Revista Brasileira de
Risco e Seguro

Blockchain e seu Impacto no Mercado de Seguros

Raquel Fernández dos Santos
Atuária graduada pela Universidade do Estado do Rio de Janeiro – UERJ; Membro do Instituto Brasileiro de Atuária; certificada em Global Branding pela Faculdade de Economia e Business – Amsterdam University of Applied Sciences; Técnica em informática com ênfase em comunicação pelo Instituto de Tecnologia ORT e aluna do curso MBA em Gestão de Seguros e Resseguros da Escola Nacional de Seguros. Experiência profissional no mercado de resseguros e com perícias em previdência complementar.
raquel.fnz@gmail.com

Resumo

Blockchain é uma tecnologia de infraestrutura de dados que ganhou atenção por fazer da *bitcoin* a primeira moeda digital descentralizada a superar o problema de gasto duplo. A solução inovadora proposta por Satoshi Nakamoto para garantir segurança e transparência em transações descentralizadas com *bitcoin* tem quatro pilares: *Ledger* digital descentralizado *blockchain*, Protocolo de consenso *Proof of Work* – PoW, criptografia e redes *peer-to-peer* – P2P. A *blockchain* é uma das tecnologias usadas pela *bitcoin* e outras moedas digitais, que despertou o interesse de muitas empresas de seguros em adotar esse tipo de *ledger* em seus negócios. Este artigo tem por objetivo explicar como o armazenamento de dados no *ledger* digital *blockchain* funciona, o que é uma função *hash* e no que se constituem os protocolos de consenso PoW. Também pretende ressaltar possíveis aplicações *blockchain* no mercado segurador e a importância da troca de conhecimento entre profissionais de tecnologia da informação e de seguros, a fim de superar possíveis barreiras na implementação de novas tecnologias digitais no modelo de negócio das seguradoras no Brasil.

Palavras-chave

Blockchain; Seguros; Tecnologia; *Ledger* digitais descentralizados; PoW; *Hash*; Contratos inteligentes.

Sumário

Abstract

Blockchain and its impact on the insurance market

Raquel Fernández dos Santos
Actuarial graduated from the State University of Rio de Janeiro – UERJ; Member of the Brazilian Institute of Actuarial; Certified in Global Branding by the Faculty of Economics and Business – Amsterdam University of Applied Sciences; Computer technician with emphasis in communication by the ORT Institute of Technology and student of the MBA course in Insurance and Reinsurance Management of the National School of Insurance. Professional experience in the reinsurance market and with expertise in private pension.
raquel.fnz@gmail.com

Summary

Blockchain is an infrastructure technology that has gained attention by making bitcoin the first decentralized digital currency to overcome the Double Spending problem. The innovative solution proposed by Satoshi Nakamoto in his 2008 article for secure, transparent and decentralized transactions in bitcoin has four pillars: Digital Ledger Technology Blockchain, Proof of Work consensus protocol, encryption, and a peer-to-peer network. The blockchain was one of the technologies used by bitcoin and by other digital currencies that has aroused the interest of many companies by applications of technologies like decentralized digital Ledgers in their businesses. This article aims to explain how data storage in the blockchain works, what is a hash function, what is an PoW consensus protocols, besides highlighting possible blockchain applications in the insurance market and the importance of exchanging knowledge between information technology and insurance professionals to overcome possible barriers for the implementation of new digital technologies in the insurance business model in Brazil.

Keywords

Blockchain, Insurance, Technology, Distributed Ledger Technology, PoW, hash, Smart Contracts.

Contents

Sinopsis

Blockchain y su impacto en el mercado de seguros

Raquel Fernández dos Santos
Actuarial se graduó de la Universidad Estatal de Río de Janeiro – UERJ; Miembro del Instituto Brasileño de Actuarial; Certificado en Global Branding por la Facultad de Economía y Empresa de la Universidad de Ciencias Aplicadas de Amsterdam; Técnico informático con énfasis en comunicación por el Instituto de Tecnología de ORT y estudiante del curso de MBA en Gestión de Seguros y Reaseguros de la Escuela Nacional de Seguros. Experiencia profesional en el mercado de reaseguros y con experiencia en pensiones privadas.
raquel.fnz@gmail.com

Resumen

Blockchain es una tecnología de infraestructura de datos que ha llamado la atención por hacer de Bitcoin la primera moneda digital descentralizada en superar el problema del doble gasto. La solución innovadora propuesta por Satoshi Nakamoto para garantizar la seguridad y la transparencia en las transacciones descentralizadas de bitcoins tiene cuatro pilares: ledger de bloque digital descentralizado, Prueba de trabajo: protocolo de consenso PoW, cifrado y redes P2P de igual a igual. La cadena de bloques es una de las tecnologías utilizadas por bitcoin y otras monedas digitales, lo que ha despertado el interés de muchas compañías de seguros en adoptar este libro de contabilidad digital en sus negocios. Este artículo tiene como objetivo explicar cómo funciona el almacenamiento de datos en el libro de contabilidad digital blockchain, qué es una función hash y protocolos de consenso PoW, así como destacar las posibles aplicaciones de blockchain en el mercado de seguros y la importancia del intercambio de conocimiento entre los profesionales de la tecnología en la industria. información y seguros para superar posibles barreras en la implementación de nuevas tecnologías digitales en el modelo de negocio de las aseguradoras en Brasil.

Palabras-Clave

Blockchain; Seguro; Tecnología; Libro mayor descentralizado digital; PoW; Hash; Contratos inteligentes.

Sumario

1. Introdução

Novas tecnologias têm mudado o modelo de negócio de seguros em todo mundo. *Startups* atuais estão encarando soluções tecnológicas como o centro de seus negócios, e não mais como uma ferramenta auxiliar. Atender à crescente demanda das áreas urbanas e manter a qualidade dos serviços e do relacionamento das empresas com seus clientes tem sido possível por intermédio de tecnologias capazes de automatizar processos e de promover transparência e segurança para milhões de cidadãos. O mercado vem encarando um desafio que vai além da implementação dessas novas tecnologias em seus processos, o de tornar o entendimento delas acessível e de fácil compreensão para *stakeholders* e órgãos reguladores que não são da área tecnológica, a fim de facilitar as tomadas de decisões e criar engajamento e consciência sobre as possíveis aplicações baseadas em evidências, e não em otimismo sem garantias.

Segundo o Departamento de Assuntos Econômicos e Sociais das Nações Unidas, o número de pessoas vivendo em áreas urbanas em 1950 era de 751 milhões. Este subiu para 4,2 bilhões em 2018. O aumento da população urbana e a crescente capacidade de grupos se conectarem vêm gerando muitos desafios e oportunidades para diversos mercados, inclusive o de seguros. Para lidar com esse novo cenário, tecnologias digitais têm sido fundamentais para resolver questões relacionadas a transportes sustentáveis, cadeias de suprimentos, transações financeiras, segurança na transferência de dados e resiliência para essa crescente população.

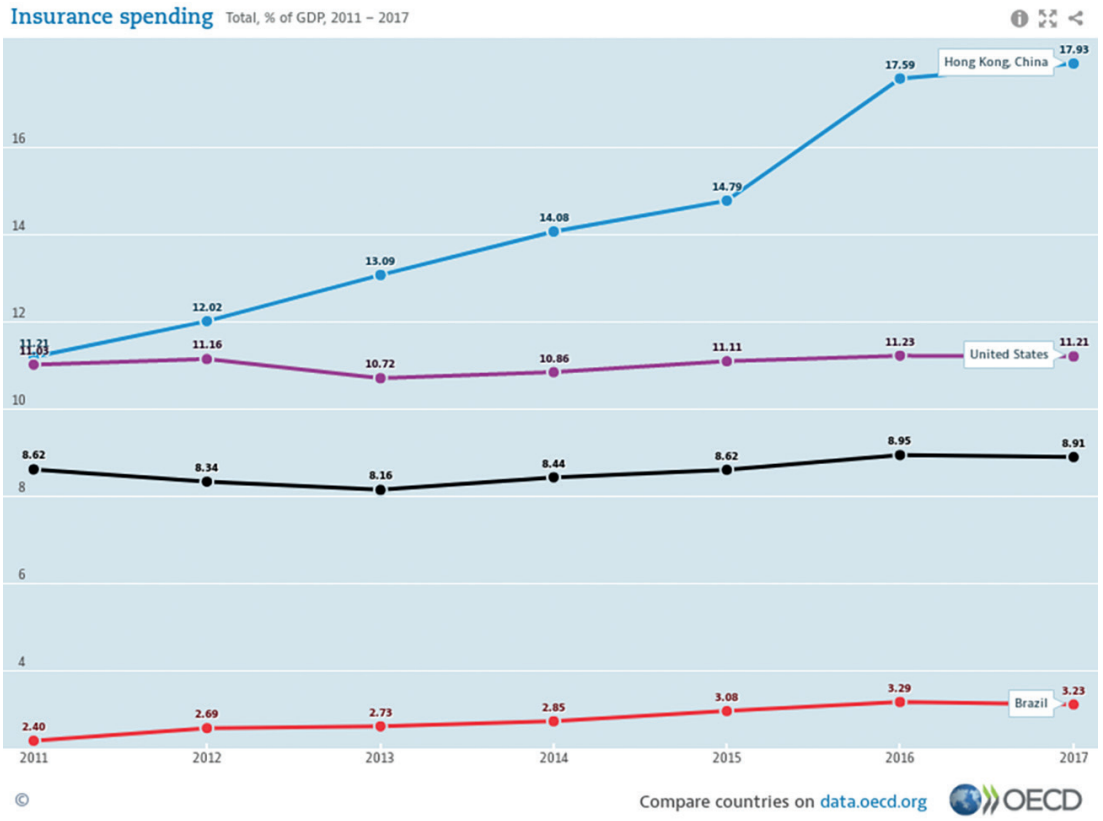
Seguradoras, por sua vez, têm usado técnicas de Inteligência Artificial na forma de *ChatBots* e algoritmos de aprendizado de máquina para oferecer produtos de seguros pertinentes aos segurados, além de verificações de fraudes. Junto com a Inteligência Artificial, *ledgers* digitais descentralizados também têm sido muito explorados no ramo de seguros pelo seu potencial na automatização de subscrição de contratos, agilidade na liquidação de sinistros, registro de informações e na redução de fraudes. As possíveis aplicações dessas tecnologias se destacam por três razões principais: segurança, transparência e custos baixos.

Há um número crescente de *startups* que estão criando inovações no setor financeiro e de seguros baseando seus processos em tecnologias, as *fintechs* e *insurtechs*. Essa nova mentalidade de inovação tecnológica em seguros também passou a despertar interesse de empresas bem consolidadas, como Allianz, IBM, Marsh, AIG, e a criação de iniciativas, como a B3i, *The Blockchain Insurance Industry Initiative.*

Apesar de o Brasil ainda não ter a cultura do seguro tão forte, esse mercado vem crescendo. Sua contribuição para o PIB e inovações disruptivas terão grande impacto na economia. O uso de *ledgers* digitais descentralizados em seguros, como a *blockchain*, ainda está em fase inicial e tem demonstrado grande potencial. Este artigo visa a exemplificar aplicações da dessa tecnologia em seguros e ajudar a promover seu entendimento, bem como a modernização de processos, incentivando o crescimento robusto e sustentável de uma nova era do mercado em questão.

"Blockchain has a powerful role to play in the future of insurance."
Rob Schimek, CEO of Commercial, AIG.

Total, % do PIB de 2011 a 2017, anual para o Brasil (BRA), Hong Kong (HKG), Estados Unidos (USA) e todo os países (OECD):



2. Importância da *blockchain*

Como há 20 anos plataformas digitais de comunicação e *e-commerce,* dentre outras, transformaram modelos de negócios, tecnologias como a *blockchain* também têm o potencial de revolucionar o modo como pessoas e empresas interagem.

Segundo o relatório *Blockchain and Insurance –The Trust Machine (Disruptive Technology: Insurance),* da Fitch Ratings, os benefícios da *blockchain* para as seguradoras incluem:

- Redução de custos;
- Redução de etapas no processo de pagamento;
- Contratos inteligentes;
- Seleção de riscos e precificação;
- Redução de fraudes e gerenciamento de sinistros.

A *blockchain* é uma tecnologia de infraestrutura que ganhou atenção ao fazer da *bitcoin* a primeira moeda digital descentralizada a superar o problema do gasto duplo. Tal se deu após a publicação do artigo *Bitcoin: A Peer-to-Peer Electronic Cash System,* em 2008, por Satoshi Nakamoto.

2.1 Gasto duplo

Dados digitais são facilmente reproduzíveis e por isso é difícil construir confiança em transações desse tipo. Normalmente se faz necessário um intermediador, um terceiro que valide essas trocas, devido ao problema que chamamos de gasto duplo. Diferente do mundo físico, arquivos digitais podem ser duplicados. O repasse de um arquivo normalmente é o de uma cópia, sem a garantia de que o remetente tenha apagado a sua versão original. O envio de uma cópia é um bom meio para transferência de informações, mas não quando se trata de dinheiro, propriedade intelectual, *loyalty points* etc.

Atualmente, pessoas de qualquer lugar do mundo já podem efetuar diversos tipos de transações *peer-to-peer* de maneira segura, através de plataformas colaborativas e criptografia. Assim, dados não são mais armazenados em uma autoridade central, mas distribuídos em *ledgers* globais. Quando uma transação é efetuada, todos os computadores da rede recebem essa informação e os conservam sob forma de blocos em uma cadeia *blockchain*, que nada mais é do que um *ledger* digital descentralizado. Este, que também é público, permite aos participantes verificar e auditar transações de maneira independente e relativamente barata.

3. Armazenamento de dados na *blockchain*

Blockchain significa “encadeamento de blocos”. Esses blocos, ligados uns aos outros de forma linear e cronológica, contêm informações como registros de transações, além de uma “impressão digital”, o *hash*.

Quando o número de registros em um bloco alcança sua capacidade máxima, então outros computadores da rede trabalham em sua validação, para anexá-lo à cadeia de blocos da *blockchain*. No contexto *bitcoin*, esse processo de validação é conhecido como mineração. Para validar os blocos, diversas máquinas trabalham na solução de um quebra-cabeças. O vendedor anexa o novo bloco à cadeia. Essa etapa é conhecida como *Proof of Work*. Em seguida, o novo bloco recebe informações dos blocos anteriores. Informações dentro da *blockchain* podem ser consideradas confiáveis, uma vez que, validadas e anexadas à cadeia de blocos, não podem ser alteradas sem o consentimento da maioria dos computadores da rede.

3.1 Função *hash*

As funções *hash* são unidirecionais, com entrada de mensagens com comprimento arbitrário e saída de valor fixo *hash,* também com comprimento fixo. Esse valor de *hash* é um tipo de assinatura para a mensagem de entrada. Por ser uma função unidirecional, o cálculo do valor do *hash* a partir de uma determinada mensagem é simples, porém, o caminho de volta, não. Transações computacionais cuja reversão é impraticável protegem os vendedores de fraude.

Funções *hash* são usadas em aplicativos de segurança, como autenticação, verificação de integridade de mensagens, certificados e assinaturas digitais.

A segurança desses aplicativos depende da força criptográfica da função *hash* subjacente. Portanto, algumas propriedades de segurança são necessárias para fazer uma função *hash H* adequada para tais usos criptográficos:

- P1. Dado um valor de *hash* h, deve ser difícil encontrar qualquer mensagem m tal que $h = H(m)$
- P2. Dada uma mensagem m_1, deve ser difícil encontrar outra mensagem $m_2 \neq m_1$, em que $H(m_1) = H(m_2)$.
- P3. Deve ser difícil encontrar diferentes mensagens m_1 e m_2 de modo que $H(m_1) = H(m_2)$.

Sendo assim, o *hash* é uma função matemática que gera um código identificador único para cada bloco de dados que é anexado ao conteúdo de cada transação. Se algo for alterado no bloco, então o resultado dessa função também se modifica.

Os blocos da *blockchain* são ligados pelo resultado dessas funções da seguinte maneira: o bloco posterior contém o valor *hash* do bloco anterior, além dos seus próprios registros de transação e valor *hash*. A *blockchain* possui inúmeros blocos, ligados uns aos outros por esses identificadores únicos. Novos blocos são adicionados linear e cronologicamente.

3.2 *Proof of Work* (PoW)

No artigo *Bitcoin: A Peer-to-Peer Electronic Cash System*, Satoshi Nakamoto sugeriu uma solução para o problema do gasto duplo usando um *peer-to-peer distributed timestamp server* para gerar prova computacional da ordem cronológica das transações. O sistema é seguro desde que os nós (computadores) honestos da rede controlem coletivamente mais energia da CPU do que qualquer grupo cooperativo de nós atacantes.

Segundo Nakamoto, o beneficiário, em uma transação via *blockchain,* precisa da prova de que a maioria dos computadores da rede concordou que ele foi o primeiro a receber o benefício (*bitcoin*, no caso).

A solução proposta começa com um servidor *timestamp,* que funciona pegando um *hash* de um bloco a ser estampado no bloco seguinte.

O PoW envolve a resolução de um quebra-cabeças, que nada mais é do que um algoritmo de consenso, como o *Proof of Stake* (PoS). Este depende da função *hash* que é aplicada em todo conteúdo do bloco: valor *hash* do bloco anterior, transações e um número arbitrário – nonce. O nonce é a única parte do bloco que o nó pode alterar a fim de resolver o quebra-cabeças. O resultado deve começar com um número *n* de bits zero. O trabalho médio gasto nesse processo é exponencial ao número *n* de bits zero requeridos e pode ser verificado pela execução de um único *hash*. A resolução desse problema é por “força bruta” e precisa de grande poder computacional. Protocolos PoW são eficientes para deter ataques abusivos, como *spam*.

Uma vez que o esforço computacional necessário foi gasto para satisfazer o sistema PoW, o bloco pode ser anexado à *blockchain* e não deve ser alterado sem que esse trabalho seja refeito. Como blocos subsequentes são ligados a essa cadeia através do *hash*, o trabalho de alteração exigiria as mudanças dos blocos posteriores também.

Em muitos protocolos criptográficos, um provador procura convencer um verificador de que ele possui conhecimento de um segredo ou que certa relação matemática é verdadeira. Em contraste, em um PoW, um provador demonstra a um verificador que ele realizou uma determinada quantidade de trabalho computacional em um intervalo de tempo específico.

Como o PoW é um algoritmo de consenso, também determina representação da maioria em processos de tomada de decisões. A decisão da maioria seria a cadeia mais longa, ou seja, aquela com maior esforço computacional de computadores honestos trabalhando.

3.2.1 Problema da ruína do jogador

Em caso de um ataque, o PoW teria que ser refeito para modificar os blocos subsequentes. A probabilidade de um atacante recuperar esse atraso diminui exponencialmente à medida que novos blocos são adicionados à *blockchain*.

Considere o cenário de um invasor tentando gerar uma cadeia alternativa mais rapidamente que a cadeia honesta. Essa corrida entre as cadeias seria caracterizada por uma *Binomial Random Walk*, ou passeio aleatório, que descreve o caminho de uma sucessão de passos aleatórios. No contexto *bitcoin*, a probabilidade de um atacante invasor se recuperar de um determinado déficit (necessidade de modificação dos blocos subsequentes) é análoga ao exemplo clássico aplicado em processos estocásticos: problema da ruína do jogador.

O problema da ruína do jogador foi proposto pela primeira vez em uma carta de Blaise Pascal para Pierre Fermati, em 1656. Contudo, o termo "ruína do jogador" foi usado anos depois.

Suponha que exista um jogador (atacante) com créditos ilimitados em uma situação de déficit e infinitas tentativas para alcançar o ponto de equilíbrio:

- p = probabilidade de um nó honesto encontrar o próximo bloco (probabilidade de ganhar).
- q = probabilidade de um nó atacante encontrar o próximo bloco (probabilidade de perder, de tal forma que $p + q = 1$).
- w = probabilidade de o atacante se recuperar do déficit dos z blocos atrás (probabilidade de ruína).

$$w = \begin{cases} 1, se\ p \leq q \\ \left(\frac{q}{p}\right)^z, se\ p > q \end{cases}$$

Supondo que p > q, a probabilidade decresce exponencialmente conforme novos blocos são adicionados à cadeia.

4. *Blockchain* pública e privada

Sendo assim, *blockchain* é uma cadeia de blocos que contém um histórico de transações. Cada novo bloco dessa cadeia se liga ao anterior e assina seu conteúdo com uma "impressão digital" (*hash*) dentro de uma rede *peer-to-peer* (P2P). Os participantes da rede podem acessar e compartilhar dados (*third-party, consensus-based trust*).

Todos os participantes mantêm um registro criptografado de cada transação nessa rede descentralizada. Não ter um intermediário e continuar executando relações comerciais de maneira confiável reduz custos indiretos ao negócio.

Empresas, então, podem fazer uso de uma plataforma *blockchain* privada em seus negócios, aquela em que os participantes precisam receber uma autorização para integrar a rede. Assim, também passam a manter um registro criptografado de cada transação ali ocorrida. Nesse tipo de plataforma *blockchain* todas as possíveis partes envolvidas são conhecidas previamente.

Plataformas *blockchain* públicas seriam aquelas em que qualquer um na internet tem acesso ao *ledger*, como a *bitcoin*.

5. Contratos inteligentes (*Smart contracts*)

Blockchain também se estende para contratos, os chamados *smart contracts* ou contratos inteligentes. A palavra "inteligente" vem do fato de que a avaliação das cláusulas do contrato e a execução do código cabível acontecem sem intervenção humana. Os contratos inteligentes são autoexecutáveis e acionados com base em eventos predefinidos e pré-acordados.

O elo entre o mundo físico e a *blockchain* dos contratos inteligentes é o *oracle* (oráculo). Este é um intermediário confiável e uma parte integrante do ecossistema dos contratos inteligentes. A *blockchain* por si só não pode acessar dados de fora de seu sistema, portanto, os dados são fornecidos através de um *oracle* que pode ser baseado em *hardwares, softwares* ou consenso. Exemplos de oráculos de *hardware* são sensores, Internet das Coisas (*IoT)* e estações meteorológicas.

A tecnologia *blockchain* da *Oracle* é baseada no Hyperledger ® Fabric, desenvolvido por uma comunidade de colaboradores e promovido pela Linux Foundation. A Linux Foundation é formada por membros corporativos de diversos setores da indústria que trabalham juntos para solucionar problemas em negócios e tecnologia através da colaboração de código aberto. A Oracle é um desses membros.

O Hyperledger ® Fabric fornece os principais recursos *blockchain* de *smart contracts* e pode executar até milhares de transações por segundo.

6. Aplicações de plataformas *blockchain* em seguros

A *blockchain* também facilita o relacionamento *business-to-business* (B2B), compartilhando dados e executando transações de maneira confiável, barata e rápida entre as partes envolvidas.

Relacionamentos comerciais confiáveis dependem do compartilhamento de dados e da verificação de transações. No mundo digital, realizar transações é uma tarefa complexa que envolve partes em todo o mundo. Até recentemente não havia como verificar a autenticidade dos itens trocados ou rastrear a execução das transações sem intermediários como bancos, fornecedores de EDI (*Eletronic Data Interchange*), parceiros comerciais e corretores de logística.

Fazer esse rastreamento entre muitas partes e seus respectivos dados pode gerar atrasos onerosos e aumentar os riscos relacionados à segurança. Como a *blockchain* tem a capacidade de amenizar algumas dificuldades operacionais, agilizando os processos de negócios e aumentando a confiança neles, essa tecnologia tem o potencial de tornar o trabalho das seguradoras menos custoso e também contribuir para a mitigação de riscos operacionais de setores segurados para realizar rastreamento de remessas, empréstimos, negociações etc.

7. Aceitação do mercado

A American Association of Insurance Services (AAIS), organização nacional de consultoria em seguros sem fins lucrativos, lançou um piloto da OpenIDL (*Open Insurance Data Link*) para transformar relatórios regulatórios de seguros na Plataforma IBM *Blockchain*, que é alimentada pelo Hyperledger ® Fabric.

OpenIDL é uma rede criada na IBM *Blockchain Platform* com a AAIS para automatizar os relatórios normativos de seguros e simplificar os requisitos de conformidade, aumentando a eficiência e a precisão para as seguradoras e os departamentos de seguros estatais.

O Hyperledger é um esforço colaborativo de código aberto criado para promover as tecnologias *blockchain* de vários setores. É uma colaboração global, hospedada pela The Linux Foundation, incluindo líderes em finanças, bancos, Internet das Coisas, cadeias de suprimentos e tecnologia.

A B3i, *The Blockchain Insurance Industry Initiative,* um desenvolvedor líder de plataformas de transações de seguros, anunciou a expansão de sua comunidade representada por mais de 40 empresas entre clientes, membros e acionistas. O B3i tem agora 16 acionistas, incluindo algumas das maiores seguradoras e resseguradoras do mundo.

A PolicyPal Network lançou um seguro para atraso de voo utilizando *blockchain*. O processo é automatizado por meio de *smart contracts*.

A Seguros Sura adotou a tecnologia dos *smart contracts* no processo de gravação e envio de apólices, endossos e boletos.

A IBM, AIG e Standard Chartered também se uniram para criar uma apólice baseada em *blockchain*, oferecendo um novo nível de confiança e transparência no processo de subscrição de seguros.

O IBM *Blockchain* oferece suporte à Marsh, ISN e ACORD na criação de *ledgers* distribuídos autorizados. Construído com base na tecnologia Hyperledger, este é usado para melhorar o desempenho e a confiabilidade das transações.

A Allianz Global Corporate & Specialty (AGCS) implementou com sucesso um protótipo de *blockchain* para um programa global de seguro cativo.

8. Conclusão

A tecnologia *blockchain* tem conquistado a atenção do mercado segurador devido ao seu potencial na redução de custos operacionais, registros eficientes e precisão na avaliação de riscos com os contratos inteligentes. Estes últimos são protocolos computacionais executados automaticamente a partir de regras pré-fixadas. Essa tecnologia emergente também permite o registro de transações de forma transparente e menos burocrática, agilizando assim processos como o de pagamento de sinistros. Por envolver muitos agentes (nós) capazes de compartilhar informações que serão validadas através de protocolos de consenso (PoW), tal tecnologia detém o potencial de criar uma rede transparente, segura e difícil de ter seus dados alterados.

Em termos regulatórios, as seguradoras precisam então garantir que dados pessoais de clientes contidos na *blockchain* estejam em conformidade com as normas vigentes de privacidade e proteção de dados, como GDPR, na Europa, e LGDP, no Brasil.

No meio segurador, todo tratamento de dados deve ser registrado. Consultas, envio de informações de segurados para o atuário fazer análises, envio de informações para órgãos fiscalizadores, para aplicações financeiras, emissão de relatórios, imposto de renda etc.: tudo se resume a um vaivém de dados que deve ser registrado. Será um grande avanço quando alguns desses processos puderem usar a segurança e a praticidade da *blockchain*.

Como os registros civis nos cartórios – nascimento, casamento, alteração de nome, divórcio –, as informações dos segurados também ficariam registradas em ordem cronológica com essa tecnologia, deixando um histórico de referências imutáveis. Assim como algumas normas que regulam o mercado segurador e que exigem o arquivamento de dados por certo período de tempo, o uso da *blockchain* também deve se adaptar às novas regras de proteção de dados que dão ao segurado o direito de pedir a exclusão de suas informações pessoais.

Para questões de inspeção e auditoria com o uso da *blockchain*, órgãos reguladores precisariam ser integrantes das redes privadas para terem acesso aos registros das seguradoras. Outro possível obstáculo regulatório para as seguradoras e resseguradoras pode vir a ser com relação às características autoexecutáveis e irreversíveis dos contratos inteligentes. A *blockchain* sozinha também não reconhece transações boas ou ruins, legais ou ilegais, apenas trabalha na validação e armazenamento de dados.

O uso de *blockchain* privada também pode ser visto como incoerente quando se pensa na natureza descentralizada dessa tecnologia, já que faz refletir novamente sobre governança de dados. Redes privadas pequenas também podem sofrer mais facilmente um ataque bem-sucedido, uma vez que, devido ao menor número de nós (computadores) na rede, o trabalho do atacante para obter controle sobre mais de 51% destes nós e torná-los maliciosos fica mais fácil. Isso porque o fraudador teria que modificar muito rápido todos os blocos anteriores ao que ele quer fraudar, conforme explicado no Problema da Ruína do Jogador.

Em redes pequenas, o uso de outros certificados digitais de segurança é uma hipótese a ser considerada. A *blockchain* usada isoladamente, ou seja, sem criptografia, protocolos de consenso e uma rede *peer-to-peer*, perde grande parte das características que fizeram com que ganhasse sua credibilidade no mercado: descentralização, transparência e segurança.

Ainda sobre as técnicas que garantem a segurança da rede, a *blockchain* também acaba exigindo um alto custo energético para a execução do protocolo PoW, que é proporcional ao número de processadores trabalhando na validação dos blocos (mineração). No atual cenário de altos riscos ambientais devido às mudanças climáticas no mundo, novos meios de produção em potencial de CO^2 devem ser ponderados. Uma possível solução seria o uso de outros protocolos de consenso, como o *Proof of Stake*.

Tecnologias disruptivas como a *blockchain* e os contratos inteligentes também geram outros tipos de preocupações devido à rápida e contínua evolução de suas plataformas. Implementação de novos processos, treinamento de funcionários, ataques cibernéticos e a possível obsolescência/incompatibilidade precoce dessas tecnologias devem ser consideradas nos cálculos de riscos. A reestruturação de departamentos e normas em função dessas inovações tecnológicas nas empresas também tende a ser cada vez mais frequente, exigindo rápida adaptação e flexibilidade de órgãos reguladores, gestores e funcionários.

Além da necessidade de adequação das seguradoras à atual dinâmica dos processos, as tecnologias digitais demandam profissionais com conhecimentos técnicos específicos. Ao mesmo tempo que seguradoras enfrentam desafios para encontrar pessoas qualificadas para a implementação de plataformas *blockchain*, a introdução de tais modernizações nos processos contribui para o desemprego estrutural.

A regulação excessiva do setor financeiro e securitário também pode criar barreiras para pequenas empresas com grande capacidade de inovação nesse setor. Tais regras podem ter baixo custo para quem as executa, porém são potencialmente dispendiosas para quem as cumpre, sendo capazes de frear o desenvolvimento tecnológico neste setor. Diante desse cenário, o Governo Federal apresentou, em junho de 2018, as Diretrizes Gerais e o Guia de Análise de Impacto Regulatório, cujo foco preliminar está voltado para as agências reguladoras. Um dos princípios desse guia é sobre a importância de realizar uma análise de impacto logo nos estágios iniciais do processo regulatório.

Ambientes previamente regulados, como o de seguros, que não estão apropriadamente prontos para receber tecnologias disruptivas, podem fazer uma análise do impacto dessas atividades no mercado através de uma *Sandbox*. Nesse contexto, a *Sandbox* é uma adaptação do *Minimum Viable Product* – MVP e consiste em isolar um sistema oferecendo condições diferenciadas para empresas inovadoras enquanto limita a sua atuação para que não afete negativamente a economia. A *Sandbox* permite que órgãos reguladores do mercado de seguros possam tirar conclusões a respeito da melhor maneira de regular a nova dinâmica desse setor.

As seguradoras hoje vivem em dois mundos: o digital e o impresso. Como fazer a migração de todos os processos para o digital? Devemos mudar tudo nesse sentido? A *blockchain* tem a capacidade de revolucionar muitos processos em termos de consenso, segurança, governança de dados e processos regulatórios na área de seguros. Por tamanha relevância e possível impacto no modelo de negócio, o entendimento detalhado dessa tecnologia por profissionais de seguros experientes é de grande importância, para que possíveis barreiras relativas a operações e regulação sejam superadas e investimentos corretos na melhoria dos processos possam ser feitos de maneira consciente, e não especulatória. A colaboração mútua de profissionais de tecnologia da informação e de seguros pode trazer mudanças positivas, sustentáveis e robustas no mercado segurador, a um ritmo sem precedentes. Além disso, essa troca de conhecimentos é fundamental para alcançarmos a resposta sobre até que ponto as novas tecnologias devem se adequar às regras do mercado e até onde as regras do mercado devem se adaptar às novas tecnologias.

9. Referências bibliográficas

AGCS. **Allianz pioneers blockchain prototype for the captive insurance market**. 2019. Disponível em: https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/about-agcs/AGCS-ART-Captive-Blockchain.pdf. Acesso em: 25 mai. 2019.

B3I. **Industry-Led InsurTech B3i Announces Expanded Group of Investors In Its Current Funding Round**. 2019. Disponível em: https://b3i.tech/files/B3i_Content/PDF/News_and_press_releases/190403_Media_Release_B3i_Funding.pdf. Acesso em: 25 mai. 2019.

BRASIL. Fintechs e Sandbox no Brasil. **Diretrizes gerais e guia orientativo para elaboração de Análise de Impacto Regulatório-AIR**. Brasília, DF: Ministério da Economia, 2019.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm**. Acesso em: 27 mai. 2019.

DAVID, Florence Nightingale. **Games, Gods, and Gambling**: A History of Probability and Statistical Ideas. Nova York: Courier Dover Publications, 1998. p. 81-97.

EDCHAIN. POW vs. PoS: a comparison of two blockchain consensus algorithms. **Medium**. 2018. Disponível em: https://medium.com/@EdChain/pow-vs-pos-a-comparison-of-two-blockchain-consensus-algorithms-f3effdae55f5. Acesso em: 26 mai. 2019.

FITCH RATINGS. *Blockchain and Insurance: The Trust Machine (Disruptive Technology: Insurance).* **Site**. 2018. Disponível em: www.fitchratings.com. Acesso em: 26 mai. 2019.

GDPR. **Site**. [2019]. Disponível em: https://eugdpr.org/. Acesso em: 26 mai. 2019.

HOGANLOVELLS PUBLICATIONS. A look at the impact and insurance regulatory challenges of InsurTech innovations, AI, machine learning, blockchain, and smart contracts. **Hogan Lovells**. 2019. Disponível em: https://www.hoganlovells.com/en/publications/the-impact-and-insurance-regulatory-challenges-of-insurtech-innovations-ai-machine-learning-blockchain-and-smart-contracts. Acesso em: 27 mai. 2019.

HYPERLEDGER.ORG. **Site**. [2019]. Disponível em: https://www.hyperledger.org/about. Acesso em: 26 mai. 2019.

IBM. Blockchain for insurance delivers trust: a use case with Marsh, ACORD and ISN. **IBM Insurance Industry Blog**. 2018. Disponível em: https://www.ibm.com/blogs/insights-on-business/insurance/blockchain-for-insurance-delivers-trust-a-use-case-with-marsh-acord-and-isn/. Acesso em: 25 mai. 2019.

IBM. Insurance. Industries. **Site**. [2019]. Disponível em: https://www.ibm.com/blockchain/industries/insurance. Acesso em: 27 mai. 2019.

JAKOBSSON, Markus; JUELS, Ari. **Proofs of Work and Bread Pudding Protocols**. Secure Information Networks: Communications and Multimedia Security. Dordrecht: Kluwer Academic Publishers, 1999. p.58-272.

MAHLSMEISTER, Ana Luisa. Adoção de blockchain tem impacto na inadimplência. **Valor**, São Paulo, 29 mar. 2019. Disponível em: https://mobile.valor.com.br/financas/6187457/adocao-de-blockchain-tem-impacto-na-inadimplencia. Acesso em: 14 jun. 2019.

MOREIRA, Fernando; BORTOLOTTI, Silvana; COELHO, Antônio. **Considerações sobre a ruína do jogador**. Disponível em: http://www2.ime.unicamp.br/sinape/sites/default/files/Artigo_SINAPE_Ru%C3%ADna%20do%20Jogador.pdf. Acesso em: 27 mai. 2019.

NAKAMOTO, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 27 mai. 2019.

OECD. Insurance spending (indicator). **Site**. 2019. Disponível em: https://data.oecd.org. Acesso em: 20 mai. 2019.

ORACLE. **Site**. 2019.Disponível em: https://www.oracle.com/. Acesso em: 20 mai. 2019.

ORACLE. Oracle Cloud. Blockchain Technology for the Enterprise. Disponível em: https://www.oracle.com/a/ocom/docs/cloud/cloud-essentials-blockchain-for-the-enterprise.pdf. Acesso em: 24 mai. 2019.

PAL NETWORK TEAM. **Introducing FlightPAL: Two-in-One Flight Protection**. Medium. 2019. Disponível em: https://medium.com/pal-network/introducing-flightpal-two-in-one-flight-protection-b7d2f678c2b4. Acesso em: 24 mai. 2019.

STEVENS, M.M.J. **On Collisions for MD5**. 2007. Disponível em: https://www.win.tue.nl/hashclash/On%20Collisions%20for%20MD5%20-%20M.M.J.%20Stevens.pdf. Acesso em: 24 mai. 2019.

TEMPLE, James. Bitcoin mining may be pumping out as much CO_2 per year as Kansas City. **MIT Technology Review**. 2019. Disponível em: https://www.technologyreview.com/s/613658/bitcoin-mining-may-be-pumping-out-as-much-cosub2-sub-per-year-as-kansas-city/. Acesso em: 12 jun. 2019.

THE LINUX FOUNDATION. Inaugural Hyperledger Global Forum Showcases Strong Community Momentum. **Site**. 2018. Disponível em: https://www.linuxfoundation.org/press-release/2018/12/inaugural-hyperledger-global-forum-showcases-strong-community-momentum/. Acesso em: 25 mai. 2019.

UNITED NATIONS. Annual Urban Population at Mid-Year by region, subregion and country, 1950-2050 (thousands). World Urbanization Prospects: The 2018 Revision. **Site**. Disponível em: https://population.un.org/wup/Download/. Acesso em: 25 mai. 2019.