**1a.5 - Proof-of-Work e Mineração**

Como já vimos o Proof-of-Work (PoW) é um tipo de Mecanismo de Consenso que é utilizado para a validação da adição de um bloco no Blockchain.

O PoW é o Algoritmo de Consenso utilizado pelo Bitcoin para validar um bloco no ledger (Blockchain), a validação ocorre por meio de um objetivo (prova de trabalho) que os mineradores tentam efetuar, este objetivo exige uma grande capacidade de Hardware. O minerador que conseguir cumprir o objetivo adicionará o bloco ao Blockchain e também será recompensado com bitcoin.

**Como funciona?**

No caso de blockchains que utilizam o PoW como mecanismo de consenso, o bloco possui mais um campo: o Nonce.

O Nonce é o número aleatório definido pelo máquina do minerador que juntamente com o Dado do bloco e o Hash Anterior do bloco resultará, através do Hash-SHA256, no Hash atual do bloco.

Veja um exemplo de um bloco portanto:



O objetivo é voce gerar um Hash (numero hexadecimal) que seja menor que um determinado Hash, então por exemplo um objetivo pode ser gerar um Hash que tenha pelo menos 4 zeros à esquerda.

Então os mineradores terão que de ir variando o Nonce para que consigam resultar um Hash que tenha pelo menos 4 zeros à esquerda. Você deve entender que essa tarefa não é fácil, pois há uma imensa quantidade de numeros possíveis maiores que o objetivo, e não há nenhuma lei lógica que o Nonce fará com que gere um Hash menor, ou seja, o minerador terá que usar uma capacidade gigantesca de Hardware para gerar Nonces aleatórios, tal que gere um que faça com que o Hash daquele bloco cumpra o objetivo.

Após 10 minutos o minerador que gerou o menor Hash ganhará, adicionando o bloco no Blockchain e sendo recompensado com bitcoin.



