contratos para gerar consenso e sistema antifraude na plataforma *Ethereum* [57]. Portanto, esta empresa conseguiu se adequar às regras estabelecidas pelo regulador, demonstrando como é possível adaptar novas tecnologias à legislação existente.

---

[54] GOMES, Orlando. *Contratos*. 26. Ed. Rio de Janeiro: Forense, 2009, p. 510.
[55] RIZZARDO, Arnaldo. *Contratos*. 18. ed. Rio de Janeiro: Forense. 2019, p. 478.
[56] MATOS, Gino. Blockchain na área de seguros pode reduzir inadimplência no Brasil. *Webcoin*. 2019. Disponível em: https://webitcoin.com.br/blockchain-na-area-de-seguros-pode-reduzir-inadimplencia-no-brasil-mar-31. Acesso em: 22 dez. 2020.
[57] CONEXÃOFINTECH. *Geração de apólices validadas juridicamente via Blockchain já é realidade no Brasil*. 2017. Disponível em: https://www.conexaofintech.com.br/insurtech/geracao-de-apolices-via-blockchain. Acesso em: 22 dez. 2020.

Recentemente, o IRB Brasil RE anunciou uma parceria com a B3 para desenvolver uma plataforma que conectará corretores, seguradoras e resseguradoras em uma única rede. A plataforma será baseada na tecnologia *blockchain* e visa permitir que operações envolvendo contratos de seguros e resseguros sejam realizadas via internet[58].

Outro exemplo é o uso da tecnologia para registro e seguro de bicicletas na Holanda. As seguradoras, então, disponibilizam cadeados ligados a *blockchain* que, por meio de dispositivos, registram hora, data e local em que eles foram abertos e fechados. Se houver furto ou roubo da bicicleta, a empresa tem os dados necessários para verificar se os procedimentos de segurança estabelecidos no contrato foram cumpridos. Isso torna o pagamento do seguro mais ágil, além de diminuir o custo das operações das apólices.

O consórcio *Blockchain Insurance Industry Initiative* (B3i), formado pela colaboração de seguradoras e resseguradoras, como a Zurich, Liberty Seguros e Allianz, para explorar o potencial da *blockchain*, realizou uma pesquisa de mercado em 2017 que constatou que o uso desta tecnologia no ramo de seguros pode diminuir 30% dos custos administrativos, pois possibilita a diminuição de tarefas manuais atualmente executadas pela equipe de administração[59]. Assim, a tecnologia *blockchain* diminui custos administrativos ao automatizar procedimentos realizados para a execução de contratos de seguro.

Os contratos de seguro de dano marítimo também podem se beneficiar desta tecnologia, inclusive a Ernst & Young, a Guardtime e a Azure *Blockchain* da Microsoft estão colaborando para desenvolver uma plataforma inovadora habilitada para *blockchain* que pode atender às necessidades de todas as diferentes partes envolvidas em um contrato de seguro marítimo[60]. A plataforma digitaliza as regras entre seguradoras e segurados, automatizando todo o processo com o uso de contratos inteligentes para minimizar a emissão de papéis. Assim, as companhias de seguros podem atualizar imediatamente as informações on-line ou ver onde um navio está em qualquer lugar do mundo, a qualquer momento ou se ele mudou de rota[61].

Recentemente, a SUSEP autorizou os seguros com vigência reduzida e período intermitente, por meio da Circular nº 592, permitindo que as seguradoras ofereçam apólices de seguros por meses, dias, horas ou limitados a viagens e trechos, que são acionados pelo consumidor somente durante o uso[62]. Este modelo é adotado pela *insurtech* brasileira 88i, que, por meio da *blockchain* e de contratos inteligentes, permite a contratação de um seguro de dano para celulares, acidentes pessoais e assistência automotiva[63]. Dessa forma, o regulador pátrio

---

[58] ANDRADE, Gene. IRB Brasil e B3 firmam parceria para plataforma à base de blockchain, Estadão, 2020. Disponível em: https://einvestidor.estadao.com.br/mercado/irb-parceria-b3-plataforma-blockchain. Acesso em: 21 dez. 2020.

[59] Blockchain could cut insurers' admin costs by 30%; B3i goes comercial. *Intelligentinsurer*. 2018. Disponível em: https://www.intelligentinsurer.com/news/blockchain-could-cut-insurers-admin-costs-by-30-b3i-goes-commercial-14473. Acesso em: 22 dez. 2020.

[60] CRAWFORD, Shaun. How blockchain is reducing the fluidity of risk in marine insurance. *Ernst & Young*. 2019. Disponível em: https://www.ey.com/en_gl/blockchain/how-blockchain-is-reducing-fluidity-of-risk-in-marine-insurance. Acesso em: 23 dez. 2020, p. 01.

[61] *Ibid*. P. 01.

[62] GUSSON, Cassio. Brasil regulamenta seguro personalizado e abre caminho para soluções em blockchain. *Cointelegraph*. 2019. Disponível em: https://br.cointelegraph.com/news/brazil-regulates-custom-insurance-and-paves-the-way-for-blockchain-solutions. Acesso em: 19 dez. 2020.

[63] REDAÇÃO PANORAMACRYPTO. 88 Insurtech quer democratizar acesso a seguros com a blockchain. *Panoramacrypto*. 2019. Disponível em: https://panoramacrypto.com.br/88-insurtech-quer-democratizar-acesso-a-seguros-com-a-blockchain. Acesso em: 19 dez. 2020.

está abrindo precedentes para a utilização da *blockchain* em contratos de microsseguros de danos.

4.2. COMPATIBILIDADE DA TECNOLOGIA BLOCKCHAIN EM CONTRATOS DE SEGURO DE DANO COM A LGPD

A Lei 13.709, de 14 de agosto de 2018, conhecida como Lei Geral de Proteção de Dados (LGPD), dispõe sobre a proteção de dados pessoais, entendidos como aqueles que identifiquem pessoas naturais ou, ao menos, permitam a sua identificação. Dados que não permitam tal identificação, tais como, os dados anonimizados, não se sujeitam à proteção da LGPD.

Existe uma divergência sobre se os dados compartilhados publicamente por meio de uma *blockchain* seriam anonimizados ou pessoais. Na rede *bitcoin*, por exemplo, a chave pública é chamada de endereço da carteira bitcoin e é formada por um código com caracteres e números, de modo que alguns autores, como William Mougayar[64], afirmam ser um dado anonimizado. Contudo, segundo estudos realizados pelo European Parliamentary Research Service, as chaves públicas compartilhadas na rede devem ser consideradas como dados pessoais, pois se o usuário usar diversas vezes o mesmo endereço da carteira *bitcoin* há um risco de vinculação dele à determinado código IP, sendo possível identificá-lo[65].

Apesar de este estudo ter sido realizado no âmbito do Regulamento Geral sobre Proteção de Dados Europeu (RGPD), de igual maneira, a LGPD não se descuidou dessa possibilidade, estabelecendo que não são anonimizados os dados cuja anonimização puder ser revertida, com esforços razoáveis e por meios próprios[66]. Portanto, caso não sejam utilizadas técnicas de anonimização, as chaves públicas compartilhadas na *blockchain* devem ser consideradas como dados pessoais.

As técnicas de anonimização de dados devem ser boas o suficiente para impedir a identificação de uma pessoa singular por meio de todos e quaisquer meios razoavelmente prováveis de serem utilizados. O processo deve ser irreversível, de modo que não seja possível reconstituir os dados originais por meio da forma anonimizada. Os dados que cumprirem essas regras são considerados como pseudonimizados e não são submetidos à Lei Geral de Proteção de Dados.

Contudo, ainda não existe consenso sobre a eficácia das técnicas que possam ser utilizadas para anonimizar completamente dados pessoais em *blockchains* públicas. Apesar de as identidades por trás das chaves públicas não serem conhecidas existe um risco de reversão em que são utilizados sistemas de força bruta e riscos de vinculação, quando torna-se possível vincular dados criptografados a um titular de dados através do exame de padrões de uso ou do contexto, ou ainda pela comparação com outras informações.

Dessa forma, estão surgindo novas técnicas criptográficas com a finalidade de resolver este problema, como a variação do endereço da carteira bitcoin para dificultar a vinculação com o usuário; a utilização da função *hash* para anonimizar dados pessoais; o processamento de

---

[64] MOUGAYAR, William. Blockchain para negócios: promessa, prática e aplicação da nova tecnologia da internet, 1ª Ed. Rio de Janeiro: Alta Books, 2017, p. 55.

[65] FINCK, Michèle. Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law? 2019. Panel for the Future of Science and Technology, European Parliamentary Research Service, Scientific Foresight Unit, p. 27.

[66] SOARES, Pedro Silveira Campos. Anonimização na Lei Geral de Proteção de Dados requer posição da ANPD. CONJUR. 2019. Disponível em: https://www.conjur.com.br/2019-mar-10/pedro-soares-anonimizacao-lei-geral-protecao-dados. Acesso em: 21 dez. 2020.

dados pessoais e sensíveis em *off chain* (fora da rede *blockchain*) ou em *side chain* (em uma *blockchain* paralela e independente da rede principal)[67].

Outro problema, no caso de *blockchains* públicas, seria identificar quem é o responsável pelo tratamento dos dados. Em contrapartida, nas *blockchains* privadas e híbridas é mais fácil identificar o responsável pelo tratamento dos dados, por causa da centralização. Além disso, seus dados ficam protegidos num ecossistema privado, portanto, as *blockchains* privadas e híbridas cumprem mais facilmente os requisitos da Lei Geral de Proteção de Dados, do que as públicas.

4.3. O USO DA TECNOLOGIA BLOCKCHAIN EM CONTRATOS DE SEGURO DE DANO NO BRASIL: *SANDBOX* REGULATÓRIO

A incerteza regulatória é uma das maiores barreiras na adoção da *blockchain* no setor de seguros. A Resolução CNSP nº 294/2013, dispõe sobre a utilização de meios remotos nos mecanismos relacionados a contratos de seguro e de previdência complementar aberta, portanto a validade do uso da tecnologia *blockchain* em contratos de seguro de dano, atualmente, depende do respeito às disposições previstas no Código Civil, no Código de Defesa do Consumidor, nas Resoluções do CNSP e nas Circulares da SUSEP.

Uma das iniciativas empreendidas por muitos supervisores para permitir a adoção de novas tecnologias é a chamada "*sandbox regulatória*"[68]. *Sandbox regulatório* é uma autorização temporária outorgada pelo regulador para que projetos inovadores para os quais ainda não existe regulamentação específica possam funcionar num ambiente monitorado pelo supervisor. As empresas operam projetos após a obtenção de licenças especiais, com limitações às suas áreas de operação e sujeitas a uma atenção permanente e especial do supervisor. Por outro lado, o supervisor operaria, na *sandbox*, de forma colaborativa, viabilizando uma inovação efetiva e segura para consumidores e, até mesmo, potenciais investidores em empresas inovadoras [69].

No Brasil, a Secretaria Especial de Fazenda do Ministério da Economia, o Banco Central do Brasil, a Comissão de Valores Mobiliários e a Superintendência de Seguros Privados implantaram um modelo de *sandbox* regulatório, devido às transformações que estão acontecendo nos segmentos financeiro, de capitais e securitário. O uso de tecnologias inovadoras, como *blockchain* e inteligência artificial, tem permitido o surgimento de novos modelos de negócio, com reflexos na oferta de produtos e serviços de maior qualidade e alcance no ramo securitário, financeiro e de capitais[70].

Eduardo Fraga, diretor da SUSEP, afirma que a sociedade deve ser de capital aberto, deve cumprir as normas de proteção de dados, de prevenção à lavagem de dinheiro, bem como,

---

[67] GREGORY, Gabriel. Blockchain e a Lei de proteção de dados. Compatíveis ou não? Jusbrasil, 2018. Disponível em: https://ggregory096.jusbrasil.com.br/artigos/648118524/blockchain-e-a-lei-de-protecao-de-dados-compativeis-ou-nao. Acesso em: 21 dez. 2020.

[68] *CONJUR*. Órgãos federais buscam implementar modelo de sandbox regulatório no país. 2019. Disponível em: https://www.conjur.com.br/2019-jun-13/orgaos-federais-buscam-implementar-modelo-sandbox-regulatorio. Acesso em: 20 dez. 2020, p. 01.

[69] *Ibid.* P. 01.

[70] SUPERINTENDÊNCIA DE SEGUROS PRIVADOS. Comunicado Conjunto: Ação coordenada para implantação de regime de sandbox regulatório nos mercados financeiro, securitário e de capitais brasileiros. *SUSEP*. 2019. Disponível em: http://www.susep.gov.br/setores-susep/noticias/noticias/implantacao-de-regime-de-sandbox-regulatorio-nos-mercados-financeiro-securitario-e-de-capitais-brasileiros. Acesso em: 23 dez. 2020.

deve arcar com a taxa de fiscalização e se o número de reclamações for elevado, a autorização para funcionar poderá ser cancelada[71].

O edital SUSEP nº 02/2020 prevê que a autorização para funcionamento será de trinta e seis meses, contados a partir da efetiva data do começo da comercialização dos planos de seguro ou sessenta dias a partir da expedição, pela Susep, da autorização temporária, o que ocorrer primeiro. Além disso, a qualquer tempo ao longo do período de trinta e seis meses, a participante pode solicitar autorização permanente, seguindo a regulamentação vigente.

A Resolução CNSP nº 381, de 4 de março de 2020 e a Circular SUSEP nº 598, de 19 de março de 2020 dispõem sobre as principais regras a serem cumpridas pelos participantes do *sandbox* regulatório[72]. Em 08 de outubro de 2020, a SUSEP divulgou os onze projetos selecionados para participar da *sandbox*, dentre eles foi selecionada a empresa de seguros que utiliza a tecnologia *blockchain*, a *insurtech* 88i[73]. O projeto apresentado pela 88i oferece seguros para o impedimento para o trabalho, perda de renda, acidentes pessoais individual, celular e outros, automóveis (casco), deslocamento de volumes, bagagem e objetos em circulação.

Diante disso, tais iniciativas mitigam a desvantagem da incerteza regulatória, permitindo que os reguladores compreendam as novas tecnologias antes de disciplinar definições jurídicas, verifiquem se tais inovações vão funcionar de modo a garantir a proteção ao consumidor, além de incentivarem o desenvolvimento de projetos inovadores, chancelando o uso da tecnologia *blockchain* no setor de seguro de dano no Brasil.

5 CONCLUSÃO

Em síntese, a *blockchain* tem grande potencial de utilização nos ramos de seguros de danos agrícolas, em embarcações, em automóveis, em viagens, em aparelhos celulares, bem como, viabilizam os microsseguros com vigência reduzida e/ou intermitentes. Dentre as principais vantagens da utilização desta tecnologia em contratos de seguro é possível citar: (i) a diminuição de cerca de 30% (trinta por cento) dos custos administrativos; (ii) a segurança na transferência de dados por meio da utilização de modernas técnicas de criptografia; (iii) a automatização dos contratos de seguro com a utilização dos oráculos; (iv) a interoperabilidade entre segurados, seguradoras, resseguradoras, cosseguradoras, corretoras e regulador numa única plataforma digital.

Por sua vez, uma desvantagem na utilização desta tecnologia em contratos de seguro de dano no Brasil consiste na incerteza regulatória, pois a Superintendência de Seguros Privados é o órgão governamental responsável pelo controle, fiscalização e por conceder autorizações às sociedades seguradoras e poderia a qualquer momento impedir a utilização desta tecnologia, se houver desrespeito ao arcabouço de normas que regem os contratos de seguro de dano. Este arcabouço é formado, sobretudo, pelas normas do Código Civil, do Código de Defesa do Consumidor, do Decreto 7.962/2013, das Resoluções CNSP e das Circulares da SUSEP.

---

[71] Reguladores debatem o projeto sandbox, com vistas a ampliar a competição e fomentar a inovação, *CNSEG*, 2019. Disponível em: http://cnseg.org.br/noticias/reguladores-debatem-o-projeto-sandbox-com-vistas-a-ampliar-a-competicao-e-fomentar-a-inovacao.html. Acesso em: 23 dez. 2020.

[72] Perguntas e respostas sobre o sandbox regulatório, SUSEP, 2020. Disponível em: http://www.susep.gov.br/setores-susep/ditec/perguntas-e-respostas-sobre-o-sandbox-regulatorio. Acesso em 23 dez. 2020.

[73] LIMA, Bruno Ignácio de. Empresa de seguros com blockchain é aprovada em Sandbox da Susep, Portal do Bitcoin, 2020. Disponível em: https://portaldobitcoin.uol.com.br/empresa-de-seguros-com-blockchain-e-aprovada-em-sandbox-da-susep/. Acesso em: 20 dez. 2020.

Ademais, as *blockchains* privadas e híbridas se adequariam melhor ao contexto de proteção de dados, dinamicidade e imputação de responsabilidade, viabilizando a utilização desta tecnologia no ramo de seguros.

Para mitigar essa incerteza regulatória, a Superintendência de Seguros Privados implementou um *sandbox* regulatório, com o fim de conceder autorizações temporárias para o desenvolvimento de projetos que utilizem novas tecnologias, como a *blockchain*, em contratos de seguro de dano, flexibilizando as normas existentes para o desenvolvimento de projetos inovadores, sem olvidar da proteção dos consumidores, da proteção de dados pessoais e da prevenção à lavagem de dinheiro.

Dessa maneira, é possível concluir que a tecnologia *blockchain* já está sendo utilizada no Brasil, com validade jurídica, como meio remoto para emissão de apólices, boletos e endossos pela Seguros SURA, bem como, pela *insurtech* 88i, que foi uma das empresas selecionadas pela SUSEP no *sandbox* regulatório para explorar as potencialidades desta tecnologia no setor de seguro de dano.

REFERÊNCIAS

ABOBOREIRA, Edgar Carmo. *A Imutabilidade Dos Smart Contracts é Um Entrave à Dinâmica Dos Negócios?* 2018. Trabalho de Conclusão de Curso (Graduação em Direito) - Universidade Presbiteriana Mackenzie. São Paulo, 2018.

ALEXANDRE, Ana. Iniciativa de seguro blockchain B3i expande seu grupo de investidores. *Cointelegraph,* 2019. Disponível em: https://br.cointelegraph.com/news/blockchain-insurance-initiative-b3i-expands-its-group-of-investors. Acesso em: 20 dez. 2020.

ALVIM, Pedro. *O Contrato de seguro*. 1. ed. Rio de Janeiro: Forense, 1983.

AMARO, George. *Criptografia simétrica e assimétrica de chaves públicas: vantagens e desvantagens*. Disponível em: publica.fesppr.br/index.php/rnti/issue/download/4/33. Acesso em: 22 dez. 2020.

ANDRADE, Gene. IRB Brasil e B3 firmam parceria para plataforma à base de blockchain, Estadão, 2020. Disponível em: https://einvestidor.estadao.com.br/mercado/irb-parceria-b3-plataforma-blockchain. Acesso em: 21 dez. 2020.

BACON, Jean; MICHELS, Johan David; MILLARD, Christopher; SINGH, Jatinder. *Blockchain Demystified:* A Technical and Legal Introduction to Distributed and Centralised Ledgers, 25 Rich. J.L. & Tech., no. 1, 2018.

BARANIUK, Chris. Bitcoin's energy consumption 'equals that of Switzerland'**.** *BBC News*. 2019. Disponível em: https://www.bbc.com/news/technology-48853230. Acesso em: 22 dez. 2020.

BECK, Ulrich. *Sociedade de risco rumo a uma outra modernidade*. São Paulo: Ed. 34, 2010.

Blockchain could cut insurers' admin costs by 30%; B3i goes comercial. *Intelligentinsurer*. 2018. Disponível em: https://www.intelligentinsurer.com/news/blockchain-could-cut-insurers-admin-costs-by-30-b3i-goes-commercial-14473. Acesso em: 22 dez. 2020.

BLOG DINHEIRO NINJA. Sem título. 2019. 1 gravura. Disponível em: https://www.dinheironinja.com/bitcoin. Acesso em 19 dez. 2020.

CARDOSO, Bruno. *Contratos inteligentes:* descubra o que são e como funcionam. Brasil, 23 abr. 2018. Disponível em: https://brunonc.jusbrasil.com.br/artigos/569694569/contratos-inteligentes-descubra-o-que-sao-e-como-funcionam. Acesso em: 19 dez. 2020.

CONEXÃOFINTECH. *Geração de apólices validadas juridicamente via Blockchain já é realidade no Brasil*. 2017. Disponível em: https://www.conexaofintech.com.br/insurtech/geracao-de-apolices-via-blockchain. Acesso em: 20 dez. 2020.

CRAWFORD, Shaun. How blockchain is reducing the fluidity of risk in marine insurance. *Ernst & Young.* 2019. Disponível em: https://www.ey.com/en_gl/blockchain/how-blockchain-is-reducing-fluidity-of-risk-in-marine-insurance. Acesso em: 19 dez. 2020.

FINCK, Michèle. *Blockchain and the General Data Protection Regulation*: Can distributed ledgers be squared with European data protection law? 2019. Panel for the Future of Science and Technology, European Parliamentary Research Service, Scientific Foresight Unit.

FORMIGONI FILHO, José Reynaldo; BRAGA, Alexandre Mello; LEAL, Rodrigo Lima Verde. *Tecnologia Blockchain: uma visão geral*. 2017. Disponível em: https://www.cpqd.com.br/wp-content/uploads/2017/03/cpqd-whitepaper-blockchain-impresso.pdf. Acesso em: 18 dez. 2020.

FORTUNA, Eduardo. *Mercado Financeiro: produtos e serviços*. 18. ed. rev. e atual. Rio de Janeiro: Qualymark, 2010.

FREIRE, Lucas. Sem título. 2018. 1 gravura. Disponível em: https://medium.com/@luccafreire/os-sete-princípios-do-blockchain-1-integridade-na-rede-dc0e5294d95f. Acesso em 19 dez. 2020.

GNIPPER, Patrícia. Indústrias precisarão repensar seus negócios graças ao blockchain. *Canaltech*. 2018. Disponível em: https://canaltech.com.br/blockchain/industrias-precisarao-repensar-seus-negocios-gracas-ao-blockchain-116656/. Acesso em: 17 dez. 2020.

GOMES, Ezequiel. O que é uma blockchain híbrida? *Infochain*. 2019. Disponível em: https://infochain.com.br/o-que-e-uma-blockchain-hibrida. Acesso em: 20 dez. 2020.

_____. *Contratos*. 26. Ed. Rio de Janeiro: Forense, 2009.

GONÇALVES, Carlos Roberto. Direito Civil Brasileiro, Vol. 3: contratos e atos unilaterais. 15. Ed. São Paulo: Saraiva Educação, 2018.

GREGORY, Gabriel. Blockchain e a Lei de proteção de dados. Compatíveis ou não? Jusbrasil, 2018. Disponível em: https://ggregory096.jusbrasil.com.br/artigos/648118524/blockchain-e-a-lei-de-protecao-de-dados-compativeis-ou-nao. Acesso em: 21 dez. 2020.

GUSSON, Cassio. Brasil regulamenta seguro personalizado e abre caminho para soluções em blockchain. *Cointelegraph*. 2019. Disponível em: https://br.cointelegraph.com/news/brazil-regulates-custom-insurance-and-paves-the-way-for-blockchain-solutions. Acesso em: 19 dez. 2020.

_____. Quais as diferenças entre blockchain pública e privada? *Criptofacil*. 2018. Disponível em: https://www.criptofacil.com/quais-as-diferencas-entre-blockchain-publica-e-privada. Acesso em: 20 dez. 2020.

LAURENCE, Tiana. *Blockchain para leigos*. 1ª Ed. Rio de Janeiro: Alta Books, 2019.

LIMA, Bruno Ignácio de. Empresa de seguros com blockchain é aprovada em Sandbox da Susep, Portal do Bitcoin, 2020. Disponível em: https://portaldobitcoin.uol.com.br/empresa-de-seguros-com-blockchain-e-aprovada-em-sandbox-da-susep/. Acesso em: 20 dez. 2020.

MAGAS, Julia. Imutabilidade na dúvida: precisamos proteger dados de blockchain? *Cointelegraph.* 2018. Disponível em: https://br.cointelegraph.com/news/immutability-in-doubt-do-we-need-to-protect-blockchain-data. Acesso em: 20 dez. 2020.

MARTINO, Luís Mauro Sá. *Teoria das Mídias Digitais. Linguagens, ambientes e redes.* 2ª Edição. Rio de Janeiro: Vozes, 2015.

MATOS, Gino. Blockchain na área de seguros pode reduzir inadimplência no Brasil. *Webcoin*. 2019. Disponível em: https://webitcoin.com.br/blockchain-na-area-de-seguros-pode-reduzir-inadimplencia-no-brasil-mar-31. Acesso em: 18 dez. 2020.

MOUGAYAR, William. *Blockchain para negócios*: promessa, prática e aplicação da nova tecnologia da internet, 1ª Ed. Rio de Janeiro: Alta Books, 2017.

NADER, Paulo. Curso de Direito Civil: contratos. 9. Ed. Rio de Janeiro: Forense, 2018.

NAKAMOTO, Satoshi. *Bitcoin: A peer-to-peer Electronic Cash System*. 2008. Disponível em: https://Bitcoin.org/Bitcoin.pdf. Acesso em: 22 dez. 2020.

Órgãos federais buscam implementar modelo de sandbox regulatório no país. *CONJUR*. 2019. Disponível em: https://www.conjur.com.br/2019-jun-13/orgaos-federais-buscam-implementar-modelo-sandbox-regulatorio. Acesso em: 18 dez. 2020.

O que é blockchain? [indo além do bitcoin]. *Tecnoblog*. 2017. Disponível em: https://tecnoblog.net/227293/como-funciona-blockchain-bitcoin. Acesso em: 23 dez. 2020.

Perguntas e respostas sobre o sandbox regulatório, SUSEP, 2020. Disponível em: http://www.susep.gov.br/setores-susep/ditec/perguntas-e-respostas-sobre-o-sandbox-regulatorio. Acesso em 23 dez. 2020.

REDAÇÃO PANORAMACRYPTO. 88 Insurtech quer democratizar acesso a seguros com a blockchain. *Panoramacrypto*. 2019. Disponível em: https://panoramacrypto.com.br/88-insurtech-quer-democratizar-acesso-a-seguros-com-a-blockchain. Acesso em: 04 dez. 2020.

Reguladores debatem o projeto sandbox, com vistas a ampliar a competição e fomentar a inovação, *CNSEG*, 2019. Disponível em: http://cnseg.org.br/noticias/reguladores-debatem-o-projeto-sandbox-com-vistas-a-ampliar-a-competicao-e-fomentar-a-inovacao.html. Acesso em: 19 dez. 2020.

RIZZARDO, Arnaldo. *Contratos*. 18. ed. Rio de Janeiro: Forense. 2019.

ROCHA, Lucas Salles Moreira; GOMES, Frederico Felix; MAFRA, Tereza Cristina Monteiro. Validade e Eficácia dos "Testamentos Inteligentes" via Tecnologia Blockchain. *Scientia Iuris*, Londrina, v.23, n.1, p.63-80, 2019.

SMART, Evander. Bitcoin is 100 times More Powerful than Google. *Cryptocoinsnews*. ac. 2015. Disponível em https://www.cryptocoinsnews.com/bitcoin-100-times-powerful-google. Acesso em: 16 dez. 2020.

SOARES, Pedro Silveira Campos. Anonimização na Lei Geral de Proteção de Dados requer posição da ANPD. CONJUR. 2019. Disponível em: https://www.conjur.com.br/2019-mar-10/pedro-soares-anonimizacao-lei-geral-protecao-dados. Acesso em: 21 dez. 2020.

STIGLITZ, Rubén S. Controle do Estado sobre a Atividade Seguradora. In: FÓRUM DE DIREITO DO SEGURO. 2., 2002, São Paulo. *Anais [...]*. São Paulo: IBDS/EMTS, 2002.

SUPERINTENDÊNCIA DE SEGUROS PRIVADOS. Comunicado Conjunto: Ação coordenada para implantação de regime de sandbox regulatório nos mercados financeiro, securitário e de capitais brasileiros. *SUSEP*. 2019. Disponível em: http://www.susep.gov.br/setores-susep/noticias/noticias/implantacao-de-regime-de-sandbox-regulatorio-nos-mercados-financeiro-securitario-e-de-capitais-brasileiros. Acesso em: 19 dez. 2020.

SZABO, Nick. *Smart Contracts*: *Building Blocks for Digital Markets*. ac. 1996. Disponível em: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html. Acesso em: 19 dez. 2020.

ULRICH, Fernando. *Bitcoin: a moeda na era digital*. São Paulo: Instituto Ludwig von Mises Brasil, 2014.

VENOSA, Sílvio de Salvo. *Direito Civil: Contratos em espécie*. 13. Ed. São Paulo: Atlas, 2013.