II CONGRESSO INTERNACIONAL DE DIREITO E INTELIGÊNCIA ARTIFICIAL

TECNOLOGIAS DISRUPTIVAS, DIREITO E PROTEÇÃO DE DADOS I

T255
Tecnologias Disruptivas, Direito e Proteção de Dados - I [Recurso eletrônico on-line] organização Congresso Internacional de Direito e Inteligência Artificial: Skema Business School – Belo Horizonte;

Coordenadores: Lorena Muniz e Castro Lage; Yuri Nathan da Costa Lannes; Marco Antônio Sousa Alves. – Belo Horizonte:Skema Business School, 2021.

Inclui bibliografia
ISBN: 978-65-5648-272-9
Modo de acesso: www.conpedi.org.br
Tema: Um olhar do Direito sobre a Tecnologia

1. Direito. 2. Inteligência Artificial. 3. Tecnologia. II. Congresso Internacional de Direito e Inteligência Artificial (1:2021 : Belo Horizonte, MG).

CDU: 34

II CONGRESSO INTERNACIONAL DE DIREITO E INTELIGÊNCIA ARTIFICIAL

TECNOLOGIAS DISRUPTIVAS, DIREITO E PROTEÇÃO DE DADOS I

Apresentação

Renovando o compromisso assumido com os pesquisadores de Direito e tecnologia do Brasil, é com grande satisfação que a SKEMA Business School e o CONPEDI – Conselho Nacional de Pesquisa e Pós-graduação em Direito apresentam à comunidade científica os 12 livros produzidos a partir dos Grupos de Trabalho do II Congresso Internacional de Direito e Inteligência Artificial (II CIDIA). As discussões ocorreram em ambiente virtual ao longo dos dias 27 e 28 de maio de 2021, dentro da programação que contou com grandes nomes nacionais e internacionais da área em cinco painéis temáticos e o SKEMA Dialogue, além de 354 inscritos no total. Continuamos a promover aquele que é, pelo segundo ano, o maior evento científico de Direito e Tecnologia do Brasil.

Trata-se de coletânea composta pelos 255 trabalhos aprovados e que atingiram nota mínima de aprovação, sendo que também foram submetidos ao processo denominado double blind peer review (dupla avaliação cega por pares) dentro da plataforma PublicaDireito, que é mantida pelo CONPEDI. Os oito Grupos de Trabalho originais, diante da grande demanda, se transformaram em doze e contaram com a participação de pesquisadores de vinte e um Estados da federação brasileira e do Distrito Federal. São cerca de 1.700 páginas de produção científica relacionadas ao que há de mais novo e relevante em termos de discussão acadêmica sobre a relação da inteligência artificial e da tecnologia com os temas acesso à justiça, Direitos Humanos, proteção de dados, relações de trabalho, Administração Pública, meio ambiente, formas de solução de conflitos, Direito Penal e responsabilidade civil.

Os referidos Grupos de Trabalho contaram, ainda, com a contribuição de 36 proeminentes professoras e professores ligados a renomadas instituições de ensino superior do país, os quais indicaram os caminhos para o aperfeiçoamento dos trabalhos dos autores. Cada livro desta coletânea foi organizado, preparado e assinado pelos professores que coordenaram cada grupo. Sem dúvida, houve uma troca intensa de saberes e a produção de conhecimento de alto nível foi, mais uma vez, o grande legado do evento.

Neste norte, a coletânea que ora torna-se pública é de inegável valor científico. Pretende-se, com esta publicação, contribuir com a ciência jurídica e fomentar o aprofundamento da relação entre a graduação e a pós-graduação, seguindo as diretrizes oficiais. Fomentou-se, ainda, a formação de novos pesquisadores na seara interdisciplinar entre o Direito e os vários

campos da tecnologia, notadamente o da ciência da informação, haja vista o expressivo número de graduandos que participaram efetivamente, com o devido protagonismo, das atividades.

A SKEMA Business School é entidade francesa sem fins lucrativos, com estrutura multicampi em cinco países de continentes diferentes (França, EUA, China, Brasil e África do Sul) e com três importantes acreditações internacionais (AMBA, EQUIS e AACSB), que demonstram sua vocação para pesquisa de excelência no universo da economia do conhecimento. A SKEMA acredita, mais do que nunca, que um mundo digital necessita de uma abordagem transdisciplinar.

Agradecemos a participação de todos neste grandioso evento e convidamos a comunidade científica a conhecer nossos projetos no campo do Direito e da tecnologia. Já está em funcionamento o projeto Nanodegrees, um conjunto de cursos práticos e avançados, de curta duração, acessíveis aos estudantes tanto de graduação, quanto de pós-graduação. Em breve, será lançada a pioneira pós-graduação lato sensu de Direito e Inteligência Artificial, com destacados professores da área. A SKEMA estrutura, ainda, um grupo de pesquisa em Direito e Inteligência Artificial e planeja o lançamento de um periódico científico sobre o tema.

Agradecemos ainda a todas as pesquisadoras e pesquisadores pela inestimável contribuição e desejamos a todos uma ótima e proveitosa leitura!

Belo Horizonte-MG, 09 de junho de 2021.

Profª. Drª. Geneviève Daniele Lucienne Dutrait Poulingue

Reitora – SKEMA Business School - Campus Belo Horizonte

Prof. Dr. Edgar Gastón Jacobs Flores Filho

Coordenador dos Projetos de Direito da SKEMA Business School

COMO O BLOCKCHAIN E O INTERNET OF THINGS PODEM REDUZIR FRAUDES NO MERCADO DE SEGURADORAS AUTOMOBILÍSTICAS

HOW MAY BLOCKCHAIN AND INTERNET OF THINGS REDUCE FRAUDS ON MOTOR INSURANCE MARKET

Marina Moretzsohn Chust Trajano [1]
Luísa de Almeida Naves [2]

Resumo

O presente artigo analisa o potencial das tecnologias de Blockchain e IoT na redução do número de fraudes em contratos de seguro automobilístico. Identificou-se que as fraudes acontecem principalmente em dois momentos: (i) no momento da contratação, quando há a tendência de enaltecer características positivas do motorista, e (ii) após o sinistro, com a tentativa de relatar um mesmo dano repetidamente ou de intensificá-lo. Conclui-se que, apesar das limitações do método, essas tecnologias podem contribuir para a manutenção da relação mutualística de confiança entre as partes, característica do contrato de seguradoras, possibilitando maior segurança jurídica.

Palavras-chave: Seguro automobilístico, Blockchain, Internet of things, Fraudes, Smart contracts

Abstract/Resumen/Résumé

This paper analyses the potential of Blockchain and IoT technologies on reducing the number of frauds in motor insurance contracts. It was identified that fraud occurs mainly on two moments: (i) while hiring, when there is a tendency to praise positive characteristics of the driver, and (ii) after the accident, with the report of aggravated damages or the attempt to make the claim repeatedly. It is concluded that, despite the limitations of the method, these technologies can contribute to the maintenance of the mutualistic relationship of trust between the parties, characteristic of the insurance contract, allowing greater legal certainty.

Keywords/Palabras-claves/Mots-clés: Motor insurance, Blockchain, Internet of things, Frauds, Smart contracts

[1] Graduanda em Direito na UFMG. Pesquisadora Associada do Centro DTIBR. Colaboradora da Muzzi e Advogados Associados, em âmbito cível e empresarial. Vice-Presidente da Liga de Mercado e Negócios da UFMG.

[2] Graduanda em Direito na UFMG e em Administração na SKEMA Business School.

1 INTRODUÇÃO

A pandemia da Covid-19 acentuou o *boom* digital que, além de romper com limites físicos de distância e tempo, ampliando o fluxo informacional, provocou consequências como a explosão da quantidade de tentativas de fraude. Nesse sentido, destaca-se o aumento no número total de tentativas de fraude, em 2020. No denominado "ano das fraudes", foram 371 mil tentativas de atos fraudulentos[1], um aumento de 276% em relação a 2019. Uma das causas para tamanha elevação foi a migração digital a partir do distanciamento social. Durante o ano, o número de transações online quase triplicou e, frente à adaptação do mercado ao digital, as perspectivas são de que essa alta continue.

Diante da relevância do tema, destina-se o presente artigo a analisar a jornada do consumidor do seguro, para discutir o potencial da tecnologia na assertividade das fraudes detectadas frente às suspeitas, a fim de garantir benefícios mútuos à seguradora e ao segurado.

No contrato de seguro, o segurador "se obriga, mediante o pagamento do prêmio, a garantir interesse legítimo do segurado, relativo a pessoa ou a coisa, contra riscos predeterminados″ (DINIZ, 2019). O prêmio é dividido por todos os segurados, e, quanto maior o risco, maior a contraprestação deverá ser para cobrir a garantia.

Percebe-se um problema: a partir do momento em que os valores do ressarcimento aumentam em razão de fraudes, o prêmio aumenta para todos os segurados. Assim, os prejuízos causados pela fraude não se limitam à relação entre a seguradora e o fraudador, mas se estendem à comunidade de segurados. Rompe-se, assim, a base fundamental do mercado de seguro, o mutualismo (CNSeg, 2019), que somente é alcançado com a boa-fé nas relações contratuais.

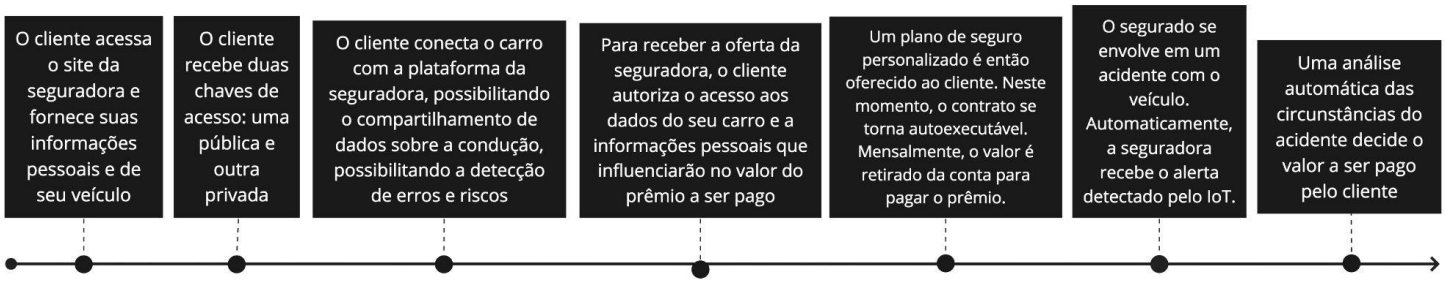
Em 2019, 14,09% do valor total pago por sinistros corresponde a suspeita de fraudes, 3,19% a fraudes detectadas, e 2,14% a fraudes comprovadas (CNSeg). Observa-se uma discrepância entre o número de sinistros suspeitos e o número detectado e comprovado.

3 METODOLOGIA

A fim de apresentar o impacto das tecnologias na prevenção de fraudes no seguro automobilístico, o presente artigo utiliza-se da jornada do consumidor descrita por Tim Roughton

[1] VALOR INVESTE. Tentativas de fraudes saltaram 276% em 2020.

e Peter Bidewell (2017) para identificar os pontos de melhora. A partir das oportunidades



identificadas, é desenvolvida uma discussão sobre benefícios e riscos no mercado brasileiro.

Dessa forma, diante da análise da jornada do cliente de uma seguradora automobilística, são detectados dois principais momentos de oportunidades tecnológicas para a redução das fraudes, como destacado por Nídia Cristino (2020). O primeiro é no momento da contratação, quando há a tendência de enaltecer características positivas do motorista, e, o segundo, após o sinistro, com o relato de danos agravados e tentativa de fazer a queixa do sinistro várias vezes, para obter mais recompensas.

4 SMART CONTRACTS

Nick Szabo (1996) define os *smart contracts* como sendo mais funcionais do que os contratos tradicionais, automatizando a performance das promessas previamente feitas no instrumento. Szabo ressalta o potencial dos smart contracts em minimizar *reactive security*, por meio de duas características: *verificable* (verificabilidade) e *observability* (observância). *Observability* se refere a observar a performance da outra parte, sendo essencial para detectar possíveis fraudes. *Verificable* consiste em poder provar o não cumprimento do contrato. Essas características são parte de uma *proactive security,* que dificulta a violação de contratos, sendo essenciais para detectar mais fraudes suspeitas, além de prevenir seu acontecimento.

O *smart contract* é uma forma de automatização das promessas contratuais. No processo em discussão, isso se daria principalmente no momento do pagamento do prêmio - com o desconto automático da conta do segurado -, no momento da detecção do sinistro e no pagamento do recurso, que se daria automaticamente a partir dos dados transmitidos pela *Internet of Things*.

Ainda, ressalta-se que *smart contracts* são baseados em uma ideia de condicional. Assim, no contrato de seguro automobilístico, temos que: se um sinistro ocorrer, então o segurado recebe

um valor (modelo: “se X, então Y”). A segunda parte dessa operação cabe à seguradora, que define previamente os valores de pagamento. Porém, o *input* dos dados da ocorrência de um evento pode ser uma limitação ao caráter inteligente desses instrumentos, devido à complexidade do modelo de negócio das seguradoras - que pode requerer a figura dos “oráculos”, a intervir no contrato a fim de introduzir a ocorrência do evento. Nídia Cristino (2020) discute a possibilidade da não existência da figura dos oráculos, de forma que sua função de inserir os eventos seria designada a outra tecnologia conectada aos veículos: *Internet of Things* (IoT).

6 *BLOCKCHAIN*

Como mencionado, *smart contracts* não são exclusivamente ligados a tecnologias. Sua raiz é baseada em contratos funcionais e autoexecutáveis (SZABO, 1996). É indiscutível, porém, a aplicação de tecnologias como meios de executar esses contratos automaticamente.

Blockchain é uma *distributed ledger technology* (DLT). É uma rede *peer-to-peer*, que valida transações baseando-se em um esquema de consenso, no qual todos devem aceitar os dados a serem inseridos na cadeia de registros, caracterizando a descentralização e garantindo segurança e imutabilidade (CONG, HE, 2018). Essa noção de rede de consenso descentralizada gera discussões sobre a necessidade de se balancear transparência e privacidade (CONG, HE, 2018), mas Daniel Batalha (2018) destaca que isso não representa um perigo eminente à privacidade, pois é possível utilizar sistemas de acesso restrito (*permissioned*).

O *Blockchain* em questão seria uma rede privada, no qual a mineração e tratamento dos dados seria restrita a certos participantes. Além de garantir mais privacidade para o cliente, a rede privada permite delimitar responsabilidade para a seguradora e definir a figura do *data controller*, o que não seria possível em uma rede pública. Somado ao acesso restrito aos dados no *Blockchain*, informações pessoais seriam ocultas, uma vez que todos os dados são criptografados e apenas o titular, que possui a chave privada, consegue acessá-los.

Um problema derivado desse acesso exclusivo pela chave privada é: se ninguém consegue saber quem é o usuário, como as seguradoras controlam seu negócio? A resposta é dada por Bidwell & Roughton, (2018), que argumentam ser possível ceder o acesso a certos usuários de dados criptografados necessários para uma atividade bem específica do processo.

Nídia Cristino (2020) destaca que, com os benefícios de privacidade e transparência, o *Blockchain* tem o potencial de ser uma garantia contra qualquer forma de manipulação dos dados para obter benefícios. Além da segurança, a base de dados de transações anteriores torna possível identificar padrões de comportamento fraudulento, contribuindo para ações preventivas.

7 *INTERNET OF THINGS*

A *Internet of Things* (IoT) refere-se à interconexão digital de objetos resultante da articulação entre itens utilizados cotidianamente à rede mundial de computadores. Dorri, Kanhere e Jurdak (2016), apontam que essa tecnologia se apresenta como uma evolução natural da Internet, que passa de uma rede de computadores para uma de sistemas embutidos e ciber-físicos. Viabiliza-se, portanto, o uso de equipamentos dotados de sensores destinados à extração de dados relativos ao usuário de modo conexo à Internet, promovendo combinações, processamento e organização desses dados conforme a finalidade em questão.

No mercado de seguros, o uso da IoT - a partir de dispositivos instalados em automóveis - pode ser determinante no combate às fraudes. Isso se dá, principalmente, em razão do acesso direto do seguradora às informações, passando a independer de comunicações do segurado. Nesse sentido, destaca-se a atuação da IoT no combate às fraudes que ocorrem no momento da contratação do serviço. Isso se dá quando os dispositivos de IoT recolhem dados referentes à condução do veículo pelo cliente, de modo a possibilitar uma aferição do risco conforme o perfil do segurado, podendo, ainda, ser adaptado conforme eventuais alterações que venham a ocorrer. Esse fator, além de traçar um perfil do cliente que previne fraudes no momento inicial do contrato de seguro, pode ser determinante, ainda, na definição do prêmio. Ressalta-se, assim, que as vantagens do IoT não se aplicam somente ao segurador, ao possibilitar o acesso a produtos e preços personalizados conforme o perfil do cliente. Tem-se, por exemplo, a configuração de modalidades de seguro com base no uso, como são os seguros *pay as you drive* (PAYD) e *pay how you drive* (PHYD), que oferecem cobertura a bens cujo preço está ligado à quantidade e à qualidade de circulação, respectivamente.

Referida aplicação tecnológica é importante, ainda, para resguardar a seguradora em caso de imbróglios em momentos posteriores à contratação - como a ocorrência de sinistros. Assim, a coleta e o tratamento de dados referentes ao evento em questão permitem à seguradora o

aferimento da veracidade das alegações do segurado, além da mensuração dos danos agravados. Ainda, em atuação conjunta com o *Blockchain*, agrega maior celeridade à cobertura do infortúnio, ao promover a comunicação imediata à seguradora em caso de acidente e promover a quitação automática do valor necessário.

8 ASSERTIVIDADE DE DETECÇÃO DE FRAUDE E INVERSÃO DO ÔNUS DA PROVA

Ressalta-se que a grande maioria das relações contratuais entre seguradoras e seus clientes é classificada como contrato de adesão. Dadas as limitações negociais dessa modalidade e o predomínio da vontade de um dos contratantes, pode-se presumir a hipossuficiência do consumidor, caracterizando uma vulnerabilidade acentuada que permite a utilização de instrumentos contundentes de defesa do consumidor, como a inversão do ônus da prova.

Essa aplicação é possível quando é consumerista a relação entre contratante e contratado, em que os seguradores se encaixam na definição de fornecedor prevista no artigo 3º do Diploma Consumerista - sendo pessoa jurídica de direito privado nacional que desenvolve atividade de prestação de serviços, ou seja, qualquer atividade fornecida no mercado de consumo, mediante remuneração, inclusive as de natureza securitária.

Nos casos de fraudes em que a determinação da redistribuição do ônus da prova gera dificuldade às seguradoras para provar que é falso o alegado pelo segurado, o uso das tecnologias como o Iot - junto à capacidade do *Blockchain* de aportar mais eficiência, velocidade e transparência às transações com registros invioláveis e inalteráveis- pode tornar muito mais céleres e assertivas as ações judiciais que litigam em torno dessas questões.

9 CONSIDERAÇÕES QUANTO À PROTEÇÃO DE DADOS

A Lei Geral da Proteção de Dados (LGPD) entrou em vigor em 15 de agosto de 2020. Desde então, passou a ser essencial que o tratamento de dados pessoais entre seguradoras e segurados se adequasse a novas políticas de privacidade e proteção de dados, visando à consagração do fim último da LGPD - devolver ao titular de dados o poder de decisão e conhecimento sobre a forma com que seus dados são tratados, e, a partir da proteção concedida a essas informações, garantir o livre desenvolvimento da personalidade da pessoa natural.

A LGPD apresenta requisitos de forma e conteúdo específicos para o consentimento[2], de forma que o titular apresente efetiva consciência sobre seus dados. Assim, o consentimento deve ser: (i) livre, podendo o titular escolher se seus dados serão tratados ou não; (ii) informado, de modo que o indivíduo tome conhecimento da forma e da finalidade[3] - que, por sua vez, deve ser específica, legítima e explícita; e (iii) inequívoco, não restando dúvidas de que foi concedido de modo específico para determinado fim, devendo ser escrito, de modo destacado, ou representado para demonstrar a manifestação de vontade do titular. Ainda, ressalta-se que o consentimento pode ser revogado a qualquer momento.

Mesmo com o devido consentimento sobre o tratamento dos dados, o artigo 18 da LGPD[4] dispõe que o titular tem o direito de solicitar a eliminação dos dados pessoais. Além disso, o artigo 16[5], determina que esses dados sejam eliminados após o término do tratamento, momento que eles não são mais necessários. Ambas exigências legais conflituam com a natureza imutável do *Blockchain*, uma vez que não é tecnicamente possível a remoção de dados. Roughton e Bidewell (2018) resolvem esse problema, argumentando que (i) as características de armazenamento permanente dos dados, intrínsecas do funcionamento do *Blockchain* configuram como um motivo para a necessidade de manter os dados, e são legítimos se comunicados ao titular no momento do consenso; (ii) como os dados são criptografados, eles não configuram dados pessoais, porque apenas o titular que possui a chave privada consegue acessar.

10 CONCLUSÃO

O presente trabalho foi realizado por meio de pesquisa teórica e estudo de casos das potencialidades das tecnologias, o que apresenta-se como limitação, uma vez que não há dados para provar a real eficácia do demonstrado no mercado de seguradoras do Brasil. Assim,

---

[2] XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;
[3] Art. 6º (...) I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível (...)
[4] IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei; … VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
[5] Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades: IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

recomenda-se um aprofundamento nas pesquisas buscando experiências em outros países que já tenham testado essas tecnologias no mercado em discussão.

O *smart contract* possibilita então, por meio da utilização das tecnologias de IoT e *Blockchain*, agir sob os principais problemas discutidos na introdução do presente artigo. Assim, as fraudes no momento da contratação seriam minimizadas, uma vez que o comportamento do usuário do carro seria baseado em critérios objetivos frutos da IoT. As fraudes relativas a um incidente específico também seriam evitadas por meio da auto execução do contrato e imutabilidade das informações no *Blockchain*. Dessa forma, as tecnologias contribuíram para manter a relação mutualística de confiança, característica do contrato de seguradoras, possibilitando maior segurança jurídica e assertividade do instituto.

REFERÊNCIAS

BATALHA, Daniel Augusto de Senna Fernandes, **Criptocontratação : Uma nova forma de contratação automatizada?** Dissertação de Mestrado em Direito: Especialidade em Ciências Jurídico-Forenses apresentada à Faculdade de Direito, Coimbra, Disponível em: http://hdl.handle.net/10316/85817. Acesso em: 18 Abr. 2021

BRASIL. **Lei nº 13.709**, de 14 de agosto de 2018.

CONFEDERAÇÃO NACIONAL DAS EMPRESAS DE SEGUROS GERAIS, PREVIDÊNCIA PRIVADA E VIDA, SAÚDE SUPLEMENTAR E CAPITALIZAÇÃO - CNseg. **Prevenção e Combate à Fraude em Seguros.** 2019. Disponível em: https://bityli.com/k42fu Acesso em: 20 Abr. 2021.

CONFEDERAÇÃO NACIONAL DAS EMPRESAS DE SEGUROS GERAIS, PREVIDÊNCIA PRIVADA E VIDA, SAÚDE SUPLEMENTAR E CAPITALIZAÇÃO - CNseg. **Quantificação da Fraude no Mercado de Seguros Brasileiro.** 2019. Disponível em: https://bityli.com/cXZpg Acesso em: 20 Abr. 2021.

CONG, Lin William; HE, Zhiguo. **Blockchain disruption and smart contracts**. Social Science Research Network, [s. l.], p. 1-40, Dec. 2018. Disponível em: https://bityli.com/6ehFg. Acesso em: 18 Abr. 2021

CRISTINO, Nídia Simões, **Insurtech: a Aplicação da Tecnologia ao Setor dos Seguros.** Dissertação no âmbito do Mestrado em Ciências Jurídico Empresariais, Coimbra, Disponível em: https://eg.uc.pt/handle/10316/92716 Acesso em: 18 Abr. 2021

DINIZ, Gustavo Saad. **Curso de Direito Comercial**. 1. ed São Paulo: Atlas, 2019, 693-694 p.

DORRI, A.; KANHERE, S. S.; JURDAK, R. Blockchain in Internet of Things: challenges and solutions. Agosto de 2016. Disponível em: <https://arxiv.org/ftp/arxiv/papers/1608/1608.05187.pdf>. Acesso em: 24 abr. 2021.

ROUGHTON, Tim; BIDWELL, Peter. **Smart Insurance Contracts.** 2017. Disponível em:https://bityli.com/q7zgH. Acesso em: 18 Abr. 2021

SZABO, Nick. **Smart Contracts: Building Blocks for Digital Markets**. Phonetic Sciences Amsterdam. 1996. Disponível em: https://bityli.com/RfN7H. Acesso em: 18 Abr. 2021.

VALOR INVESTE. **Tentativas de fraudes saltaram 276% em 2020**. Disponível em: https://bityli.com/spNCm. Acesso em: 17 abr. 2021