Decifrando o blockchain

Ferramenta criada para dar suporte ao comércio de criptomoedas hoje é usada em uma série de outras aplicações

Gigante global na área de logística marinha, a multinacional dinamarquesa Maersk descobriu há alguns anos que uma remessa de produtos refrigerados da África para a Europa poderia passar por quase 30 pessoas e organizações, totalizando mais de 200 diferentes interações entre os parceiros comerciais. Os custos associados ao processamento e à administração da documentação, calculou a empresa, equivaliam a até um quinto do valor do transporte em si. Para simplificar esse processo, reduzir gastos e diminuir o tempo de entrega das mercadorias, a Maersk decidiu recorrer a uma nova tecnologia, conhecida como blockchain.

Traduzido livremente por corrente de blocos, o blockchain funciona como um livro de registro digital, em que os dados são armazenados de forma descentralizada por cada um dos agentes da transação em questão. Protegidas por mecanismos de criptografia, as informações colocadas no sistema são, em tese, invioláveis e à prova de fraude. A segurança da rede também se dá pelo fato de os dados não estarem centralizados em um servidor único, mas dispersos por um grupo de computadores independentes que fazem parte da rede, dificultando a ação de hackers. As informações sobre as operações são inseridas no *ledger*, espécie de livro de contabilidade digital, formando uma cadeia sequencial de blocos, no qual cada um se liga ao anterior, recuperando suas informações e, ao mesmo tempo, agregando novos dados à cadeia (*ver infográ-*

Como funciona

O segredo do blockchain está no *hash*, uma impressão digital que garante a autenticidade e a inviolabilidade dos dados

1

CONTABILIDADE DIGITAL

Os blocos com informações sobre as transações de compra e venda, como de bitcoins (identificação do vendedor e do comprador, valor da transação etc.), são inseridos em uma espécie de livro de contabilidade digital chamado *ledger*

2

RECUPERAÇÃO DE INFORMAÇÕES

Quando um participante A vende um bitcoin para o participante B, é criado um bloco com o registro dessa operação. Se essa moeda for posteriormente vendida por B para um participante C, os dados da nova venda são inseridos em um novo bloco, ampliando o número de registros no *ledger*

3

PROTEÇÃO CONTRA HACKERS

A segurança das informações é garantida pela função *hash*, uma impressão digital intrínseca a cada bloco, que funciona para identificá-lo e para impedir alterações no seu conteúdo. Se os dados do bloco forem alterados, o *hash* muda e denuncia a violação

4

VALIDAÇÃO DAS TRANSAÇÕES

Quem garante que as novas informações inseridas na cadeia são válidas são os mineradores, pessoas ou empresas que usam computadores com grande poder de processamento para autenticar cada passo da transação. Isso é feito por meio da resolução de cálculos complexos, definidos pela própria rede

fico acima). Rastreabilidade, segurança e imutabilidade dos dados são aspectos centrais da ferramenta.

A tecnologia surgiu em 2008 para apoiar a comercialização do bitcoin, a primeira moeda digital ou criptomoeda. Cercada de mistério, sua origem é creditada a Satoshi Nakamoto, o mesmo criador do bitcoin, mas não há informações seguras sobre quem é essa pessoa nem seu país de origem. Há quem aposte, inclusive, que Nakamoto não é um indivíduo, mas um grupo de programadores.

Nos últimos anos, o uso da ferramenta expandiu-se e hoje ela é empregada no registro de operações bancárias, na gestão de documentos corporativos, no rastreamento da cadeia produtiva de alimentos e no transporte de mercadorias, como no caso da Maersk. Em conjunto com a IBM, a multinacional dinamarquesa acabou lançando, dois anos atrás, uma plataforma digital baseada no mecanismo, a Tradelens, que já contabiliza dezenas de membros, entre transportadoras, portos e autoridades alfandegárias.

"O blockchain serve para ordenar eventos em um sistema totalmente descentralizado, do qual participam pessoas que não se conhecem nem confiam umas nas outras, e quando é preciso saber a ordem em que esses eventos aconteceram", diz o especialista em segurança da informação Marcos Antônio Simplício Júnior, professor da Escola Politécnica da Universidade de São Paulo (Poli-USP). "Em um cenário de transações financeiras, o blockchain pode ser usado quando não há uma entidade dentro desse sistema responsável por ordenar eventos, como faz um banco nas operações entre seus correntistas."

É o que acontece, por exemplo, no caso do bitcoin, em que as operações de compra e venda de moedas ocorrem de forma descentralizada, sem um banco intermediando ou controlando as transações (*ver box na página 74*). Isso é feito pelos próprios participantes do sistema. A segurança das operações baseia-se na função *hash*, espécie de impressão digital que identifica cada bloco pertencente à cadeia e garante a inviolabilidade dos dados. Se houver uma tentativa de alterar as informações do bloco, o *hash* muda e denuncia a mudança.

Mas fica a indagação: como ninguém se conhece na rede, quem seria o ator

INFOGRÁFICO ANA PAULA CAMPOS **ILUSTRAÇÃO** FABIO OTUBO

confiável para dizer que o próximo bloco da cadeia a ser inserido no *ledger* é o correto? Isso foi resolvido por meio da criação dos chamados mineradores, usuários – comumente, empresas – dotados de poder computacional responsáveis por validar, a partir de cálculos complexos, os blocos a serem inseridos no *ledger*. Os registros de todas as transações da cadeia ficam armazenados nos computadores dos mineradores, que funcionam como auditores do processo. "Qualquer entidade capaz de processar dados computacionais pode se candidatar e participar de uma rede de blockchain como mineradora. No comércio de bitcoins, elas são remuneradas em criptomoedas", explica Marcos Simplício.

Ele esclarece que, além das redes públicas de blockchain, como as utilizadas no comércio de criptomoedas, que não têm um controlador e cuja participação é franqueada a qualquer interessado (os compradores e os vendedores das moedas digitais), também existem as redes privadas, criadas por empresas que desejam fazer uso da ferramenta – é o caso, por exemplo, do blockchain criado pela IBM e Maersk. "O que diferencia uma da outra", explica o professor da USP, "é que as redes privadas contam necessariamente com uma entidade permissionária, normalmente a organização que a criou. Ela é responsável por definir quem pode participar do sistema". Frequentemente, esse ente permissionário também faz a validação das informações inseridas na cadeia de blocos, dispensando ou complementando o trabalho dos mineradores.

Há no mercado softwares abertos que podem ser empregados para criar redes privadas de blockchain

Uma das empresas que mais investe nessa tecnologia é a IBM, especializada na criação de sistemas privados de blockchain para diferentes aplicações – também há no mercado softwares abertos, como MultiChain e HyperLedger, que podem ser usados por quem queira criar redes para seus negócios. "Temos mais de 300 produtos rastreados e mais de 3 milhões de operações realizadas em blockchain na cadeia de alimentos de vários países", diz o cientista da computação Percival Lucena, responsável por projetos em blockchain no Laboratório de Pesquisas da IBM em São Paulo.

A rede de supermercados Walmart é um dos parceiros da IBM. Ela utiliza o sistema Food Trust para gerir sua cadeia de suprimentos nos Estados Unidos. Em caso de produtos contaminados, é possível saber exatamente de que região eles vieram, por onde passaram e onde estão sendo vendidos. Nos primeiros testes da tecnologia, o Walmart reduziu de sete dias para cerca de dois segundos o tempo de rastreamento dos produtos.

No Brasil, a IBM aplicou o Food Trust em um projeto-piloto com a fabricante de alimentos BRF e o Carrefour com o intuito de informar aos consumidores a procedência dos alimentos. O sistema foi testado em 2017, quando unidades do supermercado receberam um lote de uma linha de lombos congelados da BRF e cujas embalagens continham um QR Code (código de barras bidimensional). O código dá acesso a informações detalhadas sobre a mercadoria, como o nome do fabricante, a data de produção e os dados do transporte do local de origem ao de venda. O projeto evoluiu e uma nova versão do Food Trust está sendo testada no país. A IBM também desenvolveu uma solução de blockchain para exportadores de produtos agrícolas, a rede AgTrace, em teste no país com alimentos orgânicos e produtores de café.

Sediada em São Paulo, a startup Compplied Computação Aplicada também investe em aplicações de blockchain para uso no campo. Uma de suas soluções, chamada de Corrente, é voltada para rastreabilidade de transações financeiras no setor agrícola. "Nosso foco foi otimizar processos já existentes, adotando um modelo de blockchain que valida as transações, de modo a agilizar e diminuir incertezas", explica o cientista da computação David Kwast, pesquisador da Compplied responsável pelo projeto.

Documentos como notas fiscais, conhecimentos de transporte e laudos fitossanitários e de qualidade do produto já são elaborados pelos integrantes da

O comércio de criptomoedas

As negociações desses ativos digitais não são regulamentadas e implicam risco elevado

Ao contrário do dinheiro convencional, emitido em papel ou cunhado em forma de moeda, as criptomoedas, como bitcoin, litecoin ou binance coin, não existem fisicamente – são arquivos digitais. Elas são um ativo financeiro muito similar às ações negociadas em bolsas de valores, com a diferença que as transações de compra e venda não passam por uma instituição reguladora, como o Banco Central, mas são feitas diretamente entre quem detém a moeda e quem pretende adquiri-la.

Para operar nesse mercado, os interessados devem criar uma carteira virtual. Para isso, é necessário abrir uma conta numa corretora de criptomoedas. A partir daí, todas as transações são feitas entre os interessados usando como plataforma o blockchain, ferramenta que valida e registra as transações financeiras.

Desde seu lançamento, o valor do bitcoin, principal criptomoeda, sofreu forte oscilação e em março de 2019 estava valendo por volta de R$ 16 mil – em dezembro de 2017 atingiu seu pico, R$ 64 mil. A cotação das criptomoedas oscila com base na oferta e na demanda, a exemplo do que ocorre no mercado acionário. Por não ser um setor regulamentado, as transações são consideradas de alto risco.

Plantio de café no interior de São Paulo: blockchain pode facilitar negociação da produção agrícola

cadeia em sua rotina. Com o blockchain, eles se transformam em dados digitais invioláveis e se tornam visíveis para todos os participantes. Para o engenheiro de software José Ricardo de Oliveira Damico, um dos fundadores da Compplied, a adoção do Corrente pode tornar mais ágil o processo de aquisição de crédito e seguro nos bancos. "O blockchain facilita a negociação da produção agrícola, já que os compradores querem ter certeza de que o agricultor terá recursos para produzir naquela safra, sob as condições contratadas", afirma o engenheiro.

Apoiada pelo programa Pesquisa Inovativa em Pequenas Empresas (Pipe), da FAPESP, a empresa criou uma funcionalidade no Corrente que permite aos participantes da rede operar off-line, o que, em princípio, quebraria a lógica do blockchain, que é ordenar as operações em tempo real conforme a sequência em que são realizadas. Isso é relevante porque nem sempre os produtores rurais podem se conectar à internet imediatamente para lançar seus dados. Ainda em curso, o projeto deve ser concluído este ano.

Apesar de a tecnologia blockchain estar ganhando terreno, alguns desafios ainda não foram superados. "Preocupa o elevado gasto de energia do processo", destaca o engenheiro da computação Lucas Lago, do Centro de Estudos Sociedade e Tecnologia da USP (Cest-USP). O site Digiconomist criou uma metodologia para estimar o consumo de energia dos mineradores no mundo. Em março, o sistema calculava que a rede bitcoin exigia pelo menos 44 terawatts-hora por ano (TWh), equivalente ao consumo de um país como o Peru. Segundo Lago, há iniciativas para solucionar esse problema, como mudanças no algoritmo do blockchain, mas esse ainda é um obstáculo a ser superado. Um problema local, de acordo com o especialista, são as poucas iniciativas em formação de recursos humanos para trabalhar com a tecnologia.

DIREITO AO ESQUECIMENTO

O professor Marcos Simplício, da Poli-USP, usa um clichê para definir o blockchain: muitas vezes, é uma solução em busca de um problema a ser resolvido. "De 10 coisas que ouço falar sobre aplicações do blockchain, nove não fazem muito sentido", sustenta. Para ele, várias redes privadas de blockchain não têm razão de ser, pois existe nelas algum laço de confiança entre os participantes, que necessariamente se conhecem. "Nesses casos, bastariam assinaturas digitais sobre os eventos ou um sistema de arquivos distribuído para a consulta de todas as transações, dispensando-se o custoso processo de mineração", afirma.

Simplício aponta ainda que, nas redes privadas, a decisão sobre a validade dos blocos é muitas vezes concentrada em uma ou em um grupo de empresas, corrompendo o espírito original do blockchain, que é a inexistência de uma instituição centralizadora. Além disso, a tecnologia não necessariamente dispensa a fiscalização humana. "Não é possível ter certeza de que uma caixa de flores contém, de fato, o produto, a não ser que uma entidade, como, por exemplo, um fiscal confiável, abra a caixa, confira e registre essa conferência no blockchain, criando um 'registro digital' válido de um produto real", afirma o professor da Poli-USP.

Outra questão que preocupa usuários e desenvolvedores da ferramenta são as novas regulamentações para proteção de dados, como a europeia General Data Privacy Regulation (GDPR) e a brasileira Lei Geral de Proteção de Dados. Entre outras medidas, elas estabelecem o direito ao esquecimento – o direito que qualquer pessoa tem de que fatos relacionados à sua vida privada não sejam expostos ao público na internet ou em outro meio qualquer. Com o blockchain, não se sabe como isso se dará na prática, uma vez que as informações contidas no sistema não podem ser alteradas. ■

Projeto

Desenvolvimento de sistema em blockchain para o rastreamento e intermediação de operações e transações agrícolas (nº 17/01037-6); **Modalidade** Pesquisa Inovativa em Pequenas Empresas (Pipe); **Pesquisador responsável** José Ricardo de Oliveira Damico (Compplied); **Investimento** R$ 81.981,91.

FOTO LÉO RAMOS CHAVES ILUSTRAÇÃO FABIO OTUBO