Arthur Gomes de Siqueira

Blockchain é um sistema que permite rastrear o envio e recebimento de alguns tipos de informação pela internet. São pedaços de código gerados online que carregam informações conectadas – como blocos de dados que formam uma corrente, por isso o nome blockchain. Ele armazena as informações de um grupo de transações em blocos, marcando cada bloco com um registro de tempo e data. A cada período de tempo (10 minutos no blockchain), é formado um novo bloco de transações, que se liga ao bloco anterior. Tudo isso é registrado no livro de razão pública ou livro contábil, a qual qualquer um pode ter acesso, nele são registrados o histórico das transações como a quantia, quem enviou, quem recebeu, quando essa transação foi feita e em qual lugar do livro ela está registrada.

Dois exemplos:

O Bitcoin é uma moeda emitida de forma descentralizada e um software de código-fonte aberto, sustentado por uma rede de computadores distribuída (*peer-to-peer*) em que cada nó é simultaneamente cliente e servidor. Não há um servidor central nem qualquer entidade controlando a rede. O protocolo do Bitcoin, baseado em criptografia avançada, define as regras de funcionamento do sistema, às quais todos os nós da rede aquiescem, assegurando um consenso generalizado acerca da veracidade das transações realizadas e evitando qualquer violação do protocolo.

O maior exemplo de Blockchain pode-se dizer que é o Bitcoin porque a maior função do blockchain é a segurança dos dados e assegurar que seus blocos não sejam roubados, e quando nos tratamos de dinheiro, queremos evitar ao máximo perdé-lo então ai que entra a questão do blockchain dentro do bitcoin. Blockchain é a tecnologia que possibilitou a criação da bitcoin e de outras criptomoedas, como Ether e Litecoin. O Blockchain age como protetor do bitcoin, além de usar varias criptografias, varias formas de segurança pra proteger a moeda, ele ainda age como um livro de registro, como dito anteriormente, a quantia, quem enviou, quem recebeu, quando foi feita e em qual lugar do livro ela está registrada.

O segundo exemplo de Blockchain é a avalanche que é um protocolo blockchain criado para fornecer uma plataforma de código aberto para lançar aplicações financeiras descentralizadas e soluções empresariais em blockchain, essa plataforma de blockchain possui contratos inteligentes que confirmam transações em menos de um segundo, permitindo que milhões de validadores

independentes participem como nós de produção de blocos completos. O protocolo Avalanche integra o DirectAuth da Torus para fornecer aos usuários logins de apenas um clique. Essa Torus é uma empresa que permite que usuários comecem a usar aplicações em blokchain usando métodos familiares de autenticação, como o login no Google ou no Facebook.

Proof of Work (PoW): Usa poder computacional para solucionar problemas matemáticos

Proof of Stake (PoS): Usa capital alocado, riqueza de um elemento da rede, idade das moedas e fatores de randomização.

O Proof of Work é um algoritmo de consenso no qual é caro e demorado produzir uma parte dos dados, mas é fácil para outras pessoas verificarem se os dados estão corretos, é baseada em uma forma avançada de matemática chamada 'criptografia'. É por isso que moedas digitais como Bitcoin e Ethereum são chamadas de criptomoedas. A criptografia usa equações matemáticas que são tão difíceis que apenas computadores poderosos podem resolvê-las. Nenhuma equação é a mesma, o que significa que, uma vez resolvida, a rede sabe que a transação é autêntica. O problema de usar um sistema assim é que isso acaba dependendo muito das vezes do poder computacional sem falar que gasta muito energia para fazer um processamento. Devido a isso, não só precisa de quantidades significativas de eletricidade, mas também é muito limitado no número de transações que pode processar ao mesmo tempo. Como resultado, outros mecanismos de consenso foram criados, sendo um dos mais populares o modelo de Proof of Stake. O algoritmo de Proof of Stake usa um processo de eleição pseudo-aleatória para selecionar um nó (node) para ser o validador do próximo bloco, com base em uma combinação de fatores que podem incluir a idade da participação, a randomização e a riqueza do nó. Os benefícios iniciais incluem um sistema de mineração mais justo e igualitário, transações mais escalonáveis e menos dependência de eletricidade.

O Blockchain inicialmente adotou o Proof of Work como ponto de partida, toda vez que uma transação é enviada, demora cerca de 10 minutos para a rede confirmá-la. Além disso, o blockchain Bitcoin só pode manipular cerca de 7 transações por segundo.

As transações são verificadas com Proof of work da seguinte forma, lembra que as transações com o Bitcoin demoram 10 minutos antes de serem confirmadas como válidas. Bem, em cada intervalo de 10 minutos, algo chamado de “novo bloco” é criado. Cada bloco contém diferentes transações dentro dele, que

devem ser verificadas independentemente. Para que a rede Bitcoin consiga isso sem um terceiro, alguém deve usar seu poder computacional para resolver um algoritmo criptográfico, por isso que muitas das vezes as pessoas relacionam o Proof of Work com o poder computacional porque quem consegue resolver, é quem tem o maior poder computacional. Uma vez que isso seja alcançado, não apenas a transação é marcada como válida, mas também é postada no blockchain público para que todos possam ver. As pessoas são recompensadas com Bitcoins adicionais (ou qualquer outra criptomoeda confirmada através da PoW) através desse acerto, caso seu poder computacional resolva o algoritmo de criptografia, você recebe uma recompensa. Milhares de dispositivos individuais competem para se tornar os primeiros a resolver o algoritmo criptográfico. Quem chegar primeiro, ganha a recompensa.

Mas o problema disso como dito anteriormente, é o alto custo de energia porque o algoritmo de Proof of Work se basea no poder computacional e lembre-se que demora cerca de 10 minutos para que a transação esteja correta e apenas um está correto, ou seja, os demais que também estavam correndo atrás para decifrar a criptografia também estavam gastando tempo e energia, devido a isso, o Proof of Work tem essa desvantagem de gastar muito dinheiro com energia, além de ser um sistema injusto, porque aqueles com os dispositivos de hardware mais poderosos e caros sempre terão a maior chance de ganhar recompensa. Por isso foi desenvolvido uma outra técnica pra mudar essa ideia, que é o Proof of Stake. O modelo de Proof of Stake usa um processo diferente para confirmar transações e chegar a um consenso. O sistema ainda usa um algoritmo criptográfico, mas o objetivo do mecanismo é diferente. Enquanto a Proof of Work recompensa seu minerador pela resolução de equações realmente complexas, em Proof of Stake, o indivíduo que cria o próximo bloco é baseado no quanto eles “colocaram”. O Proof of Stake é baseada na quantidade de moedas que a pessoa possui da blockchain específica que está tentando minerar. No entanto, tecnicamente falando, os indivíduos não estão realmente minerando. Em vez disso, eles são chamados de "cunhadores", porque não há recompensa em bloco. Enquanto o Bitcoin, que usa o modelo de Proof of Work, concede uma recompensa de bloco toda vez que um novo bloco é verificado, aqueles que contribuem para o sistema de Proof of Stake simplesmente ganham a taxa de transação. Para ter a oportunidade de validar transações, o usuário deve colocar suas moedas em uma carteira específica. Esta carteira congela as

moedas, o que significa que elas estão sendo usadas para "estacar" a rede. A maioria dos blockchains que utilizam Proof of Stakes possui um requisito mínimo de moedas necessárias para iniciar o staking, o que, é claro, requer um grande investimento inicial, ou seja, suas chances de ganhar a recompensa (taxas de transação) estão vinculadas à porcentagem total de moedas que você possui.

Resumindo

A Proof of Work exige que TODOS os mineradores tentem resolver uma equação realmente complexa, com o vencedor sendo determinado pela pessoa que possui dispositivos de hardware mais poderosos.

O modelo da Proof of Stake aleatoriamente escolhe o vencedor com base na quantidade de moeda que ele resolveu colocar para validar as transações.

Desvantagens do Proof of Work:

Além do aspecto da energia, que usam grandes quantidades de eletricidade temos duas outras desvantagens como a centralização que dão às pessoas que compram dispositivos de hardware poderosos uma chance maior de ganhar a recompensa de mineração. Devido a isso, a pessoa média não tem chance de ganhar a recompensa da mineração. Outra desvantagem é o Ataque de 51% que é usado para descrever o evento infeliz que um grupo ou uma pessoa solitária ganha mais de que 50% do poder total de mineração. Se isso acontecer em uma blockchain de Proof of Work como Bitcoin, permite que o grupo ou a pessoa faça alterações em um determinado bloco. Se essa pessoa ou o grupo tiver intenções criminosas, o blockchain será alterado de modo a prover ganhos pessoais.

Desvantagens do Proof of Stake:

O tópico mais obvio seria que a pessoa que tem mais dinheiro sai com mais vantagem aqui, Isso porque quanto mais moedas você puder comprar, mais moedas você pode congelar e ganhar com as taxas de transação, ou seja, aqueles que têm mais dinheiro sempre terão a melhor chance de ganhar a recompensa, tornando os ricos mais ricos. A outra desvantagem é que ela permite que as

pessoas verifiquem transações em várias cadeias, o que a Proof of Work não faz. A razão pela qual isso pode ser um problema é que ele pode permitir que um hacker realize um ataque de "gasto duplo". É quando alguém transfere fundos para outra pessoa, mas antes que a transação seja confirmada, eles conseguem gastar os fundos novamente