COMO FUNCIONA A MINERAÇÃO DO CRIPTOMOEDAS:

Processo exige realização de 'apostas'

1.

ELO

Código matemático que liga o bloco ao seu antecessor.

2.

TRANSAÇÕES

Conjunto de transferencias solicitadas pelos usuários da rede.

3.

CHAVE NONCE

Número 'apostado' pelo minerador para criar um bloco aceito na rede.

Os dados da composição do bloco são processados por uma fórmula de 'hash' - um gerador de números com características especiais para validação de dados.

O sorteio: A formula hash que valida o bloco tem resultados imprevisíveis, criando um ciclo de tentativa e erro. Esse mecanismo atua como contrapeso para evitar desestabilizar a rede pela criação desenfreada de blocos. As transações já foram validadas antes desse 'sorteio' mas elas dependem dele parra serem registradas.

O bolão do sorteio: Mineradores que colaboram entre si dividem as apostas, formando um 'bolão'. Os concorrentes realizam a tarefa ao tempo, tentando 'acercar primeiro'.

RESULTADO INVÁLIDO

O minerador escolhe outra chave nonce e repete o processo.

RESULTADO VÁLIDO:

O minerador envia o bloco de rede para liga-lo a sequencia de blocos(Blockchain).

ENCAIXE DO BLOCO:
O bloco válido é ligado á sequência de blocos.

O ELO DA PROVA DE TRABALHO: Para o biltcoin, o processamento empregado define a força do elo. Quanto maior for a carga de processamento, mais difícil é refazê-la para anular transferências passadas, gerando mais segurança.

10 minutos

TEMPO: Nas moedas, esse processo deve levar 10 minutos. O número de chaves possíveis é reduzido ou aumentado periodicamente para mantes esse ritmo.

TUDO DE NOVO:
Após o bloco na sequência, forma-se um novo bloco com transferências pendentes. Como os dados são inéditos, o processo de tentativa e erro recomeça do zero.

DEFINIÇÕES:	
CRIPTOMOEDAS:	São moedas que usam princípios da criptografia para substituir bancos por elos matemáticos.
BLOCO:	Um segmento de dados que contém transações.
BLOCKCHAIN	O conjunto de todos os segmentos de dados e suas transações.
TRANSAÇÃO	Criptomoedas não precisam de saldos, pois todas as trocas são registradas pelas transações.
HASH:	Algoritmo de computador criado para gerar resultados ao mesmo tempo imprevisíveis e reprodutíveis.
MINERAÇÃO:	Processo que agrega as transações em blocos. O hash do bloco deve atender um critério da rede.
ASIC:	Chip criado para uma tarefa específica, como o hash do bitcoin.
GPU:	Chip de processamento de vídeo que é mais veloz para a mineração de algumas moedas.
CHAVE DE BLOCO:	Número que teve de ser encontrado pelo minerador para direcionar o hash para o resultado desejado.
ATAQUE DE 51%:	Cenário em que alguém controla poder de processamento suficiente para encontrar muitas chaves de bloco consecutivas, formar uma nova blockchain e apagar transferências realizadas no passado.