03

Algoritmos de consenso

Transcrição

[00:00] Como comentei, vamos entender um pouco quais são os principais algoritmos de consenso que hoje as diferentes plataformas de Blockchain vem oferecer. O primeiro, e mais conhecido, é a prova de trabalho. Também conhecido em inglês como Proof of Work. Que é usado, é famoso, porque a rede Bitcoin é a que é utilizada. Mas também você já deve ter ouvido que ela tem uma reputação de consumir muita energia.

[00:31] Essa arquitetura do consenso é baseada em um processo chamado de mineração. Essa mineração, consideremos que é um algoritmo como se trabalhasse um quebra-cabeça computacional que serve para determinar quem vai ser o nó que vai criar um novo bloco. Ou seja, ele vai pegar todas essas transações, vai consolidá-las num novo bloco, vai validar. E logo depois, uma vez que estas transações também são validadas por outros nós, por outros participantes, essa transação é replicada entre esses outros nós.

[01:16] Agora, todo consenso dentro de Blockchain, todo algoritmo de consenso trabalha de maneira muito parecida. Mas a forma da execução que o consenso é executado é o que é diferente. O consenso dentro de prova de trabalho, um consenso dentro da rede de Bitcoin, cria mais ativos. De maneira automática, ele cria mais ativos Bitcoin. Vocês já devem conhecer que muitas pessoas entram na rede como mineradores por conta dos retornos econômicos que a rede acaba produzindo e distribuindo para os participantes que mineram essa informação.

[02:02] Mas o lado negativo é que esse tipo de consenso tem um grande desperdício de energia. Às vezes, é tão sério que a rede inteira de Bitcoin, do consenso prova de trabalho, acaba consumindo tanto quanto um pequeno país consome de energia.

[02:28] O segundo consenso está sendo adotado por plataformas como Ethereum, está dentro do mapa para serem adotadas em um futuro próximo. Vemos que é um consenso diferente ao de prova de trabalho. Chama-se prova de investimento, ou Proof of Stake. Onde validadores são responsáveis de validar a transação. Esses validadores são aqueles que têm maior investimento dentro da rede.

[03:07] Ou seja, se eu tenho mais investimento em dinheiro ou maior investimento em moedas, eu vou ser um validador, porque eu quero preservar a transparência da informação e a estabilidade da rede. Porque quanto mais investimento, mais recurso eu coloco dentro da rede, mais eu vou querer que esta rede funcione de maneira fidedigna.

[03:39] Os validadores validam as transações e também ganham uma taxa. Os nós são selecionados aleatoriamente para, entre esses validadores, validar e gerar os blocos do mesmo jeito que é gerado um bloco dentro da prova de trabalho.

[03:58] Obviamente, como comentei, depende do investimento. Os validadores participantes que tem maior investimento dentro da rede serão aqueles que têm mais possibilidade de minerar esse novo bloco. E garante uma maior economia de recursos computacionais e diminuindo o consumo de energia total da rede.

[04:24] O terceiro tipo de consenso é o prova de tempo decorrido. Proof of Elapsed Time, também conhecido como PoET. É um tipo de consenso que foi criado pela Intel e foi implementado dentro de plataformas de Blockchain, dentro do consórcio de Hyperledger, a plataforma de Sawtooth, que está muito mais focada para a operação de transações dentro de IoT.

[05:00] Podemos considerar que um consenso híbrido. O que é um consenso híbrido? É uma mistura entre uma Proof of Stake e um Proof of Work. Esse consenso determina que o algoritmo de consenso vai repartir, entre participantes,

numerinhos. E esse numerinho determina quanto tempo o participante tem que esperar na fila. Aquele que tem menor número, vai ser quem vai processar as suas transações primeiro.

[05:32] Seria, basicamente, como se tivesse um monte de gente dentro de uma sala, e uma pessoa estivesse repartindo números aleatoriamente e se organizando numa fila com base nesses números. Portanto, cada validador recebe um tempo de espera que simboliza sua posição dentro da fila para executar as transações.

[05:57] O quarto tipo de consenso é o Byzantine Fault Tolerance, ou seja, o consenso Bizantino tolerante a falhas. De que trata esse consenso? Esse consenso está muito mais focado em redes que chamamos de redes privadas, redes permissionadas. Por que é mais eficiente do que consensos anteriores, de prova de trabalho, prova de investimento? Porque é um consenso sistêmico, onde pode ser programável.

[06:36] Ou seja, dentro de um grupo de participantes, ou dentro de um grupo de nós, eu posso determinar quais serão os nós que irão validar a transação. Isso pode ser de maneira ordenada ou pode ser de maneira configurada dentro da rede. Ou seja, eu posso fazê-lo de maneira Round Robin, onde, dependendo da posição do servidor, ou do nó dentro da rede, pode executar essa validação.

[07:05] Ou, pode ser de maneira pré-programada dentro da plataforma de Blockchain. Portanto, sempre um único validador é o responsável de criar o bloco e consolidar todas as transações dentro dessa estrutura. É extremamente performático. A execução das transações basicamente é em segundos.

[07:33] O último tipo de consenso é a prova de autoridade, ou Proof of Autority. É basicamente um consenso parecido com uma prova de investimento, onde é um conjunto de autoridades que são as responsáveis de validar essas transações. E para submeter, ou criar um bloco validador, quem vai criar esse bloco requer a aprovação de todas as autoridades envolvidas, que são consideradas como autoridades dentro dessa rede.

[08:20] Para concluir este módulo, podemos ver que realmente Blockchain não é um bicho de sete cabeças. Blockchain está formado de 4 pilares. Temos um Ledger, que é uma base de dados que armazena informação e está configurada de maneira distribuída. Portanto, esse Ledger também garante a transparência e a imutabilidade da informação.

[08:53] Outro fator importante é criptografia. Cada participante dentro da rede, assim como também cada transação, é criptografada pelo próprio participante. O participante tem um certificado digital com o qual ele vai assinar essas transações. Portanto, toda transação dentro de Blockchain é de maneira privada e criptografada.

[09:27] Dependendo do Blockchain, dependendo da plataforma, dados também podem ser criptografado e podemos determinar quais participantes, ou quais usuários, podem ter acesso a essa informação e desencriptá-la. Isso vai depender um pouco das tecnologias de Blockchain que iremos adotar.

[09:53] O terceiro pilar tecnológico da plataforma são os Smart Contracts. E o que são Smart Contracts? Como vimos, Smart Contracts são as regras de negócio que são aplicadas sobre esses dados. Eu gosto de exemplificar Smart Contracts como a estrutura, como o Blockchain vai se comportar.

[10:18] Por exemplo, se eu tenho que transacionar um carro, a venda de um carro para outra pessoa. A regra de negócio do que deve acontecer nessa transação, quando eu transfiro o nome do meu carro para essa pessoa. É o que deve acontecer depois, uma vez que eu mudo esse nome, é o que está determinado em Smart Contract. Vamos supor que eu vendo o carro e essa pessoa tem que me pagar. O pagamento, uma vez que eu faço a transferência, pode ser feito de maneira automatizada.

[10:54] Porque, essa pessoa declarando a conta, e eu também declarando a conta origem e eu declarando a conta destino, o Smart Contract pode executar essa ação na hora que ele recebe a transação de transpasso ou de transferência

desse carro. O quarto pilar tecnológico é o consenso que garante a estabilidade e valida as transações para garantir uma ordem transacional dentro dessa rede.