Introdução

Em 2009, um sistema de criptomoeda ou moeda virtual chamado Bitcoin foi lançado e, desde então, vem representando uma grande revolução nos meios de pagamentos digitais. O principal ingrediente do êxito do Bitcoin é um sistema de registro que ficou um bom tempo sem ser notado: o **blockchain.**

Então o que é blockchain?

O blockchain é um livro digital incorruptível de transações econômicas que pode ser programado para registrar não apenas as transações financeiras, mas praticamente tudo de valor

O blockchain também pode ser usado em outros sistemas, dos mais diversos tipos e com diversas possibilidades.

Bitcoin

Antes de entrar no universo do blockchain, vale a pena entender o que é **Bitcoin**. Assim fica mais fácil compreender a importância e o funcionamento do blockchain.

o Bitcoin é uma moeda totalmente digital, de alcance global e que não é controlada por governos ou instituições. Não há banco central, casa da moeda ou fundos monetários privados, enfim, não há nenhuma entidade por trás da plataforma do Bitcoin.

Estamos falando de um sistema, com modo de operação distribuído sem um elemento central e autorregulado. Tudo se baseia em transações digitais criptografadas, razão pela qual o Bitcoin é considerado um tipo de criptomoeda.

O valor do bitcoin depende da demanda da oferta e da via de regra, quanto mais transações existirem em dado momento, mais caro um Bitcoin será.

Mas como uma moeda digital pode ter e gerar valor se não há nenhum tipo de comando central?

Acontece que o Bitcoin é uma rede Peer-to-Peer (P2P), ou seja, ponto a ponto, o que significa que as transações são gerenciadas por cada um dos usuários que fazem parte do sistema.

Quando você realiza transações com Bitcoin, o computador ou tele móvel que você utiliza passa a participar da rede por meio da sua carteira Bitcoin. Se um nó sai dessa rede, os demais continuam mantendo o sistema funcionando. Se houvesse um controle central, bastaria que este fosse derrubado para o sistema cair para todo mundo.

Como estamos falando de um sistema de banco de dados distribuído e sem intermediários, precisamos de um mecanismo confiável para permitir transações diretas ponto a ponto. Esse é papel do blockchain.

Ok, agora vamos direto ao ponto o que realmente é a tecnologia blockchain?

O blockchain é um sistema de registro que contém todas as transações processadas no sistema. Traduzindo o nome significa *cadeia de blocos*. E uma cadeia de blocos é um conjunto de informações registradas que é ligada a blocos de informações anteriores e sucessores.

Esses blocos de informações também são públicos e todos os participantes da rede têm acesso. Porém, quando processados, os blocos não podem ser apagados ou alterados. Além disso, novos registros só podem ser feitos diante um processo de validação.

Esse sistema, por ser distribuído, está em milhares de computadores. Quando uma atualização legítima é feita, todos as cópias são sincronizadas em questão de segundos. Pode até ser que um ou outro computador desapareça da rede, mas isso não afetará o sistema, pois todos os outros nós ainda estão lá.

Para certificar uma informação em uma cadeia de blocos e evitar fraudes, o blockchain conta com um mecanismo chamado *prova de trabalho*. Trata-se de um protocolo criptográfico que valida uma transação em um dispositivo por meio da resolução de um problema matemático.

Adulterações nas cadeias de blocos, por menores que sejam, gerarão resultados diferentes do esperado para esse problema matemático. Isso impede o processamento da transação e, consequentemente, o seu registro.

Parar entendermos melhor como o blockchain funciona, convém olharmos um pouco os elementos que formam o sistema, começando pelos blocos.

Além do conjunto de transações, um bloco precisa ter um código que o liga ao bloco anterior, além de um código próprio que serve para conectá-lo ao bloco seguinte.

Mas como gerar esses blocos de modo seguro, sem que as conexões sejam alteradas para direcionar para um bloco ilegítimo, por exemplo?

Aqui, entram os mineiros ou mineradores o objetivo deles é resolver os problemas complexos do bloco, criar novos blocos e fazer à validação das transações.

Funciona assim: o software analisa o bloco e aplica uma fórmula matemática específica sobre os dados. O resultado do cálculo é um código chamado *hash*. Normalmente, esse código usa base hexadecimal.

Cada conjunto de dados é único, portanto, toda vez que essa fórmula matemática for aplicada no bloco, o código hash gerado será o mesmo. Mas, se o conjunto de dados sofrer alguma modificação, por menor que seja, o código hash será totalmente diferente. Aí não dá para ir adiante.

Além do seu próprio hash, o bloco contém o hash do bloco anterior. Dessa forma, um processo de verificação conseguirá perceber quando um bloco não é legítimo, pois o código hash deste será diferente dos registrados.

Agora vamos entender o que são os “nós”

Os nós são cada integrantes de uma certa rede. Assim, se você tem um computador com um software para realizar transações com Bitcoins, essa máquina acaba sendo um nó.

Esse software mantém e ajuda a distribuir cópias atualizadas em tempo real na cadeia de blocos. Cada vez que transações são realizadas blocos são adicionados e todos os nós são comunicados para que possam atualizar os registros com as novas informações.

O mecanismo de comunicação criptografada impede que essa rede seja invadida ou que os nós sejam adicionados inadequadamente.

Finalizando

O assunto é relativamente novo, por isso, as ideias em torno do conceito estão apenas começando a surgir. Mas, a proposta da cadeia de blocos tem enorme potencial e pode beneficiar os mais diferentes ramos de atividade.

As características do blockchain podem ser desvantajosas para determinadas aplicações, por exemplo, serviços que, em respeito às leis de privacidade, precisam permitir que os usuários apaguem seus dados a imutabilidade da cadeia de blocos é uma barreira para essa necessidade.

Ou seja as vantagens e desvantagens do blockchain precisam ser avaliadas em cada caso.