Oportunidades do Mercado de Seguros Global

Blockchain: Mecânica e Mágica

Por Stephen J. Mildenhall

Sobre o Relatório GIMO

Desde seu lançamento em setembro de 2015, o relatório Oportunidades do Mercado de Seguros Global (GIMO - *Global Insurance Market Opportunities*) tornou-se rapidamente um importante estudo de referência para o setor de seguros. Para 2018, adotamos uma nova forma de divulgação, publicando artigos da série Oportunidades do Mercado de Seguros Global ao longo do ano, ao invés de lançar um relatório único e abrangente. Esta abordagem de divulgação visa aumentar a utilização do conteúdo incluindo nossos insights no mercado o quanto antes, para promover o desenvolvimento com os nossos clientes e parceiros de (re)seguros e facilitar aos leitores do GIMO a absorção da riqueza de conteúdos gerados anualmente.

O *Blockchain* cura todos os males. É um banco de dados imutável (inalterável) e não "hackeável". Reduz os custos de transação, permite a confiança entre estranhos e nos liberta do controle de uma instituição de autoridade. O Blockchain revolucionará o mercado de seguros: executivos do mundo todo devem estar atentos. O Blockchain é o novo "plástico". Pelo menos é o que dizem por aí.

Vários artigos explicam como o uso de um blockchain reduz os custos, aumenta a rentabilidade e produz uma clara vantagem competitiva para as seguradoras. Poucos artigos tratam da mecânica e mágica do blockchain – sim, mágica! É necessário que os executivos tenham uma compreensão básica da mecânica e apreciem a mágica dessa tecnologia para avaliar a aplicabilidade dos blockchains nos problemas que permeiam o setor de seguros. Neste artigo, explicaremos como funciona um blockchain sem nos apegarmos aos atuais equívocos sobre o assunto. Vamos destacar algumas capacidades surpreendentes e desmistificar alguns mitos e incoerências.

É necessário que os executivos tenham uma compreensão básica da mecânica e apreciem a mágica dessa tecnologia para avaliar a aplicabilidade dos blockchains nos problemas que permeiam o setor de seguros.

O Blockchain é um Banco de Dados

Um Blockchain é um **banco de dados**. Os bancos de dados em blockchain geralmente são **distribuídos**, ou seja, armazenados em várias máquinas, e não por uma única autoridade.

O blockchain armazena registros que podem ser considerados como transações, pois possui uma ordem temporal: as transações posteriores podem depender das anteriores. A importância dos bancos de dados transacionais para o seguro é óbvia.

Registros individuais são armazenados em **blocos encadeados** através de um índice, daí o nome "blockchain" (cadeia de blocos, em tradução literal). Os dados em cada bloco são chamados de "payload". O payload pode ser um conjunto de dados estruturados, como detalhes de uma transação financeira ou uma apólice de seguro, ou dados desestruturados, como uma imagem, vídeo ou arquivo PDF de um contrato de seguro. Para cada bloco, atribui-se um índice para localização. (Bancos de dados SQL funcionam dessa maneira. Mesmo que os dados sejam apresentados como uma tabela, são armazenados em blocos indexados.) A cadeia surge incluindo o índice do bloco anterior como parte do payload de dados em cada bloco. O encadeamento reforça a ordem temporal do banco de dados. Dado o índice do último bloco, um usuário pode extrair uma lista ordenada de blocos do banco de dados seguindo a cadeia de índices.

> Os usuários do banco de dados possuem três preocupações: os dados possuem **integridade**, **validade** e **segurança**? Os blockchains oferecem soluções inovadoras para esses três aspectos.

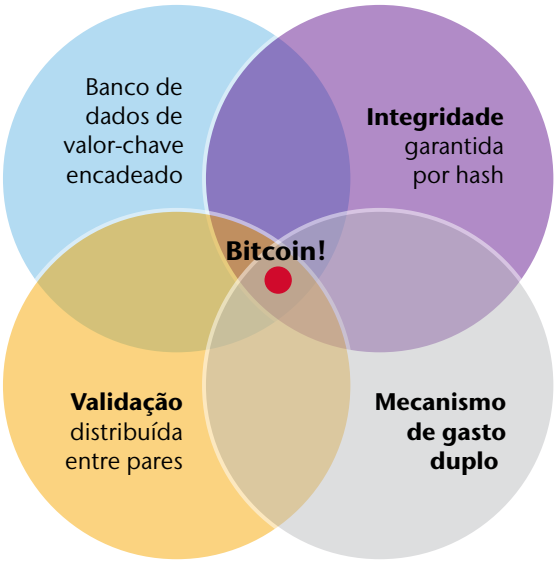
Usuários de bancos de dados possuem três preocupações: os dados possuem **integridade**, **validade** e **segurança**? Os blockchains oferecem soluções inovadoras para esses três aspectos.

Integridade e Hash

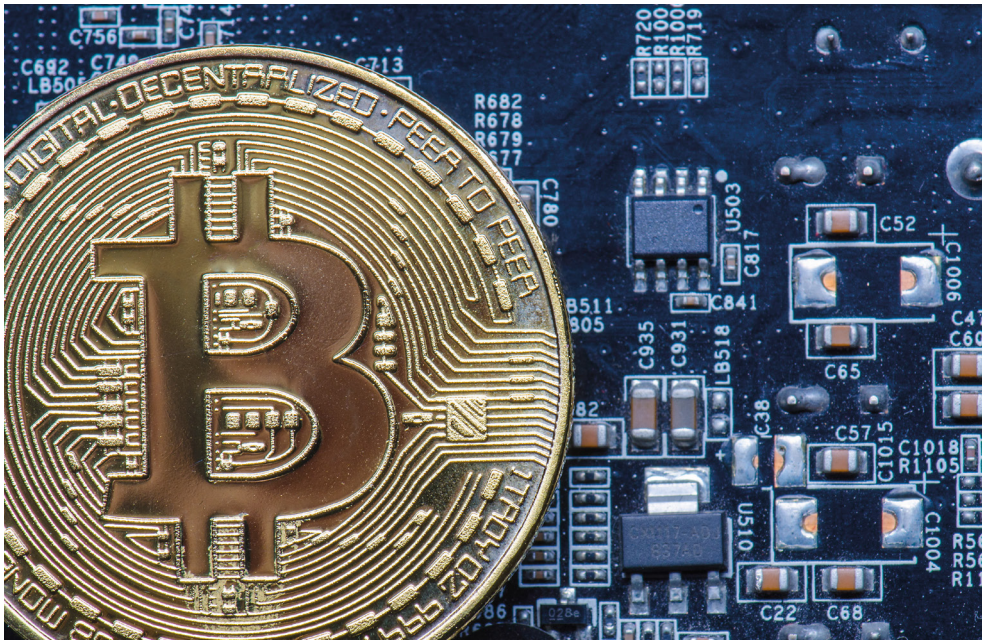
Um extrato de um banco de dados corresponde fielmente ao original? Isto é, possui **integridade**? Os *blockchains* usam funções *hash*, uma construção matemática mágica para garantir a integridade do banco de dados.

Uma função *hash* é um algoritmo determinístico que reduzirá uma entrada de comprimento arbitrário (ex., os dados em um bloco) para uma saída de comprimento fixo. Um exemplo comum de uma função *hash* é encadear as primeiras cinco letras do seu sobrenome (preenchidas, se necessário) e a primeira letra do seu primeiro nome; um dos *hashes* favoritos das equipes de TI para criar nomes de usuário. No entanto, como todos sabemos, este hash tem um problema: muitos nomes diferentes podem ser mapeados a um mesmo hash, gerando uma colisão de hash. Este é o nosso primeiro ingrediente mágico: existem funções de hash com probabilidade de **colisão** extremamente baixa. Dadas duas entradas diferentes, a probabilidade de o hash produzir a mesma saída é insignificante, não como um em cem, mas como probabilidade de colisão dentro de um bilhão de mensagens menor que a probabilidade de selecionar um átomo específico no universo. O algoritmo SHA256 é um exemplo dessa função hash. Ele produz uma saída hexadecimal de 64 dígitos, equivalente a um número decimal de 77 dígitos.

Como um blockchain usa a função hash SHA256 para garantir a integridade? É incrivelmente simples. Ele utiliza o hash do payload do bloco como o índice. Lembre-se que payload inclui o índice do bloco anterior, assim como quaisquer dados armazenados no bloco. A verificação da integridade do download de dados do banco de dados é simples: basta gerar o hash do payload e comparar a resposta com o índice do bloco. Se os dois combinam, você pode ter a certeza (não total, mas o suficiente) que seu extrato corresponde ao original, ou seja, sua cópia tem integridade. Sabendo o índice de hash do cartão mais recente do banco de dados, é possível determinar a integridade de uma cópia do banco de dados inteiro, calculando os hashes repetidamente. Um número decimal de 77 dígitos é suficiente para determinar se uma cópia de todo o blockchain de um bitcoin, 184 gigabytes, possui integridade!



O Bitcoin combina quatro funções separadas com mágica.



Validade e Nonces

A integridade do banco de dados é importante, mas uma cópia exata de dados inválidos é inútil. Os usuários também se preocupam com relação à validade de seus dados: que sejam legalmente ou oficialmente vinculantes e aceitáveis.
A validade dos dados geralmente é aplicada por uma autoridade confiável, como um banco, um empregador, uma seguradora ou agência governamental. A segunda capacidade mágica de um blockchain é permitir a validade sem uma autoridade: permitir a validação distribuída de novos registros de banco de dados.

Dado um blockchain, é fácil fazer uma cópia inválida com integridade: basta alterar um bloco, por exemplo, para creditar sua conta bancária e, em seguida, recalcular todos os hashes de índice de bloqueio.
A função SHA256 é muito rápida de avaliar e, por isso, é uma alteração rápida e fácil. Agora existem duas cópias diferentes do banco de dados com integridade. Mas qual é a cópia válida?

A validade é um problema adicional: dada uma cópia do banco de dados a qual todos os usuários concordam ser válida, como o próximo bloco de transações deve ser confirmado e anexado?
O novo bloco precisa ser coerente com as transações existentes e, em seguida, "bloqueado" de alguma forma e, assim, torna-se **imutável** ou, no mínimo, muito difícil de ser alterado.

A rede Bitcoin reforça a validade através de um mecanismo de consenso Prova de Trabalho (***Proof-of-Work***). O processo tem várias etapas. Primeiro, o chamado "minerador" verifica as novas transações para garantir que sejam válidas, consultando o registro de quem possui o quê no banco de dados existente.
Este estágio evita gastos duplos, pois o minerador permite que um Bitcoin seja gasto apenas uma vez. O minerador sabe que outros verificarão o trabalho de forma independente, assim a fraude será detectada e a sua mineração será em vão.
Em seguida, o minerador combina um número de transações válidas em um payload de bloco.
Em terceiro lugar, o minerador calcula o índice de hash do bloco. Isso é feito gerando um hash do payload encadeado com um número adicional, chamado **nonce** (do inglês, ***n****umber used* ***once***, ou "número usado uma vez"). O nonce é selecionado de modo que o hash resultante seja menor que determinado limite (a dificuldade do bloco). Os mineradores de Bitcoin tentam encontrar esses nonces por força bruta, testando diferentes nonces até encontrar um que produza um hash pequeno o suficiente. O processo de mineração por força bruta consome uma enorme quantidade de eletricidade — outro fato comum nas informações da imprensa sobre o Bitcoin!
Quarto, o bloco proposto é transmitido para outros usuários. Se concordarem que é válido, pode ser adicionado à cadeia e o processo recomeça. Após receber o nonce, a verificação da validade de um bloco ocorre rapidamente. Os mineradores são recompensados com Bitcoins recém-criados para seus esforços de mineração.

Por que esse processo cria um registro (quase) imutável? Suponha que eu queira mudar um bloco antigo. É possível fazê-lo, mas leva tempo, o tempo para encontrar o nonce para cada bloco a ser alterado. Conforme esse tempo passa, novos blocos são criados. A menos que eu controle a maior parte do poder de computação para mineração (ou 51% de ataque), nunca conseguirei alcançar o bloco atual. Assim, é praticamente impossível voltar e alterar o blockchain.

Segurança e Encriptação

Um banco de dados distribuído, onde todos têm acesso aos registros subjacentes, parece não comportar boa segurança. Os blockchains utilizam criptografia para garantir a segurança. Os payloads de dados em cada bloco são públicos, porém criptografados. Sem uma chave emitida pelo proprietário dos dados, é impossível (novamente, não matematicamente impossível, mas quase impossível) extrair a informação subjacente. Mediante a suposta segurança de um blockchain, por que há tantos relatos de ataques de hackers e roubos de Bitcoin? A criptografia é um bloqueio inquebrável, mas todos os bloqueios possuem uma chave.

Mediante a suposta segurança de um blockchain, por que há tantos relatos de ataques de hackers e roubos de Bitcoin? A criptografia é um bloqueio inquebrável, mas todos os bloqueios possuem uma chave.

Para o Bitcoin, a chave é um simples número. E este número deve ser armazenado. Roubando esse número, controla-se o Bitcoin. Todos os casos de hacks de blockchain relatados envolvem o roubo de chaves, não uma violação da criptografia subjacente. Se os indivíduos tiverem suas próprias chaves e não houver bancos de dados extensivos de chaves expostas a hackers, as violações de dados em massa não poderão ocorrer; a segurança foi distribuída.

A tecnologia de segurança criptografada oferece algumas possibilidades mágicas. É possível emitir chaves de segurança com um único acesso aos dados: chaves que expiram. Por exemplo, para conceder acesso a terceiros para verificar meu registro de crédito utilizando um serviço de crédito em blockchain, seria emitida uma chave única de leitura. A parte interessada acessaria meu registro em um determinado momento, mas não conseguiria usar a mesma chave duas vezes. Hoje, obviamente, ainda é necessário revelar o número de CPF e outras informações confidenciais e confiar que o destinatário verificará o registro do indivíduo apenas uma vez. Há um enorme potencial de uso da tecnologia blockchain para devolver a propriedade e o controle de informações privadas aos indivíduos.

Aplicações

Comentaristas frequentemente promovem os blockchains como uma solução para o processamento de dados na indústria de seguros e ineficiências administrativas. Mas esta é uma visão muito limitada, em que o verdadeiro potencial para as seguradoras se perde completamente.

A internet, que forneceu acesso livre a uma série de informações, criou, paradoxalmente, um vácuo de confiança. Supostas instâncias de hackeamento eleitoral destacam a necessidade de verificação de identidade. O ataque cibernético à Equifax, nos EUA, revela as fraquezas dos repositórios de informações privadas de controle centralizado. A tecnologia Blockchain nos permite redemocratizar os dados e reafirmar o controle do indivíduo sobre seus dados privados. Para isso, será necessária uma infraestrutura e um modelo de receita alternativa. As seguradoras estão preparadas para fornecer esses serviços e lucrar com o **vácuo de confiança**, substituindo redes centralizadas ultrapassadas e inseguras por soluções de blockchain distribuídas. Esse modelo revolucionário representa o verdadeiro potencial do blockchain para o setor.

As seguradoras estão preparadas para fornecer esses serviços e lucrar com o vácuo de confiança, substituindo redes centralizadas ultrapassadas e inseguras por soluções de blockchain distribuídas.

Sobre o Autor:

Stephen Mildenhall é professor assistente na Escola de Gestão de Risco, Seguros e Ciências Atuariais da Universidade St. John, em Nova York. Anteriormente, foi CEO Global da Analytics da Aon plc, com sede em Singapura, e chefe da Aon Benfield Analytics. Durante sua carreira, Stephen adquiriu ampla experiência no setor global de seguros.

Sobre a Aon

A Aon Plc (NYSE: AON) é uma empresa global líder de serviços profissionais, que oferece ampla gama de soluções em riscos, previdência e saúde. Globalmente, nossos 50 mil colegas, em 120 países, potencializam resultados para clientes utilizando dados e análises proprietários para fornecer perspectivas inovadoras, que reduzam a volatilidade e melhorem o desempenho. Possuímos cinco linhas de soluções globais específicas: Soluções para Riscos Comerciais, Soluções para Resseguros, Soluções em Previdência, Soluções em Saúde e Serviços em Dados e Análises.

www.aon.com

GDM06967

Empower Results®