Centro de Estudos Sociedade e Tecnologia
Universidade de São Paulo
Boletim - Volume 2, Número 4, Outubro/2017

Blockchain: confiança através de algoritmos

Lucas Lago

Muitas pessoas provavelmente já leram ou ouviram falar de Bitcoin, a principal criptomoeda entre outras, como o Ethereum, Litecoin e Nxt. Porém nem todos ouviram falar de *blockchain*, tecnologia proposta em 1991, mas que ganhou fama juntamente com o conceito dessa moeda em 2008, e foi fundamental para o seu sucesso; já que a tecnologia não é tão retratada na mídia não-especializada quanto as criptomoedas.

Enquanto a moeda digital ganhava notoriedade, principalmente pela evolução do seu valor em relação ao dólar, a *blockchain* ganhou diversas implementações, demonstrando a flexibilidade dessa tecnologia. Ele foi desenvolvido a partir da necessidade de se manter um registro íntegro de todas as transações realizadas no mercado de Bitcoin.

Diversos problemas tanto na esfera pública quanto privada podem ser solucionados com implementações baseadas em blockchain.

Para isso, a *blockchain* foi desenvolvido como um livro-razão para o Bitcoin, registrando as últimas transações realizadas num processo que pode ser resumido nos seguintes passos:

1. Todas as transações realizadas nos últimos minutos são agrupadas em um único bloco;
2. Esse único bloco é distribuído por toda a rede da *blockchain*;
3. Usuários da rede com computadores utilizam algoritmos para validar um bloco, e recebem recompensas a cada sucesso. Esses usuários são chamados de mineradores;
4. O bloco validado recebe uma marcação temporal e é adicionado no final da lista.

Como todas as transações são mantidas públicas, qualquer transação pode ter sua origem traçada até o momento em que foi inserida, garantindo a transparência do processo. A natureza aberta e descentralizada da *blockchain* é utilizada para fornecer confiança às transações, eliminando a necessidade de instituições intermediárias.

Para garantir a integridade de um bloco a tecnologia *blockchain* recorre a uma técnica matemática conhecida como *hash criptográfico*: uma função *hash* simples transforma dados de comprimento variável em dados de comprimento fixo; já a função *hash* criptográfica faz isso de forma unidirecional. O poder de processamento necessário para reverter uma função *hash* e encontrar detalhes da informação original é muito superior ao poder de processamento necessário para criar a *hash*.

Uma função *hash* pode transformar qualquer informação em uma lista de letras e números que aparenta ser aleatória. Cada novo bloco da blockchain utiliza as informações de índice do bloco, hash do bloco anterior, dados do bloco, data e hora, e um número chamado de "*nonce*" como entrada para a sua função hash.

Caso o *hash* gerado por essa entrada seja válido o bloco é aceito como válido e transmitido para todos os membros da rede distribuída; caso o *hash* não seja válido, o número "*nonce*" é alterado por um novo valor. Esse processo é repetido até que um número "*nonce*" capaz de validar o bloco seja encontrado. Esse processo é chamado de mineração de bloco.

Como para cada bloco é utilizado o que seria a assinatura do bloco anterior para criar a assinatura do bloco atual, não seremos capazes de criar blocos que não estejam na mesma cadeia.

Uma característica importante nas funções de *hash* é que existirão poucas saídas diferentes que geram assinaturas idênticas. Com isso, a partir do momento que um bloco é validado, é extremamente custoso criar um segundo bloco com alguma modificação que também seja válido. Com essa garantia, a cadeia acaba se tornando praticamente imutável. A imutabilidade dessa cadeia acaba permitindo aplicações digitais, onde antes isso era impensável, pela necessidade de registros não manipuláveis.

Diversos problemas tanto na esfera pública quanto privada podem ser solucionados com implementações baseadas em *blockchain*, pois esta tecnologia pode mudar desde o modo como realizamos contratos até a forma como nossas informações de saúde são armazenadas.

Na indústria fonográfica, por exemplo, artistas como Imogen Heap estão criando seu próprio ambiente baseado em *blockchain:* o Mycelia. A ideia da artista é criar um ambiente que, além de permitir que músicos tenham mais controle sobre as suas músicas, eles sejam capazes de receber honorários sem a interferência de intermediários.

No âmbito governamental, também existem exemplos do desenvolvimento de *blockchains* para diversas soluções; a Suécia e a Estônia, por exemplo, possuem usos de *blockchains* para finalidades bem diferentes.

Desde junho de 2016, a Suécia vem elaborando um registro de imóveis baseado em um banco de dados. A ideia é que a *blockchain* seja mantido pela autoridade de registros sueca, a *Lantmäteriet*, sendo replicado em bancos, imobiliárias interessadas, compradores e vendedores, de forma que todas as informações sejam mantidas de forma acessível e segura para todos os envolvidos em uma transação imobiliária. A solução sueca ainda está em fase de testes. Porém, com a expectativas de economia na casa da centena de milhões de dólares essa tecnologia deve estar funcionando em breve.

A Estônia, que tem como bandeira a implementação de tecnologias digitais no país, possui um projeto para utilizar a tecnologia *blockchain* em seu sistema de saúde. Os dados de saúde dos cidadãos da Estônia já são tratados de forma online, mas ainda, não em uma plataforma distribuída como o novo projeto pode permitir. Caso tenha sucesso, essa nova implantação permitirá que médicos e pacientes tenham acesso às suas informações de saúde de forma segura e privada, além de as informações permanecerem armazenadas por tempo indeterminado na *blockchain*.

Com a tecnologia implementada atualmente, há a necessidade de se confiar em certas instituições para garantir que determinadas informações estejam corretas: cartórios de registro civil garantem o fato de que casamentos realmente aconteceram; cartórios de registro de imóveis garantem a posse de imóveis pelas pessoas. Esses registros estão em papel, em livros que "garantem" a impossibilidade de serem manipulados.

Sempre existiu o medo de que em um futuro *orwelliano* esses dados pudessem ser alterados ou manipulados pelos detentores do poder, antes mesmo do advento do armazenamento de dados em mídias digitais – que de certa forma facilitam a edição e substituição de informações. Com a migração dessas informações para *blockchains* existirá maior segurança de que pessoas, como Winston Smith, terão bastante dificuldade para manipular informações importantes, sem a perda das vantagens de velocidade e eficiência trazidas pelo armazenamento de informações em meio digital.

Lucas Lago *é doutorando em Engenharia de Computação na Escola Politécnica da Universidade de São Paulo e pesquisador do CEST-USP.*

Coordenador: Edison Spina

Este artigo resulta do trabalho de apuração e análise do autor, não refletindo obrigatoriamente a opinião do CEST.