01

Criação de blocos e Mineração

Transcrição

[00:00] Neste laboratório, vamos visualizar e entender como é que funciona o Blockchain com exemplo de criação do bloco e simulação também de um processo de mineração. É legal que nós vamos exercitar e visualizar como funciona internamente a plataforma.

[00:27] Nesse exercício, a primeira coisa que vamos ver será a geração do Hash. O que é a geração do Hash? A geração do Hash é a criação de um número randômico, um número aleatório com base em um input. Esse número aleatório, com base na inserção de qualquer tipo de informação. Esse número aleatório chama-se o digest. Isso serve para validar informação que é armazenada tradicionalmente em um Blockchain público.

[01:07] Lembra quando eu comentei que nos Blockchains públicos é conveniente armazenar informação de uma maneira para garantir a prova de existência de informação de uma fonte, porque um Blockchain público você conseguiria visualizar toda informação que você grava? Então, melhor é gravar o código que referencia a informação que você possui? Bom, esse código é feito mediante o algoritmo, e esse código chama-se Hash.

[01:42] Então, vamos ver na prática como funciona a geração de um Hash. Clicando nesse link, entramos no site de anders. Ele fornece um exemplo de geração de Hash, assim como também geração de algoritmos de mineração. Então, primeiro conceito, vamos entender o que é essa geração desse código.

[02:10] Vamos colocar aqui: olá, estamos no curso de Blockchain para negócios. Cada vez que eu ia inserindo informação dentro deste texto, vocês viram que essa parte de Hash ia modificando e, automaticamente, ele vai gerando informação, mediante um algoritmo interno, vai gerando informação única para a informação que eu estou inserindo.

[02:54] Esta frase aqui tem está codificação que é única e irrepetível, ou seja, uma frase diferente a esta que acabo de colocar, não deveria gerar este mesmo código que estamos visualizando aqui. Para facilitar o entendimento, vejamos que esse código Hash termina em 35e. E a frase que eu acabo de colocar aqui, se eu mudo alguma coisa, esse Hash irá mudar. Mas se eu volto exatamente à mesma posição, ou à mesma frase, ela vai trazer o mesmo código que vemos aqui.

[03:4] Vamos para o exemplo. Se eu coloco um espaço, vocês viram que o Hash acabou mudando. Se eu tiro o espaço, vai voltar com 35e. O importante é que todo Hash que é gerado é único e é resistente a condições. Duas entradas diferentes nunca podem provocar um mesmo Hash, um mesmo resultado.

[04:16] Havendo entendido esse conceito, vamos para o segundo conceito que é o bloco. E agora, vamos entender porque eu acabo de explicar para que serve o Hash. Agora, dentro desta estrutura, vemos que o bloco tem uma numeração. Até por isso que se chama Blockchain. O que é Blockchain? Blockchain é um conjunto, uma cadeia de blocos, que armazena informação.

[04:44] Então, vemos aqui, o bloco vai ter uma numeração, nós estamos falando de uma cadeia, o bloco sempre tem que ter um bloco número 1. E posteriormente vai ser bloco 2, bloco 3. Pensem no Blockchain como se fosse um livro, onde cada bloco é uma página. E essa página tem uma numeração.

[05:05] Vemos aqui que no bloco número 1, podemos inserir informação. Então, vamos colocar curso de Blockchain. Vocês viram que quando eu mudei aqui e coloquei curso de Blockchain, passou de verde para o vermelho. Por que isso? Porque aqui o que nós vamos provar, é demonstrar como funciona o algoritmo de mineração.

[05:41] Todo bloco precisa ser validado. Lembra que eu comentei que a informação precisa ser validada pelos diferentes nós? Essa é base do consenso. Então, quando está vermelho, nesse caso aqui, significa que esse bloco não está validado. Neste exemplo, para que exista uma validação, um Hash calculado, todo bloco deve ser validado com o Hash que começa com 4 zeros.

[06:15] Ou seja, o bloco se considera como ok, que pode ser válido e aprovado dentro de um consenso, se o Hash desse bloco começa com 4 zeros. Não me perguntem, isso foi o que o fulano que criou, o Anders que criou este laboratório, especificou. O fato é que a regra de negócio de validação deste exemplo de Blockchain é um Hash que começa com 4 zeros.

[06:47] Vamos apagar todo o texto. Vocês viram que agora voltou a ficar verde. Por quê? Porque o bloco sem nenhum tipo de informação, e com o código, vemos aqui o Nonce 72608 mais nenhum tipo de informação, ou seja, os dados em estado de vazio, tem um Hash que começa com 4 zeros.

[07:22] Se eu coloco aqui o número 1, esse número 1, ou seja, a combinação do dado mais o Nonce, muda o número de Hash. Então, esse Hash aqui é a combinação do Nonce, que é um número aleatório, mais o que nós escrevemos aqui dentro do da parte dos dados.

[07:52] Como foi modificado esse bloco, nós temos que executar o processo de mineração. De que trata esse processo de mineração? Esse processo de mineração, o algoritmo que está por trás desta simulação, vai procurar, vai exercitar diferentes Nonces para que o dado, nesse caso o número 1, mais o Nonce que ele vai calculando, produza um Hash que começa com 4 zeros. Para quê? Para validar e dar o ok, que esse bloco está validado.

[08:29] Vamos fazer a mineração desse bloco. O que ele está fazendo agora? Vocês veem aqui que, internamente, ele está testando vários Nonces para calcular que, com o número 1, qual é o Nonce que vai gerar um Hash de 4 zeros. Nesse caso, foi rapidinho. Ele viu que o número 1, mais o Nonce 64840, gerou um bloco que começa com 4 zeros. Então, podemos dizer que este bloco está validado. Se eu faço algum tipo de modificação sobre os dados, novamente, esse bloco vai ficar inválido ou não validado.

[09:12] Vamos colocar aqui Blockchain. Veja que mudou, e agora o bloco não está validado. Então, nós temos que executar novamente o processo de mineração para que o algoritmo procure um Nonce contra a palavra, o valor ask da palavra Blockchain, para ver qual vai ser o Hash que vai produzir um Hash com 4 zeros na frente.

[09:38] Esse aqui vai demorar um pouquinho mais, foi rápido até. Mas o importante é que isso é a base de todo o Blockchain. Ou seja, eu não posso mudar nada sem ficar exposto.

[09:54] Com isso aqui, vamos passar para o terceiro passo, que é Blockchain. Estamos vendo aqui mais ou menos a mesma estrutura que nós vimos no laboratório anterior, no exercício anterior, mas o que vemos aqui é que temos vários blocos. Lembra que eu comentei que um bloco é uma página com o número. É o Nonce que é um número aleatório, para garantir um Hash de 4 zeros para validar essa informação. Aqui vemos bloco 1, bloco 2 e bloco 3. Imagina como se fosse um livrinho somente com três páginas.

[10:37] Todos eles estão validados. Se eu chego a fazer alguma modificação. Porque, novamente, o Nonce do bloco prévio, aqui vemos o bloco prévio. Novamente, lembra que Blockchain é um encadeamento de blocos, onde o bloco número 2 está referenciando o Hash do bloco número 1. O bloco número 1, observem aqui, que o Prévio do número 1 não tem, é 00000.

[11:09] Imagina o que vai acontecer aqui se eu chego a mudar esse dado. Onde diz dado, mas que não tem absolutamente nada. Vamos colocar o número 1. O que vai acontecer? Vai mudar absolutamente tudo, porque o número 1 vai ter mudado o Hash correspondente a esse bloco, agora não é mais um bloco começando com 4 zeros, mas

observem que os encadeamentos também não são mais válidos, porque se você volta para tudo 0, o encadeamento prévio começava com 4 zeros e o bloco número 2 também tem 4 zeros, então tudo validado.

[11:58] Se eu mudo aqui para 1, agora não vai estar validado e os seguintes também não estão validados. O que nós temos que fazer? Nós temos que minerar o bloco 1. Ele vai fazendo testes diferentes em Nonce. Mas olha só que interessante o que aconteceu. Ele somente validou o primeiro bloco. O segundo bloco, agora, ele atualizou. No segundo bloco, o bloco prévio, que corresponde o bloco número 1. E também, o que ele fez foi: ele ficou vermelho, por quê?

[12:30] Porque agora eu tenho também tenho que validar esse segundo bloco, eu tenho que minerar esse segundo bloco. Então, ele vai procurar se nada mais o Prévio mais o Nonce, ele vai procurar um Hash que tenha 4 zeros. Isso pode demorar um tempinho. Mas, basicamente, o que ele está fazendo, novamente, validando e, agora sim, ele achou o número e agora esse bloco está validado. E agora vamos para o terceiro e executamos exatamente a mesma operação.

[13:14] Aqui vemos claramente que se eu chego a modificar alguma coisa no primeiro bloco, todos os blocos seguintes vão ficar sem serem validados. Portanto, aqui prova o porquê é que Blockchain vem a trazer a transparência e a imutabilidade da informação.